PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 19 (10) 2018

INTERNAL SECURITY REVIEW

WARSAW 19 (10) 2018

ISSN 2080-1335

Wszystkie artykuły zamieszczone w czasopiśmie są recenzowane
All the articles published in the magazine are subject to reviews

Deklaracja o wersji pierwotnej:
Wersja drukowana czasopisma jest jego wersją pierwotną
Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) znajduje się na liście czasopism naukowych Ministra Nauki i Szkolnictwa Wyższego z liczbą 5 punktów za umieszczone w nim publikacje. PBW można odnaleźć także w *Index Copernicus Journal Master List* z liczbą 48,72 punktów. Czasopismo jest również dostępne w bazach: *Central European Journal of Social Science and Humanities* i Polska Bibliografia Naukowa (PBN).

Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia im. gen. dyw. Stefana Roweckiego „Grota" w Emowie
05-462 Wiązowna, ul. Nadwiślańczyków 2

Redakcja
tel. (+48) 22 58 58 613
fax. (+48) 22 58 58 645
e-mail: redakcja.pbw@abw.gov.pl
www.abw.gov.pl

Numer zamknięto i oddano do druku we wrześniu 2018 r.

Druk: Biuro Logistyki
Agencji Bezpieczeństwa Wewnętrznego
00-993 Warszawa, ul. Rakowiecka 2A
tel. (+48) 22 58 57 657

SPIS TREŚCI
TABLE OF CONTENTS

I. ARTYKUŁY I ROZPRAWY

II. RECENZJE

III. SPRAWOZDANIA

IV. ARTICLES AND DISSERTATIONS

I
ARTYKUŁY I ROZPRAWY

Waldemar Walczak

Korupcja jako sieć wpływów, powiązań i zależności

Wprowadzenie

Zachowania korupcyjne wpisują się w nurt zagadnień chętnie popularyzowanych i wykorzystywanych przez media przy okazji ożywionych dyskusji oraz sporów o charakterze politycznym, jakie występują w przestrzeni publicznej. Pojawiają się zdawkowe komentarze mające charakter emocjonalny, natomiast wyraźnie zauważalny jest deficyt pogłębionej, merytorycznej wiedzy na temat omawianego zjawiska, a także jego bezstronnej analizy. Korupcja z uwagi na swoją złożoność oraz wieloaspektowość coraz częściej staje się przedmiotem licznych opracowań naukowych. Potrzeba szerszych dociekań badawczych jest racjonalnie uzasadniona zarówno z uwagi na walory teoriopoznawcze, jak i utylitarne. Poruszany temat lokuje się bowiem w kręgu zainteresowań służb specjalnych, które w ramach swoich ustawowych obowiązków zajmują się rozpoznawaniem, zapobieganiem i zwalczaniem korupcji w życiu publicznym oraz gospodarczym.

Celem rozważań i analiz prowadzonych w artykule jest przedstawienie istoty zjawiska korupcji postrzeganej w aspekcie uwarunkowań organizacyjnych i prawnych występujących w otoczeniu społeczno-gospodarczym, które w najwyższym stopniu rzutują na powszechnie stosowane metody zarządzania oraz procesy decyzyjne. Na wstępie wyjaśniono, jak należy rozumieć pojęcie k o r u p c j a, a także scharakteryzowano główne mechanizmy korupcjogenne. W dalszej części artykułu przeanalizowano zjawisko korupcji jako element systemu zarządzania. Zwrócono przy tym uwagę na zagrożenia interesów ekonomicznych państwa, a także naruszanie zasad praworządności i sprawiedliwości społecznej. Ważnym argumentem przemawiającym za zasadnością szerokiego podejścia do tego problemu badawczego jest komunikat umieszczony na stronie internetowej Centralnego Biura Antykorupcyjnego. Jego treść w sposób czytelny doprecyzowuje niebezpieczeństwa związane z występowaniem omawianego zjawiska: *Korupcja zagraża praworządności, demokracji, prawom człowieka, narusza zasady uczciwości społecznej, spowalnia rozwój gospodarczy i zagraża stabilności instytucji demokratycznych i moralnym podstawom państwa* (preambuła *Prawnokarnej Konwencji o Korupcji sporządzonej w Strasburgu dnia 27 stycznia 1999 r.*, Dz.U. z 2005 r. nr 29 poz. 249)[1].

[1] Biuletyn Informacji Publicznej CBA, https://bip.cba.gov.pl/bip/nabor-do-sluzby/profile-kandydatow/ekonomisci/14,Ekonomisci.html [dostęp: 10 I 2018].

Definiowanie korupcji

Punktem wyjścia do dalszych rozważań jest wyjaśnienie przyjętego w pracy rozumienia terminu k o r u p c j a. Jest bezwarunkowo konieczne ze względu na różnorodność oraz wieloznaczność ujęć definicyjnych[2], a także na postrzeganie omawianego zjawiska przez pryzmat określonych wzorców zachowań stanowiących punkt odniesienia[3]. Należy zaznaczyć, że informacje wskazujące na sposób rozumienia i pojmowania istoty korupcji mają znaczenie fundamentalne[4], gdyż determinują wykładnię interpretacyjną danego pojęcia, a w konsekwencji – wyznaczają kierunki dalszych czynności analitycznych oraz dociekań badawczych. Przy uwzględnieniu powyższych przesłanek, k o r u p c j a będzie postrzegana w szerokim ujęciu jako **wykorzystywanie władzy**, **wpływów**[5] i **pozycji zawodowej** do realizacji **partykularnych interesów i celów**. Oznacza to, że analizowane zjawisko obejmuje swoim zakresem pojęciowym zarówno przestępstwa korupcyjne, jak i wszystkie pozostałe formy tzw. legalnej korupcji, która nie jest sankcjonowana na gruncie przepisów kodeksu karnego.

W zaproponowanej definicji trzeba zwrócić uwagę na celowo użyte sformułowanie „wykorzystywanie władzy", w istotny sposób różniące się z prawnego punktu widzenia od sfomułowania „nadużywanie władzy", które może być traktowane w odniesieniu do określonej kategorii osób jako „przekroczenie uprawnień" opisywane w art. 231 kk. Przedstawiając merytoryczną i rzeczową argumentację uzasadniającą słuszność poczynionych założeń, warto odwołać się do zapisów zawartych w oficjalnym dokumencie rządowym, jakim jest *Rządowy Program Przeciwdziałania Korupcji na lata 2014–2019*[6] przyjęty przez Radę Ministrów. We wstępnej części przywołanego opracowania znajduje się następujący fragment: *Legalna definicja korupcji zawarta jest w art. 1 ust. 3a ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (Dz.U. z 2012 r. poz. 621, z późn. zm.) i do takiej w głównej mierze odwołuje się*

---

[2] A. Kubiak, *Działania antykorupcyjne – wybrane przykłady*, „Acta Universitatis Lodziensis Folia Oeconomica" 2013, nr 288, s. 45–46; K. Nowakowski, *Korupcja a instytucje w gospodarce*, „Ekonomia i Prawo" 2006, nr 1, s. 140–148; A. Stachowicz-Stanuch, A. Sworowska, *Definiowanie korupcji w kontekście różnic kulturowych*, „Organizacja i Zarządzanie" 2012, nr 1, s. 97–116.

[3] K. Dzietczyk, *Zjawisko korupcji jako element życia społecznego*, „Seminare. Poszukiwania naukowe" 2016, nr 3, s. 111–121; A.Z. Kamiński, *Korupcja jako symbol instytucjonalnej niewydolności państwa i zagrożenie dla rozwoju polityczno-gospodarczego Polski*, „Zeszyty Centrum im. Adama Smitha" 1997, nr 29, s. 3–32; K. Nowakowski, *Korupcja jako problem teoretyczny i społeczno-ekonomiczny*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 2, s. 77–94; J. Svensson*, Osiem pytań na temat korupcji*, „Gospodarka Narodowa" 2006, nr 9, s. 77–106.

[4] R. Maćkowska, *Informacja w przestrzeni publicznej a zjawisko korupcji i jego postrzeganie*, w: *Public relations w perspektywie naukowej*, A. Adamus-Matuszyńska (red.), Katowice 2016, s. 116–124.

[5] Wyróżnienia w tekście pochodzą od autora (przyp. red.).

[6] *Uchwała nr 37 Rady Ministrów z dnia 1 kwietnia 2014 r. w sprawie Rządowego Programu Przeciwdziałania Korupcji na lata 2014–2019* (M.P. z 2014 r. poz. 299); https://cba.gov.pl/pl/publikacje/strategia-antykorpcyjna/3409,Rzadowy-Program-Przeciwdzialania-Korupcji.html [dostęp: 10 I 2018].

„Program". Nie należy jednak zapominać ***o niekaralnych formach korupcji****, jak konflikt interesów, nepotyzm i kumoterstwo, które stanowią również problem życia publicznego, i dlatego niniejszy dokument odnosi się również do tych rodzajów szeroko pojmowanego zjawiska korupcji.*

Wnikliwa analiza zacytowanej wykładni interpretacyjnej dokonanej przez Radę Ministrów odnośnie do występujących form korupcji w jednoznaczny sposób potwierdza prawidłowość przyjętej w artykule koncepcji na temat wieloaspektowego podejścia do rozpatrywanego zjawiska. Ponadto daje podstawy prawne do tego, aby przy opisywaniu określonych działań, podejmowanych decyzji i wzorców zachowań konkretnych osób było możliwe używanie adekwatnej terminologii.

Zdaniem szefa CBA (…) *korupcja to wielowymiarowe zjawisko analizowane i diagnozowane w najważniejszych dla funkcjonowania państwa aspektach: społecznym, etycznym i prawnym*[7]. Można natomiast polemizować z poglądem, że (…) *przestępczość korupcyjna narusza podstawowe zasady funkcjonowania państwa*[8]*,* ponieważ wszystkie kategorie zachowań korupcyjnych obejmujące swoim zakresem tzw. legalną korupcję zagrożają interesom ekonomicznym kraju, poczuciu bezpieczeństwa obywateli, a także rażąco dewastują zasady praworządności i sprawiedliwości społecznej. Zasadne będzie tutaj odwołanie się wprost do brzmienia art. 2 Konstytucji RP, w którym wyraźnie stwierdzono: *Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej*[9].

Agata Miętek, analizując ten konstytucyjny zapis, słusznie zauważa, że ostatni człon tego zdania, wskazujący na potrzebę urzeczywistniania zasad sprawiedliwości społecznej przez państwo, jest przedmiotem znacznie mniejszego zainteresowania niż idea demokratycznego państwa prawa[10]. Jest to bardzo zasadna refleksja, z którą trzeba się zgodzić.

Mechanizmy korupcjogenne

Alina Hussein, która opisała główne obszary zagrożenia korupcją widziane z perspektywy Najwyższej Izby Kontroli, zwraca uwagę na zlecanie przez podmioty publiczne usług zewnętrznych podmiotom prywatnym oraz na sferę lokalizacji inwestycji budowlanych[11]. Korzystanie z usług eksperckich i doradczych jest opisywane następująco: (...) *zlecanie usług zewnętrznych często odbywa się bez analizy potrzeb (wskutek czego zamawiane są zbędne usługi), przestrzegania reguł zamówień publicznych i kon-*

[7] *Mapa korupcji. Zwalczanie przestępczości korupcyjnej w Polsce w 2016 r*., Warszawa 2017, s. 5.

[8] Tamże.

[9] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r*. (Dz.U z 1997 r. nr 78 poz. 483, ze zm.).

[10] A. Miętek, *Zasada demokratycznego państwa prawnego w orzecznictwie Trybunału Konstytucyjnego*, „Dialogi Polityczne III RP" 2009, nr 11, s. 76.

[11] A. Hussein, *Obszary zagrożenia korupcją – przegląd badań NIK opublikowanych w 2016 roku*, „Kontrola Państwowa" 2017, nr 5, s. 51.

kurencji, zachowania wymaganej przejrzystości działania. Wynagrodzenia podmiotów zewnętrznych są zawyżane, warunki umów bywają jednostronnie korzystne dla prywatnych usługodawców, a niekorzystne dla instytucji publicznych[12].

W cytowanym opracowaniu są przytaczane wielomilionowe kwoty, jakie zostały wypłacone z tytułu umów ujawnionych podczas kontroli (m.in.: sfinansowanie umów z agencjami pracy tymczasowej w czterech sądach apelacji warszawskiej – 15 mln zł, umowy na usługi doradcze i eksperckie w latach 2012–2014 w czterech spółkach grupy PKP – ponad 171 mln zł), a w odniesieniu do opisywanych zdarzeń używa się następującego sformułowania: (…) *nieprawidłowości noszące cechy mechanizmów korupcjogennych*[13]. Jest to niezwykle wymowne i symptomatyczne, zwłaszcza w kontekście braku jakiejkolwiek wzmianki na temat odpowiedzialności z tytułu podejmowanych decyzji. A to dzięki określonym decyzjom pokaźne sumy pieniężne trafiły na konta wybranych beneficjentów.

Dla dalszych rozważań niezbędne jest omówienie wybranych terminów i podjęcie próby ukazania zjawiska korupcji w aspekcie systemowym. W pierwszej kolejności trzeba wyjaśnić, czym są mechanizmy korupcjogenne. W nomenklaturze stosowanej przez NIK pod tym pojęciem należy rozumieć (…) *nieprawidłowości w funkcjonowaniu instytucji publicznych, które powodują bądź zwiększają ryzyko korupcji*[14]. Innymi słowy, są to czynniki i uwarunkowania sprzyjające występowaniu praktyk korupcyjnych. Najwyższa Izba Kontroli zwraca uwagę na cztery najważniejsze przesłanki: (…) *dowolność postępowania, konflikt interesów, brak wymaganej jawności postępowania, brak lub słabość kontroli*[15]. Warto wspomnieć, że konflikt interesów został wymieniony w *Rządowym Programie Przeciwdziałania Korupcji na lata 2014–2019* **w podwójnym znaczeniu**, tj. jako niekaralna forma korupcji: (…) *nie należy jednak zapominać o niekaralnych formach korupcji, jak konflikt interesów*[16] oraz jako jeden z rozpoznanych mechanizmów korupcjogennych[17]. Zdaniem NIK konflikt interesów to (…) *sytuacja, w której urzędnik sprawujący funkcję publiczną jest uwikłany w kolidujące z tą funkcję interesy prywatne*[18]. W dokumencie Rady Ministrów jest z kolei znacznie szerszy opis: *O konflikcie tym mówimy wówczas, gdy urzędnik podejmujący rozstrzygnięcie w określonej sferze spraw publicznych lub uczestniczący w przygotowaniu tego rozstrzygnięcia ma lub może mieć osobisty interes w sposobie załatwienia sprawy. Do konfliktu dochodzi nie tylko wtedy, gdy urzędnik w danej sprawie działa w osobistym interesie, ale także gdy istnieje choćby tylko teoretyczna możliwość, że interes ten przeważy nad troską o interes publiczny*[19].

---

[12] Tamże.

[13] Tamże, s. 52.

[14] A. Hussein, *Mechanizmy korupcjogenne – cztery grzechy główne władz publicznych*, „Przegląd Antykorupcyjny" 2011, nr 1, s. 43.

[15] Tamże, s. 44.

[16] *Rządowy Program Przeciwdziałania Korupcji na lata 2014–2019*, s. 7.

[17] Tamże, s. 19.

[18] A. Hussein, *Mechanizmy korupcjogenne*..., s. 44.

[19] *Rządowy Program Przeciwdziałania Korupcji na lata 2014–2019*, s. 19.

Analiza komparatywna zacytowanych interpretacji pozwala zauważyć pewne różnice mające zasadniczy wpływ na sposób rozumienia istoty omawianego problemu. W jednej z opinii zostało użyte określenie „uwikłany" w aspekcie już występujących okoliczności, a z kolei w drugim przypadku akcentuje się samo prawdopodobieństwo, tj. teoretyczną możliwość zaistnienia takiej sytuacji w procesie podejmowania decyzji. Te spostrzeżenia wskazują na to, jak odmienne może być postrzeganie określonych kwestii, a także na wieloznaczność zwrotu „konflikt interesów". Niestety, w polskim ustawodawstwie nie istnieje prawna definicja tego pojęcia, co ma istotne znaczenie w prowadzonych rozważaniach. W nawiązaniu do tych refleksji pojawiają się trzy pytania:

1. Czy sytuacja, jaką jest konflikt interesów, słusznie (prawidłowo) została wprost wymieniona w dokumencie rządowym jako niekaralna forma korupcji i jednocześnie szczególnie niebezpieczny mechanizm korupcjogenny?
2. Czy jest logiczne i uprawnione, aby konflikt interesów zawężać jedynie do zdarzeń, kiedy mamy do czynienia z podejmowaniem decyzji przez urzędników?
3. Jakie są inne czynniki i uwarunkowania sprzyjające występowaniu korupcyjnych praktyk?

Odpowiedź na pierwsze pytanie jest twierdząca, co oznacza, że powstanie sytuacji konfliktu interesów jest traktowane jako jedna z form tzw. legalnej korupcji.

Odnośnie do drugiego pytania trzeba zaznaczyć, że w każdym przypadku dotyczącym wykorzystywania władzy i przyznanych uprawnień decyzyjnych w związku z zajmowanym stanowiskiem w danej organizacji może zaistnieć realny konflikt interesów. A zatem nie należy tego pojęcia ograniczać jedynie do działań urzędników, gdyż sprzeczność interesów może zachodzić nie tylko w innych instytucjach publicznych (np. sądach, prokuraturach, szpitalach czy uczelniach wyższych) bądź spółkach z udziałem kapitałowym państwowych osób prawnych, lecz także we wszystkich – bez wyjątku – pozostałych kategoriach podmiotów prywatnych. Dość powszechne są zdarzenia, procesy i decyzje, kiedy uwzględnia się zarówno interes publiczny oraz dobro wspólne, jak i interes partyjny, korzyści osobiste określonej korporacji zawodowej, profity prywatnego biznesu, danej fundacji, firmy, grupy koleżeńskiej, znajomych, kolegów itd.

W ocenie rządu RP do pozostałych **mechanizmów korupcjogennych** zalicza się:

- nieprawidłowości w procesie stanowienia prawa: naruszanie obowiązujących procedur legislacyjnych, a zwłaszcza pomijanie niezbędnego trybu opiniowania lub uzgodnień międzyresortowych; dokonywanie zmian w projektach już uzgodnionych, wydawanie aktów wykonawczych ze znacznym opóźnieniem, pozostawianie luk i niejednoznaczności**,** co sprzyja dowolnej interpretacji przepisów, niespójne nowelizowanie ustaw, wytwarzanie coraz większej liczby aktów prawnych,
- kumulowanie uprawnień: nadmierne skupianie uprawnień decyzyjnych i odchodzenie od zasady rozdzielania czynności dotyczących jednej sprawy pomiędzy różnych urzędników,

- lekceważenie dokumentacji i sprawozdawczości: przyjmowanie niepełnej dokumentacji, bez wszystkich dowodów lub załączników wymaganych procedurą, odstępowanie od wypełnienia wymaganych obowiązków sprawozdawczych, a także podejmowanie decyzji bez ich uzasadniania, wskutek czego jest utrudnione kontrolowanie procedur decyzyjnych,
- brak odpowiedzialności osobistej za podejmowane rozstrzygnięcia[20].

Z punktu widzenia praktyki zarządzania istotne znaczenie mają: kumulowanie władzy, łączenie funkcji i zajmowanie wielu stanowisk przez jedną osobę. Są to niezwykle ważne czynniki, których roli nie można deprecjonować.

Korupcja jako element systemu zarządzania

W celu prawidłowego zrozumienia **obszarów i form korupcji** występujących w rzeczywistości organizacyjnej będzie pomocne omówienie kilku zasadniczych zagadnień odnoszących się do paradygmatów zarządzania stosowanych w praktyce, które, niestety, różnią się od idei popularyzowanych w teoriach naukowych.

1. Korupcja sprowadza się do wykorzystywania możliwości wynikających ze sprawowanej władzy i przyznanych (posiadanych) uprawnień decyzyjnych w celu zapewnienia korzyści osobistych oraz majątkowych, co powoduje że staje się nieodłącznym elementem procesów zarządczych. Zgodnie z art. 115 § 4 kk (…) *korzyścią majątkową lub osobistą jest korzyść zarówno dla siebie, jak i dla kogo innego*[21]. Zdaniem CBA pod pojęciem k o r z y ś ć m a j ą t k o w a należy rozumieć różne dobra zaspokajające określone potrzeby, których wartość daje się wyrazić w pieniądzu. Do korzyści majątkowych oprócz gotówki zalicza się m.in.: (…) *atrakcyjne przedmioty, wycieczki, jak również pożyczki udzielane na preferencyjnych warunkach, umorzenia długów czy udzielenie zamówienia publicznego*[22]. Niejednokrotnie w praktyce korzyść osobista polepszająca sytuację osoby, która ją uzyskuje, bezpośrednio łączy się z korzyścią materialną, np. awans w pracy lub przyjęcie do pracy, bezpłatny wyjazd na atrakcyjne szkolenie zawodowe, przyjęcie na praktykę, wysłanie na zagraniczne stypendium itp.
2. Zarządzanie organizajami polega przede wszystkim na gospodarowaniu powierzonym majątkiem i finansami osób trzecich, co sprawia, że takie pojęcia, jak „oszczędność", „gospodarność", „celowość" i „racjonalność ponoszonych wydatków" są zupełnie inaczej postrzegane niż w sytuacji, kiedy są wydawane własne pieniądze. Dla przykładu: osoby zasiadające we władzach instytucji sektora finansów publicznych rozporządzają majątkiem państwowym i podejmują decyzje w zakresie wydawania pieniędzy podatników, a nie osobistych. Władze spółdzielni mieszkaniowej zarządzają majątkiem będącym wspólną własnością jej członków, a nie swoim własnym, a w sprawach finansów dysponują wpła-

[20] Tamże, s. 19–20.
[21] *Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny* (Dz.U. z 1997 r. nr 88 poz. 553, ze zm.).
[22] *Mapa korupcji. Zwalczanie przestępczości*…, s. 23.

tami otrzymywanymi od mieszkańców. Banki oraz inne instytucje finansowe, np. SKOK-i, zarządzają aktywami powierzonymi im przez obywateli; prezesi spółek ze stuprocentowym udziałem Skarbu Państwa gospodarują mieniem państwowym, władze spółek komunlnych – samorządowym, osoby zasiadające we władzach spółek prywatnych – majątkiem danego podmiotu i finansami otrzymywanymi od klientów, władze fundacji wydają środki finansowe otrzymywane od darczyńczów, sponsorów, pochodzące z dotacji państwowych, z 1 proc. podatku, funduszy norwerskich, środków UE, a także ze zbiórek publicznych, ale nie są to ich prywatne pieniądze.

3. Decyzje w sprawach **kadrowych i finansowych** (zarówno te podejmowane kolegialnie, jak i jednoosobowo) mają charakter **arbitralny, uznaniowy i stronniczy**. W większości przypadków jedynym wymaganym uzasadnieniem jest stwierdzenie, że decyzja została podjęta na podstawie przepisów obowiązujacego prawa przez stosowny organ lub osobę w ramach przysługujących jej kompetencji – i takie merytoryczne wyjaśnienie jest całkowicie wystarczające. Jeśli przepisy prawa regulujące działanie konkretnej kategorii organizacji nakładają obowiązek przeprowadzenia szczególnych procedur, np. tzw. otwartego i konkurencyjnego postępowania, to zawsze można tak przygotować stosowne czynności oraz umówić się z członkami komisji, że dokonany wybór będzie zgodny z wcześniejszymi ustaleniami poczynionymi nieformalnie i z nakreślonym scenariuszem działań, jakie zostały już uzgodnione i zaakceptowane do realizacji w wąskim kręgu zaufanych, wtajemniczonych osób.
4. Korupcja w istotny sposób przyczynia się do umacniania władzy oraz poszerzania sfery wpływów przez tworzenie i rozbudowywanie sieci układów, powiązań i zależności personalnych, dlatego też polityka kadrowa odgrywa tak ważną rolę z punktu widzenia sprawnej, skutecznej, bezproblemowej i bezpiecznej realizacji partykularnych interesów.
5. Korupcja jest głównym czynnikiem scalającym więzi i relacje interpersonalne, jakie łączą osoby, które dzięki niej odnoszą spektakularne sukcesy, robią karierę, zyskują ponadprzeciętne korzyści majątkowe oraz osobiste.
6. W każdej organizacji (m.in. instytucji sektora finansów publicznych oraz sektora prywatnego) zawsze można uzasadnić potrzebę zatrudnienia danych osób, podpisania umowy zlecenia, nawiązania współpracy w innej formule prawnej, a także wydatkowania środków finansowych na wykonanie uzgodnionego przedsięwzięcia biznesowego potrzebnego do realizacji wytyczonego celu zgodnego z zakresem działalności. Następnie – podporządkować tej idei scenariusze działań, które tak naprawdę będą służyć legitimizowaniu – od strony formalno-prawnej – zasadności osiągania korzyści materialnych przez faworyzowaną grupę wybranych, uprzywilejowanych beneficjentów.
7. Uczciwość, sprawiedliwość, praworządność, równe traktowanie obywateli, konstytucyjna zasada równości obywatela wobec prawa: (...) *wszyscy są wobec prawa równi. Wszyscy mają prawo do równego traktowania przez władze*

publiczne (art. 32 § 1)[23], normy moralne, przyzwoitość i odpowiedzialność nie mają najmniejszego znaczenia z punktu widzenia działań korupcyjnych. Te wartości zostają zastąpione arogancją, interesownością, stronniczością, klientelizmem, dyskryminacją, poplecznictwem, kumoterstwem, które są podporządkowane jednej ideologii: dążeniu do maksymalizacji prywatnych korzyści i ochrony własnych interesów.

8. Z punktu widzenia zarządzania podstawowe znaczenie mają procesy przejmowania kontroli nad majątkiem oraz finansami danej organizacji, tzn. ulokowanie swoich zaufanych ludzi układu na najwyższych szczeblach kierowniczych związanych z szerokim zakresem uprawnień decyzyjnych. Analizując politykę personalną, nie można pola widzenia tego problemu zawężać tylko do apanaży i profitów, jakie są przypisane danej posadzie. O wiele cenniejsze jest bowiem to, jakim budżetem dysponuje dana jednostka i jakie w ramach prowadzonej działalności można wykreować przepływy **strumieni pieniężnych** do innych podmiotów czy firm. Chodzi zatem o **zdobycie władzy** w konkretnej organizacji, o **realny wpływ na korzyści majątkowe** osiągane przez inne instytucje i osoby. Równie ważne są **kontakty i powiązania** (polityczne, biznesowe, środowiskowe, zawodowe, rodzinne), jakie wyróżniają osobę piastującą daną funkcję, a także **kumulacja stanowisk**, zajmowane wcześniej posady oraz inne obszary jej aktywności. Te zagadnienia mają istotną wartość dla realizowanych czynności analitycznych, które umożliwiają poprawne zrozumienie badanych zdarzeń i procesów[24].

Usystematyzowanie terminologii odnoszącej sie do korupcji, króre zostało zaprezentowane na schemacie, jest ważne i potrzebne, gdyż, jak zaznacza Łukasz Goczek: (...) *korupcja jest jednym z najbardziej kontrowersyjnych tematów debaty publicznej, lecz jej mechanizm jest również jednym z najmniej zrozumiałych*[25].

[23] *Konstytucja Rzeczypospolitej Polskiej*…

[24] W. Walczak, *Działania analityczno-informacyjne identyfikujące mechanizmy korupcyjne w procesach zarządzania***,** „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16**,** s. 55–72.

[25] Ł. Goczek, *Przyczyny korupcji i skuteczność strategii antykorupcyjnych*, „Gospodarka Narodowa" 2007, nr 4, s. 33.

Schemat. Rozumienie pojęcia korupcji w praktyce zarządzania organizacjami.

Źródło: Opracowanie własne.

Do podstawowych czynników, które współtworzą płaszczyznę praktyk korupcyjnych zalicza się: obowiązujące **przepisy prawne, kumulowanie władzy** oraz **poczucie bezkarności** za podejmowane działania. Jerzy Matusiak prezentuje pogląd,

że źródłem korupcji jest prawo oraz (...) *walka z korupcją jest tylko pozorowana*[26]. Autor w uzupełnieniu swoich opinii dodaje: (...) *podstawą odpowiedzialności karnej są ustawy*. *Nie ma także przestępstwa bez ustawy: nullum crimen sine lege*[27]. A zatem, jeśli konkretny wzorzec postępowania lub dany czyn nie są wyraźnie doprecyzowane w kodeksie karnym, to nie można takim zachowaniom przypisywać znamion czynu zabronionego. Pełnienie wielu funkcji przez jedną osobę z punktu widzenia praktyki zarządzania odgrywa bardzo ważną rolę, prowadzi bowiem do kumulacji uprawnień decyzyjnych, a tym samym umożliwia bezpośredni wpływ na przebieg, ocenę i kontrolę określonych zdarzeń lub procesów w kilku organizacjach. Maciej Gurtowski twierdzi, że (...) *możliwości korupcyjne można powiązać z kontrolą źródeł niepewności*[28]. Jest to bardzo istotne, zwłaszcza w kontekście realnego oddziaływania na podejmowane rozstrzygnięcia określonych spraw. Im więcej funkcji pełni dana osoba, tym bardziej poszerza i umacnia zgromadzoną władzę, co w konsekwencji sprawia, że ma zwielokrotnione wpływy oraz możliwości załatwienia różnych spraw, interesów, formalności i postępowań. Z uwagi na to, że łączenie funkcji czy zajmowanych stanowisk najczęściej dotyczy kilku różnych instytucji (organizacji, firm itd.), powstaje wielowymiarowa i rozbudowana **sieć** kontaktów, znajomości, powiązań, zależności, które mają zarówno charakter formalny i służbowy (instytucjonalny, jawny), jak i nieformalny – prywatny (ukryty). To właśnie konfiguracja **powiązań, współzależności** oraz **skumulowanie władzy i wpływów** utworzone w tej formie stanowią największą siłę sprawczą, jeśli chodzi o rzeczywiste możliwości kształtowania korupcyjnych praktyk. Wypada tutaj nadmienić, że poczucie nietykalności oraz bezkarności[29] jest bardzo istotnym elementem, który rzeczywiście determinuje skuteczność i efektywność realizowanych przedsięwzięć.

Tak zwane główne mechanizmy korupcjogenne wymienione w schemacie absolutnie nie wyczerpują katalogu czynników sprzyjających korupcji, nie negują również znaczenia wcześniej omawianych elementów, jakie zostały wyszczególnione w rządowym programie antykorupcyjnym.

Podział praktyk korupcyjnych na dwie odrębne kategorie, jakimi są: legalna korupcja oraz przestępstwa korupcyjne, w oczywisty sposób jest pochodną zastosowanego kryterium, tj. karalności określonych czynów na gruncie prawa obowiązującego w Polsce. Niestety, niektóre powszechnie występujące praktyki korupcyjne ze względu na swoją złożoność oraz wieloznaczność mogą być interpretowane odmiennie, a także oceniane w zależności od tego, kto wyraża swoje sądy wartościujące i jaki punkt odniesienia przyjmuje. Istotnym, a zarazem newralgicznym, problemem jest

[26] J. Matusiak, *Peryferyjny kapitalizm zależny*, e-book, 2006, s. 123–124.

[27] Tamże, s. 124.

[28] M. Gurtowski, *Niepewność, korupcja i granice podmiotowości w medykalizującym się świecie z perspektywy teorii władzy Michela Croziera i Erharda Friedberga*, „Pogranicze. Polish Borderlands Studies" 2016, nr 2, s. 200.

[29] P. Falenta, *Przestępstwo korupcji – uwarunkowania karnoprawne i społeczne*, „Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu" 2016, nr 1, s. 157.

percepcja określonych zachowań, decyzji, zdarzeń i procesów oraz ich kwalifikacja prawna, czy jedynie wpływają one na nieprawidłowości[30], czy też można, a nawet czy powinno się, im przypisywać znamiona czynu zabronionego[31].

Anna Pluskota prezentuje interesujące przemyślenia na ten temat: (...) *wszędzie tam, gdzie jest mowa o korupcji wynikającej z przekroczenia uprawnień, interpretacja tego zachowania może być różna w zależności od kulturowych uwarunkowań społeczeństwa. Najczęściej to obywatele – za pomocą obowiązujących przepisów prawa – decydują, czy dana czynność jest uznawana za korupcję*[32]. Trudno zgodzić się z takim sposobem myślenia, że to obywatele mają uprawnienia do dokonywania wiążącej oceny prawnej danej czynności, jeśli jest nią korupcja związana z przekroczeniem uprawnień.

Waldemar Wojtasik uważa, że korupcja polityczna narusza podstawowowe zasady demokracji, wolnego rynku i społeczeństwa obywatelskiego. Jest powszechnie postrzegana w odbiorze społecznym jako (...) *patologia współczesnych relacji gospodarczych i politycznych*[33]. Czy to oznacza, że każdy przejaw korupcji politycznej może być interpretowany tylko w tej kategorii? Zdecydowanie nie. Społeczna percepcja danego zdarzenia może różnić się od klasyfikacji prawnokarnej dokonywanej przez służby lub prokuraturę (tj. organy ścigania), a także od ostatecznej, wiążącej interpretacji i oceny dokonywanej przez **skład orzekający** sądu. Tak więc rozstrzygające znaczenie w sprawie przypisania odpowiedzialności karnej za konkretne działania korupcyjne (postępowanie, procesy, decyzje) należą do wyłącznej właściwości władzy sądowniczej RP. Zdarza się, że powszechne w odczuciu społecznym skrajne nadużywanie władzy i nieuczciwe, wysoce szkodliwe praktyki są, niestety, traktowane przez organy ścigania jako formy nieetycznego postępowania, które są dozwolne prawem. Nie zmienia to jednak faktu, że każda odmiana korupcji[34] (legalnej i karalnej) jest rażącym **naruszeniem sprawiedliwości** społeczno-gospodarczej oraz poważnym zagrożeniem moralnych podstaw polskiego społeczeństwa[35], a przyzwolenie na niektóre czyny[36] nie może tego faktu podważyć i zakwestionować.

Granica między przestępczością korupcyjną a legalną korupcją staje się coraz bardziej nieostra i rozmyta. Karalne formy korupcji rozumiane ogólnie są kojarzone

---

[30] K. Dendura, *Korupcja jako patologia kapitału społecznego*, w: *Zarządzanie bezpieczeństwem w sektorze publicznym i biznesie*, T. Białas, M. Grzybowski, J. Tomaszewski (red.), Gdynia 2009, s. 31–38.

[31] K. Laskowska, *Rola korupcji w działalności zorganizowanych grup przestępczych*, w: *Oblicza współczesnej przestępczości zorganizowanej*, K. Laskowska (red.), Białystok 2014, s. 143–154.

[32] A. Pluskota, *Czy globalizacja wspiera korupcję?*, „Ekonomia Międzynarodowa" 2017, nr 17, s. 40.

[33] W. Wojtasik, *Społeczne postrzeganie korupcji politycznej w perspektywie oceny uczciwości władz politycznych*, „Political Preferences" 2017, nr 17, s. 120.

[34] A. Stachowicz-Stanuch, A. Sworowska, *Oblicza korupcji: formy i typy zachowań*, „Organizacja i Zarządzanie" 2012, nr 1, s. 117–133.

[35] K. Kietliński, *Korupcja jako naruszenie sprawiedliwości społeczno-gospodarczej oraz zagrożenie dla moralnych podstaw społeczeństwa*, „Problemy Zarządzania" 2010, nr 2, s. 139–147.

[36] P. Chodak, *Zgoda społeczeństwa na niewielkie przestępstwa korupcyjne*, „Journal of Modern Science" 2013, nr 3, s. 193–209.

z działaniami polegającymi na obiecywaniu, proponowaniu oraz przekazywaniu jakichkolwiek nienależnych korzyści. Marcin Brol stwierdza: (...) *im trudniejsze będzie wykrycie i udowodnienie faktu wręczenia lub przyjęcia łapówki, tym częściej dochodzić będzie do wymiany korupcyjnej*[37]. W raporcie Agencji Bezpieczeństwa Wewnętrznego z 2004 r. słusznie się podkreśla, że współczesne odmiany korupcji przybierają postać skrytych i zakamuflowanych działań. Zmianie ulega sposób i forma wręczania korzyści, (...) *coraz częściej ma ona wymiar niegotówkowy*[38]. Proceder korupcyjny bardzo często wiąże się ze sferą usług o charakterze niematerialnym (np. doradztwo prawne, doradztwo biznesowe, ekspertyzy), których wartość jest trudno jednoznacznie oszacować. Zdaniem ABW (...) *w wielu przypadkach astronomiczne wręcz honoraia, sięgające kilkudziesięciu tysięcy złotych, wypłacane za np. jednostronicową opinię prawną czy ekspertyzę (często fikcyjną lub o niskiej wartości merytorycznej) są niczym innym jak ukrytą formą łapówki*[39]. Dodatkowy problem polega na tym, że nie można mówić o nienależnym wynagradzaniu w konktekście przekazywania środków pieniężnych, jeśli istnieje podstawa prawna do ich wypłaty – podpisana umowa, zlecenie na wykonanie reklamy, zlecenie na marketing, sponsoring, public relations, a także takie decyzje, jak powołanie do rady nadzorczej, zarządu, powierzenie funkcji prokuretna, pełnomocnika zarządu itp.

Prawdziwa korupcja na wielką skalę polega na stworzeniu podstaw prawnych transferu profitów w legalnych operacjach gospodarczych i finansowych. Nie można wówczas postawić zarzutu, że beneficjent otrzymuje nienależne zyski. Co więcej, dystrybucja korzyści materialnych może być odroczona w czasie z uwagi na bezpieczeństwo i zachowanie pozorów, może również trafiać do wskazanego, zaufanego odbiorcy, pośrednika (bądź kilku), aby nie wzbudzać niczyich podejrzeń. Następnie zostają wykreowane kolejne interesy, zdarzenia gospodarcze i przepływy kapitałowe, nierzadko w udziałem innych osób i podmiotów (firm, fundacji, stowarzyszeń). Im bardziej jest złożona struktura tych procesów, tym trudniej jest się zorientować w rzeczywistych intencjach wykonawców określonych operacji finansowych, gdyż przybierają one formułę pozornie normalnych zdarzeń związanych z prowadzeniem działalności gospodarczej. Korupcja staje się obecnie synonimem przemyślanej długofalowej **strategii inwestycyjnej** – liczy się nie tylko to, co jest możliwe do osiągnięcia dziś, lecz także to, co będzie można zdobyć w przyszłości dzięki określonym działaniom.

Wszystkie czynności odbywają się w wąskim gronie wtajemniczonych, zaufanych osób, które doskonale wiedzą, w czym biorą udział i jaką rolę mają do ode-

[37] M. Brol, *Ekonomiczne i instytucjonalne metody przeciwdziałania korupcji*, „Współczesne Problemy Ekonomiczne" 2017, nr 2, s. 59.

[38] *Raport Agencji Bezpieczeństwa Wewnętrznego: Korupcja w Polsce – próba analizy zjawiska*, Warszawa 2004, s. 13; dostępny także na stronie: http://www.antykorupcja.gov.pl/download/4/5356/RaportAgencjiBezpieczenstwaWewnetrznegoKorupcjawPolsce-probaanalizyzjawiska.pdf.

[39] Tamże, s. 14.

grania, a także jakie wymierne korzyści dzięki temu zyskują. Nie ma mowy o tym, że ktoś żąda, oczekuje jakichś nienależnych gratyfikacji, gdyż odwzajemnianie się za przysługi jest niewymuszone i dobrowolne. Przy okazji można w legalny sposób wesprzeć daną partię polityczną, kampanię wyborczą danego polityka, przyjazne media, zaprzyjaźnione towarzystwo naukowe, prywatną uczelnię, instytucje kultury, wybraną organizację pozarządową (np. fundacje, think-tanki), bo przecież realizuje się cele społecznie użyteczne i nie powinno nikogo dziwić, jeśli ktoś chce być darczyńczą czy mecenasem określonego przedsięwzięcia.

Niestety, po przeczytaniu 31-stronicowej publikacji CBA pt. *Mapa korupcji. Zwalczanie przestępczości korupcyjnej w Polsce w 2016 r*. lub 33-stronicowego opracowania pt. *Informacja o wynikach działalności CBA w 2016 r*. nie zdobędzie się wyobrażenia o współczesnych formach i rzeczywistej skali korupcji w naszym kraju.[40] Można tutaj oczywiście znaleźć ogólnikowe informacje, np.: (...) *analizie poddano umowy na usługi doradcze, prawne, ubezpieczeniowe i w zakresie bezpieczeństwa zawierane przez wybrane spółki Skarbu Państwa w latach 2015–2016. Działania prowadzone są w ramach kontroli koordynowanej, a przedstawienie pełnych ustaleń i wyników możliwe będzie dopiero po ich zakończeniu*[41]. Minął rok 2016 oraz 2017 i do wiadomości publicznej nie podano żadnych informacji na temat wyników i ustaleń realizowanych czynności kontrolnych. Ta wiedza ma charakter niejawny i nie jest dostępna dla potencjalnie zainteresowanych obywateli.

Analogicznie jest z praktykami korupcyjnymi. Do społeczeństwa trafiają za pośrednictwem mediów jedynie fragmentaryczne informacje, które opisują ujawnione następstwa – skutki określonych działań, natomiast sednem mechanizmów korupcyjnych jest sekwencja procesów, które miały charakter pierwotny. Chcąc dogłębnie poznać i zrozumieć daną sprawę, trzeba uzyskać odpowiedzi na pytania: kto był pomysłodawcą przedsięwzięcia, kto pomagał, kto był zaangażowany, z kim współdziałał, jakie występowały zależności i powiązania interpersonalne oraz międzyorganizacyjne, kto wywierał bezpośredni wpływ na przebieg czynności i podejmowane decyzje, z czyjego upoważnienia działał, w czyim imieniu występował, na rzecz kogo pracował, kto zapewniał nietykalność itd. To jednak pozostaje domeną ekskluzywnej wiedzy ezoterycznej, której depozytariuszem jest hermetyczny krąg wtajemniczonych osób.

Dorota Karpiel twierdzi, że korupcja jest zjawiskiem powiązanym z przestępczością zorganizowaną. *Wspólny interes wszystkich zamieszanych w ten rodzaj przestępstw sprawia, że są one bardzo trudne do wykrycia i jeszcze trudniejsze do udowodnienia. Jest to prawda na tyle powszechna, utwierdzająca w przekonaniu o bezkarności, że ma niewątpliwy wpływ na rozszerzanie się stref bezpośredniego zagrożenia tym zjawiskiem*[42]. Podobny pogląd prezentuje ABW, według której okolicznością utrudniającą wykrywalność przestępstw korupcyjnych jest to, że osoby ma-

[40] *Informacja o wynikach działalności Centralnego Biura Antykorupcyjnego w 2016 r*., Warszawa 2017.

[41] Tamże, s. 4–5.

[42] D. Karpiel, *Przestępczość zorganizowana*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 7, s. 12.

jące związek z tym procederem nie są zainteresowane jego ujawnieniem. Najczęściej demaskowane przypadki dotyczące łapownictwa, przekupstwa, płatnej protekcji czy nadużycia władzy (...) *rzadko kiedy występują samodzielnie, w licznych przypadkach ujawnione są w związku ze sprawami o charakterze gospodarczym*[43]. Korupcja w praktyce zarządzania nie sprowadza się do incydentalnych przypadków i wyizolowanych zdarzeń, lecz przybiera złożoną formę **działań zorganizowanych w wymiarze systemowym**. To stanowi jej główny wyróżnik i najważniejszy atrybut. Polega na świadomym, zamierzonym **wykorzystywaniu legalnej władzy** oraz wpływów do tworzenia i rozbudowywania **sieci układów zamkniętych**, nakładających się na płaszczyznę przepływów strumieni finansowych na konta wybranych beneficjentów. Innymi słowy, chodzi o to, aby ważne, eksponowane stanowiska, dobra praca, intratne kontrakty, zlecenia, poważne biznesy, ścieżki kariery, możliwości awansu i rozwoju były zarezerwowane oraz dostępne **tylko** i wyłącznie **dla swoich z układu**, **mających odpowiednie koneksje, powiązania, znajomości**, dzięki czemu zajmują uprzywilejowaną pozycję.

Elżbieta Durys uważa, że układy, znajomości, haki, stanowią odzwierciedlenie (…) *paranoi spiskowej w polskim kinie współczesnym*[44]. Autorka ma pełne prawo do formułowania autonomicznych poglądów i sądów wartościujących, a także prowadzenia badań naukowych w wybranym obszarze tematycznym i ogłaszania ich wyników. Wolność prowadzenia badań naukowych jest prawem gwarantowanym przez Konstytucję RP[45]. Biorąc pod uwagę powyższe przesłanki, warto się zastanowić, czy układ to tylko wymyślony abstrakcyjny byt, jaki jest zauważany przez wyznawców teorii spiskowych. Zadaniem E. Durys jest on przedstawiany w filmach następująco: *„Oni" tworzą grupę dbającą wzajemnie o swoje interesy*. (...) *Bezkarność zapewniają im znajomości i powiązania*[46].

Po przeanalizowaniu publicznej wypowiedzi przedstawiciela władzy sądowniczej można w niej odnaleźć fragment na temat zmian kadrowych: (...) *po prostu nie pasuję do* ***nowego układu****, który właśnie się tworzy*[47]. Jest to bardzo wartościowe poznawczo i merytorycznie cenne zdanie przydatne do celów naukowo-badawczych związanych z tematem pracy. Po pierwsze omawiana wypowiedź jest przemyślana, prawdziwa i autentyczna. Jest ważnym argumentem potwierdzającym **istnienie**

[43] *Korupcja w Polsce – próba analizy zjawiska*…, s. 13.

[44] E. Durys, *Układy, znajomości, „haki". Paranoja spiskowa w polskim kinie współczesnym*, „Studia Etnologiczne i Antropologiczne", t. 16, M. Rauszer, G. Studnicki (red.), Katowice 2016, s. 44–54.

[45] W myśl art. 73 Konstytucji RP takie prawo przysługuje każdemu obywatelowi: „Każdemu zapewnia się wolność twórczości artystycznej, badań naukowych oraz ogłaszania ich wyników, wolność nauczania, a także wolność korzystania z dóbr kultury". Zgodnie z art. 54 § 1 Konstytucji RP „Każdemu zapewnia się wolność wyrażania swoich poglądów oraz pozyskiwania i rozpowszechniania informacji".

[46] E. Durys, *Układy, znajomości, „haki"*..., s. 50.

[47] Zob. *Odwołany prezes łódzkiego sądu nie pasuje do nowego układu*, https://www.tvn24.pl/lodz,69/odwolany-prezes-lodzkiego-sadu-nie-pasuje-do-nowego-ukladu,807449.html [dostęp: 7 II 2018].

układu w wymiarze sprawiedliwości, a ponadto wskazuje na aktualnie zachodzące przeobrażenia jego struktury. W logiczny sposób można ją odczytać następująco: wytworzony układ podlega pewnej modyfikacji i stąd też następują zmiany personalne. Jest to racjonalne i rzeczowe uzasadnienie, a także poprawne używanie słowa „układ" jako pojęcia opisującego sposób funkcjonowania zorganizowanej grupy.

Po drugie ta informacja nie została podana do wiadomości publicznej przypadkowo, lecz była celowa. Nie pochodzi z nielegalnego podsłuchu, nie ma również charakteru prywatnego. Należy przyznać, że trafnie odwzorowuje opisywaną rzeczywistość organizacyjną. Po trzecie analiza cytowanych treści w żadnej mierze nie odnosi się do oceny zasadności kadrowych procesów decyzyjnych w sądownictwie, lecz ma na celu pozytywną weryfikację tezy o istnieniu układu, co było przedmiotem prowadzonych rozważań.

Obszary występowania, przejawy i formy zachowań korupcyjnych

Chcąc poprawnie i właściwie zidentyfikować współczesne odmiany korupcji mającej swoje realne potwierdzenie w codziennej rzeczywistości organizacyjnej, trzeba pamiętać, że są one ściśle powiązane z następującymi elementami: sprawowanie władzy (zdobywanie, utrzymywanie, umacnianie, poszerzanie wpływów), stosowane metody zarządzania, styl kierowania, podejmowane decyzje, korzyści osobiste i majątkowe możliwe do osiągnięcia.

Maciej Ciesielski bardzo słusznie zauważa, że (…) *w nowoczesnych formach korupcji chodzi o realizację scenariuszy działań opartych na złożonych zależnościach personalnych, które nie są równoznaczne z działalnością przestępczą opisaną w art. 228–230 Kodeksu karnego*[48]. Dodaje też, że coraz bardziej powszechnymi formami korupcji jest nepotyzm i klientelizm, a także (…) *relacje (powiązania), które przeważnie mają charakter nieformalny, zakulisowy oraz ogniskują się wokół wpływu, którego efektem jest realizacja partykularnych celów (osobistych, biznesowych)*[49]. Przytoczone spostrzeżenia są niezwykle celne oraz ze wszech miar poprawne, aczkolwiek z jednym drobnym zastrzeżeniem o charakterze semantycznym – owe relacje i powiązania są tworzone nie „wokół wpływu", lecz konkretnych osób mających wpływy, władzę i kompetencje decyzyjne.

Jerzy Matusiak prezentuje opinie, które rozwijają poruszany wątek: *Nepotyzm, klientelizm i kolesiostwo zagospodarowują wszelkie ciepłe posadki, a nawet ministerialne stołki. Za wszystkie synekury płaci społeczeństwo. Niejawnie podporządkowują interes państwa interesom prywatnym. W Polsce kapitalizm polityczny jest realnie usankcjonowaną treścią rządzenia*[50]. Trudno nie zgodzić się z tymi poglądami,

[48] M. Cielsielski, *Zjawiska korupcyjne jako podstawowa kategoria zagrożeń bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP – perspektywa Służby Kontrwywiadu Wojskowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 214.

[49] Tamże, s. 213.

[50] J. Matusiak, *Peryferyjny kapitalizm zależny*…, s. 123.

w syntetycznej formule bowiem odzwierciedlają charakterystykę metod i procesów zarządzania powszechnie występujących w rzeczywistości organizacyjnej. Zastanawiając się nad konsekwencjami takich wzorców zachowań, należy przyjąć za zasadne i prawdziwe twierdzenie, że (…) *korupcja podważa zaufanie do prawa i władz państwowych*, *a ponadto narusza poczucie bezpieczeństwa obywateli, dewastuje podstawowe zasady moralne, niszczy uczciwość i odpowiedzialność*[51]. Co więcej, stanowi poważne zagrożenie z punktu widzenia ochrony interesów ekonomicznych państwa, gdyż (…) *straty powodowane przez korupcję tylko w obrocie gospodarczym wielokrotnie przekraczają straty wywołane przestępczością pospolitą*[52].

Dirk Tanzler zaznacza, że (…) *korupcja nie zdarza się w próżni, lecz na styku administracji sektora publicznego z przedsiębiorstwami gospodarki prywatnej, i to wszędzie tam, gdzie są przyznawane środki publiczne*[53]. Zacytowane poglądy wymagają kilku zdań komentarza, aby poprawnie identyfikować możliwe obszary występowania korupcyjnych praktyk. Po pierwsze nie można zawężać pola widzenia jedynie do wybranej kategorii instytucji finansowanych z pieniędzy podatników, określanych mianem tzw. administracji, gdyż do sektora finansów publicznych zalicza się również: organy kontroli państwowej i ochrony prawa, sądy, trybunały, agencje wykonawcze, instytucje gospodarki budżetowej, ZUS, KRUS, NFZ, samodzielne publiczne zakłady opieki zdrowotnej, uczelnie publiczne, PAN i tworzone przez nią jednostki organizacyjne, państwowe, samorządowe instytucje kultury (art. 9 ustawy o finansach publicznych[54]). Po drugie w obrocie gospodarczym występują również inne podmioty, m.in.: spółki z udziałem Skarbu Państwa i utworzone podmioty zależne, spółki z udziałem kapitałowym jednostek samorządu terytorialnego, spółdzielnie mieszkaniowe, SKOK-i, związki sportowe, fundacje, stowarzyszenia, prywatne instytucje finansowe, koncerny medialne, spółki giełdowe czy kancelarie prawne, które zawierają rozliczne transakcje handlowe z organizacjami sektora publicznego i prywatnego.

Praktyki korupcyjne mogą ukształtować się we wszystkich kategoriach organizacji, jakie funkcjonują w gospodarce[55], chociaż są inaczej postrzegane oraz interpretowane w zależności od tego, czy występują w instytucjach pozostających pod

[51] Tamże, s. 117.

[52] Tamże.

[53] D. Tanzler, *Korupcja jako metafora*, „Roczniki Nauk Społecznych" 2012, nr 4, s. 78.

[54] *Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych* (Dz.U. z 2009 r. nr 157 poz. 1240, ze zm.).

[55] J. Burzyński, T. Burzyński, *Ryzyko zachowań korupcyjnych w instytucjach państwowych na przykładzie Służby Celnej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2013, nr 2, s. 217–229; A.E. Chodorowska, J.M. Stopińska, *Korupcja w ochronie zdrowia*, „Journal of Modern Science" 2012, nr 4, s. 163–181; K. Nowakowski, *Zagrożenia etyczne i korupcyjne w mediach*, „Studia Medioznawcze" 2017, nr 2, s. 128–140; J. Potulski, *Penalizacja korupcji w sporcie – uwagi krytyczne*, „Prokuratura i Prawo" 2012, nr 3, s. 67–78; P. Szwajdler, *The legal aspects of corruption in sport*, „Journal of Education, Health and Sport" 2016, nr 5, s. 445–451; *Postawy wobec korupcji w samorządzie terytorialnym. Raport z badań w województwie śląskim*, A. Turska-Kawa, M. Czaja (red. nauk.), Katowice 2015; L. Wilk, *Korupcja w reklamie farmaceutycznej*, „Prokuratura i Prawo" 2011, nr 10, s. 21–36.

kontrolą państwa, czy w podmiotach prywatnych[56]. Nie można jednak powiedzieć, że szeroko rozumiana korupcja ma miejsce tylko w sektorze państwowym[57], choć niewątpliwie najczęściej wykrywane przez służby i karalne formy korupcji dotyczą opisywanych sytuacji.

Inna ważna kwestia, o której koniecznie warto wspomnieć, dotyczy przekazywania publicznych pieniędzy do konkretnego podmiotu prywatnego z tytułu zawartej umowy (np. wygranego przetargu, podpisanego lukratywnego, wielomilionowego kontraktu, otrzymanego intratnego zlecenia). Te pieniądze najczęściej podlegają dalszej redystrybucji przez władze danej firmy, a tym samym trafiają do ściśle określonych organizacji, kontrahentów, dostawców, podwykonawców, zleceniobiorców, współpracowników itd. W odniesieniu do tych przepływów finansowych absolutnie nie można uznać, że są to procesy i decyzje dotyczące wydatkowania środków publicznych. Analogicznie nie jest prawdziwe twierdzenie, że fundacja utworzona przez spółki z udziałem Skarbu Państwa, których władze podjęły decyzje o przeznaczeniu określonych kwot na działalność danej organizacji, staje się dysponentem środków publicznych i zawierając umowy handlowe z osobami trzecimi, wydaje pieniądze podatnika. Dlatego też powinno się przyjmować kompleksowe spojrzenie przy rozpatrywaniu danej sprawy, nie ograniczając się do zauważania wyizolowanych pojedynczych zdarzeń gospodarczych, ponieważ równie ważna jest sekwencja procesów i występujące między nimi powiązania, zależności, a także uwarunkowania organizacyjno-prawne. W celu uzupełnienia tych refleksji można jedynie dodać, że spółki z udziałem Skarbu Państwa nie zaliczają się do organizacji sektora finansów publicznych, a firmy (podmioty) prywatne nie są zobligowane do stosowania ustawy *Prawo zamówień publicznych*[58] i mogą dowolnie rozporządzać posiadanym majątkiem, a ich władze nie muszą się tłumaczyć przed opinią publiczną ze swoich decyzji płatniczych ani ich uzasadniać.

Piotr Borowiec, który analizuje wybrane obszary wielkiej korupcji w III RP, wskazuje na prywatyzację majątku państwowego, procesy ustawodawcze, działalność mediów, zamówienia publiczne oraz korupcję w procesie zatrudniania. Dodaje, że takie praktyki są stosowane (…) *we wszelkich procedurach związanych z pozyskaniem pracy lub zmianą zajmowanych stanowisk i co należy podkreślić nie dotyczy to tylko etatów w sferze budżetowej oraz dobrze płatnych stanowisk*[59]. Zwraca także uwagę na procesy zawłaszczania instytucji publicznych: (…) *dostęp został ściśle ograniczony dla „wybranych" – niekoniecznie kompetentnych i uczciwych ludzi*[60]. Wnikliwa analiza konkretnych zdarzeń i procesów występujących w gospodarce nakazuje potwier-

[56] A. Golonka, *Korupcja gospodarcza jako przestępstwo przeciwko zasadom uczciwej konkurencji*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2013, z. 3, s. 51–69.

[57] J. Bojarski, *Korupcja gospodarcza. Studium z dziedziny polityki kryminalnej*, Toruń 2015.

[58] *Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych* (t.j.: Dz.U. z 2017 r. poz. 1579, ze zm.).

[59] P. Borowiec, *Korupcja w III RP – obszary szczególnego występowania*, „Środkowoeuropejskie Studia Polityczne" 2007, nr 1, s. 196.

[60] Tamże, s. 201.

dzić, że jest to pragmatyczne i właściwe rozumowanie. Równie zasadne jest sformułowanie, że korupcja (…) *zdecydowanie podważa zasadę równości obywateli wobec prawa oraz równego dostępu do instytucji publicznych*[61], a nagminnie uprawiany proceder korupcyjny jest (…) *największym zagrożeniem dla państwowości*[62]. Racjonalny jest również punkt widzenia: (…) *gdzie duże pieniądze, tam i ryzyko wystąpienia zachowań korupcyjnych, a im większa ich ilość, tym ryzyko wyższe*[63]. Piotr Solarz dodaje: (…) *korupcja będzie występowała, kiedy monopolistyczna decyzja w zakresie dobra jest podejmowana w sposób dyskrecjonalny, bez ponoszenia ryzyka osobistej odpowiedzialności za rezultaty danego wyboru. Korupcja = monopol + dyskrecja – odpowiedzialność*[64].

Do obszarów funkcjonalnych w zarządzaniu organizacjami, gdzie zazwyczaj występują działania korupcyjne, zalicza się:

- procesy dotyczące zatrudniania, tj. załatwianie pracy w instytucjach sektora finansów publicznych, powierzanie funkcji w radach nadzorczych i zarządach spółek z udziałem państwowych osób prawnych oraz mianowanie na eksponowane stanowiska kierownicze w tych podmiotach. Tożsame zjawiska występują w pozostałych organizacjach sektora prywatnego, lecz tam nie są odbierane jako patologie, lecz przejaw przedsiębiorczości rodzinnej i środowiskowej;
- procesy dotyczące zawierania umów z firmami zewnętrznymi, intratne zlecenia, kontrakty;
- przyznawanie dotacji ze środków publicznych, udzielanie koncesji i zezwoleń;
- przetargi i zamówienia publiczne;
- procesy związane z reprywatyzacją;
- wystawianie fikcyjnych faktur opisujących zdarzenia gospodarcze, które nie mają swojego odzwierciedlenia w rzeczywistości, wyłudzenia podatku VAT.

Polityka kadrowa jako istotny komponent zachowań korupcyjnych

Jak wcześniej wspominano, praktyki korupcyjne istnieją w każdym obszarze życia społeczno-gospodarczego i przybierają różną postać oraz skalę we wszystkich instytucjach sektora finansów publicznych, spółkach z udziałem państwowych osób prawnych, a także w pozostałych firmach i organizacjach sektora prywatnego. Przepisy prawa wyznaczające ramy funkcjnowania określonej kategorii organizji w zasadniczej mierze kształtują określone zachowania, a także wpływają na ich odmienną ocenę nie tylko od strony prawnokarnej, lecz także w kontekście społecznego nastawienia.

[61] Tamże, s. 191.

[62] M. Romański, *Znaczenie zjawiska korupcji dla bezpieczeństwa państw upadłych*, „Roczniki Ekonomii i Zarządzania" 2017, nr 1, s. 25.

[63] M. Chruściel, *Wojsko jako podatny grunt dla korupcji*, w: *Realizacja działań antykorupcyjnych w resorcie obrony narodowej*, R. Wykurz (red.), Warszawa 2017, s. 7.

[64] P. Solarz, *Korupcja, klientelizm i kapitalizm polityczny jako podstawowe pojęcia w dyskursie o jawności życia publicznego w Polsce*, „Kontrola Państwowa" 2007, nr 3, s. 118.

Powszechne jest odczucie, że w prywatnym biznesie takie zjawiska, jak nepotyzm, kumoterstwo, poplecznictwo i kolesiostwo są traktowane jako pożądany przejaw zaradności i operatywności i są odbierane pozytywnie.

Polityka kadrowa w szeroko rozmianych instytucjach pozostających pod kontrolą państwa jest jednym z tych zagadnień, które wzbudza duże zainteresowanie mediów, a także wywołuje liczne kontrowersje ze względu na wieloznaczność ocen tego zjawiska. Powszechną akceptację zyskują poglądy, że o nominacjach, awansach na eksponowane stanowiska w wielu przypadkach wcale nie przesądzają ponadprzeciętne kompetencje oraz rozległa, ugruntowana, wszechstronna wiedza, lecz takie czynniki, jak: układy, powiązania i znajomości z wpływowymi osobami, tj. ludźmi władzy, które są rozstrzygające. Co więcej, bardzo ważna jest **dostępność do intratnych i wysokopłatnych stanowisk** oraz funkcji dla polskich obywateli. W tej sprawie najważniejszą rolę odgrywają obowiązujące przepisy, które określają procedury formalno-prawne związane z obsadą personalną miejsc pracy w danej kategorii organizacji. Przykładem są procedury doboru członków do rad nadzorczych i zarządów spółek Skarbu Państwa czy do jednostek samorządu terytorialnego, które absolotnie nie wymagają otwartego i konkurencyjnego trybu konkursowego. Zastosowanie takiego trybu stwarzałoby przynajmniej iluzoryczne wrażenie, że zainteresowane osoby mające stosowne kompetencje i kwalifikacje mogą ubiegać się o takie posady. Analogicznie jest w przypadku stanowisk kierowniczych i pozostałych miejsc pracy w państwowych spółkach, a także w administracji rządowej i samorządowej, na które są mianowane osoby w trybie powołania na stanowisko. Wystarczającym uzasadnieniem podejmowanych decyzji kadrowych jest podanie podstawy prawnej i stwierdzenie, że zostały one podjęte przez właściwy (upoważniony) organ lub osobę, na podstawie obowiązujących przepisów prawa.

Takie postępowanie kadrowe może spowodować pojawienie się różnych opinii oraz interpretacji. Skoro wszystko odbywa się zgodnie z obowiązującym prawem, to w żadanym wypadku nie wolno kwestionować poczynań władzy co do kreowanej polityki personalnej. Tym bardziej nieuprawnione jest doszukiwanie się w tych procesach zachowań korupcyjnych, gdyż będzie to godzić w dobre imię, podważać uczciwość, wiarygodność i autorytet władzy, a także zaufanie obywateli do państwa i jego organów. Można jednak przyjąć nieco inną, poszerzoną i wielowymiarową perspektyw analitycznego myślenia, odwołującą się do tzw. **zasady dostępności** do służby publicznej, która wynika wprost w przepisów art. 60 Konstytucji RP: *Obywatele polscy korzystający z pełni praw publicznych mają prawo dostępu do służby publicznej* ***na jednakowych zasadach***[65].

Ustawa o zmianie ustawy o służbie cywilnej[66] uchwalona z końcem 2015 r. wprowadziła istotne zmiany w postępowaniu kadrowym, m.in. rezygnację z tzw. otwartego i konkurencyjnego trybu przy obsadzie wyższych stanowisk kierowniczych

[65] *Konstytucja Rzeczypospolitej Polskiej*…

[66] Przebieg procesu legislacyjnego zob. http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=119 [dostęp: 7 II 2018].

i w zakresie wymagań kwalifikacyjnych, jakie kandydaci muszą spełniać[67]. W debacie publicznej pojawiały się wówczas logicznie uzasadnione argumenty, że likwidacja konkursów na wyższe stanowiska w służbie cywilnej jest zasadna, gdyż i tak wszystkie te ogłoszenia były zwykłą fikcją. Zawsze wygrywał ten, kto miał zostać wybrany, a więc nie ma co udawać, że były to uczciwe i konkurencyjne postępowania. Słuszne były także inne opinie, m.in. że modyfikacje przepisów mają umożliwić szybką wymianę kadr. Oczywiście w oficjalnym uzasadnieniu projektu wskazano ogólnie, że (…) *zmiany proponowane w odniesieniu do obsadzania wyższych stanowisk są konsekwencją dotychczasowej praktyki, która ujawniła nieefektywność procedur i ich przewlekłość*[68], a w opinii Biura Analiz Sejmowych z 12 stycznia 2016 r. na temat dokonanych zmian na próżno szukać jakiejkolwiek wzmianki bądź uwag w nawiązaniu do art. 60 Konstytucji RP. To wszystko dowodzi, jak iluzoryczne i fasadowe znaczenie mają przepisy Konstytucji, które teoretycznie stanowią zbiór zasad praworządności – fundament demokratycznego państwa prawa.

Bez problemu można wskazać inne przykłady atrakcyjnych synekur państwowych, które są zajmowane w wyniku arbitralnych i uznaniowych decyzji realizowanych w formule prawnej powołania na intratne stanowisko. Oznacza to, że wszystkie procesy decyzyjne związane z obsadą tych miejsc pracy mogą być oceniane i interpretowane pod kątem zachowań etyczno-moralnych, natomiast z prawnego punktu widzenia nie można ich kwestionować. Podawane do publicznej wiadomości informacje na temat określonych nominacji opisują wyłącznie efekt finalny innych zakulisowych czynności i działań (rekomendacji, poparcia) ze strony określonych osób, wywierających bezpośredni lub pośredni wpływ na przebieg tych zdarzeń. Wiedza na temat opisanych procesów nie jest przeznaczona dla opinii publicznej i ma **charakter niejawny**. Konstytutywną cechą omawianych procesów kadrowych jest ich skuteczność i sprawność rozumiana w ten sposób, że za każdym razem uprzednio poczynione nieformalne ustalenia (w wąskim kręgu **wpływowych** osób) są następnie bez przeszkód realizowane zgodnie z nakreślonym scenariuszem działań.

Dokładnie tak samo jest w przypadku **legalnych praktyk korupcyjnych** dotyczących spraw kadrowych – ich skutki są jawne, natomiast **utajniony pozostaje przebieg zdarzeń** poprzedzających określoną czynność prawną, która ma swoją legitymizację w obowiązujących przepisach. Ten mechanizm postępowania w ramach benchmarkingu jest powielany w pozostałych procesach rekrutacyjnych jako wzorzec skuteczności tam, gdzie przepisy prawa obligują daną instytucję do publikowania ogłoszeń o wakacie. Najpierw w wąskim gronie wpływowych osób zapada wstępna decyzja o potrzebie zatrudnienia konkretnego kandydata, a następnie realizacji tego zadania zostają podporządkowane kolejne czynności dotyczące tzw. otwartego

[67] *Ustawa z dnia 30 grudnia 2015 r. o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw* (Dz.U. z 2016 r. poz. 34).

[68] M. Gintowt-Jankowicz, *Opinia prawna o projekcie ustawy o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw,* druk sejmowy nr 119 z 15 grudnia 2015 r., Warszawa 2015, http://orka.sejm.gov.pl/rexdomk8.nsf/Opdodr?OpenPage&nr=119 [dostęp: 7 II 2018].

i konkurencyjnego postępowania. Przygotowuje się stosowne kryteria i wymagania formalne, które musi spełniać poszukiwany pracownik. Bez większego trudu można w taki określić warunki formalne dotyczące szczegółowego wykształcenia kierunkowego, ukończenia studiów podyplomowych, specjalistycznych kursów, szkoleń oraz niezbędnego doświadczenia zawodowego na odpowiednich stanowiskach, aby skutecznie ograniczyć liczbę potencjalnych rywali i już na wstępnym etapie z góry **faworyzować** wskazaną osobę. Innymi słowy, ogłoszenie o naborze można tak ustawić, aby wymagania formalne spełniła tylko jedna, konkretna osoba. W praktyce jest stosowana jeszcze druga, bardziej wyrafinowana i subtelniejsza metoda uwiarygodnienia otwartości i rzetelności postępowania kadrowego oraz konkurencyjności dokonanego wyboru. Wówczas mniej precyzyjnie formułuje się wymagania, aby mogli pojawić się inni kontrkandydaci. W takim przypadku nie można powiedzieć, że inni nie mieli szansy. Wygrywa oczywiście beneficjent, który był z góry ustalony, niemniej jednak można stwierdzić, że spośród wszystkich kandydatów zwycięzca został oceniony przez „niezależną" komisję ds. naboru najwyżej.

Wobec powyższego można się zastanowić, z jakiej perspektywy należy oceniać **proceder ustawiania konkursów** i wpływania na ich przebieg oraz jak takie zachowania mogą być interpretowane od strony prawnej. Jest to niezwykle istotne, w zależności bowiem od przyjętych kryteriów i toku rozumowania będzie można wysnuć odmienne wnioski i opinie.

Osoba występująca w imieniu pracodawcy będzie argumentowała swój wybór tym, że zgodnie z uprawnieniami ma prawo do podejmowania autonomicznych decyzji kadrowych dotyczących doboru personelu. Może również szczegółowo profilować formalne wymagania, które – w jej ocenie – są niezbędne na danym stanowisku pracy, aby zapewnić najwyższy poziom realizacji zadań. To, że tylko jeden kandydat spełnił kryteria formalne podane w ogłoszeniu, może jedynie cieszyć, gdyż udało się pozyskać osobę o pożądanych kwalifikacjach i z oczekiwanym doświadczeniem. Wszystkie procedury odbyły się zgodnie z obowiązującym prawem, tak więc całkowicie bezpodstawne i nieuprawnione jest stawianie jakichkolwiek zarzutów w tej sprawie.

Trzeba jednak bezsprzecznie uznać, że **ustawianie kryteriów formalnych pod konkretnego kandydata** jest czynnością, która wywiera bezpośredni wpływ na przebieg postępowania konkursowego, a w wyniku tych działań dany beneficjent uzyskuje wymierne korzyści osobiste i materialne. Wskazana osoba jest traktowana w sposób szczególny i ma zagwarantowaną dominującą pozycję w stosunku do innych kandydatów poszukujących pracy. Zważywszy na to, że do takich przypadków dochodzi w jednostce sektora finansów publicznych, która na mocy stosownej ustawy jest zobligowana do przeprowadzania otwartych i konkurencyjnych postępowań rekrutacyjnych, opisywane działania całkowicie podważają otwartość i **rażąco przeczą** autentyczności postępowania. W tym miejscu pojawiają się kolejne dylematy, czy takie zachowania kwalifikować tylko jako uchybienia bądź nieprawidłowości, czy też świadome, celowe, zamierzone **nadużycie władzy i działanie na szkodę interesu publicznego**?

Po przeanalizowaniu ogólnie dostępnych komunikatów podawanych przez CBA na stronie internetowej tej służby można znaleźć tylko jedną informację mającą związek z ogłoszeniem o pracę: (…) *zatrzymane osoby wykorzystując zajmowane funkcje, wpływały na przebieg i rozstrzygnięcia postępowań konkursowych dotyczących naboru na stanowiska urzędnicze, czyli ukierunkowywali nabór tak, aby zatrudnienia otrzymywały z góry ustalone osoby*[69]. Niestety, te doniesienia medialne nie zawierają żadnych komunikatów o kwalifikacji prawnej czynu będącego podstawą zatrzymania, tak więc nie można szerzej się do nich odnieść. Chociaż CBA nie ujawniło więcej tego typu przypadków, absolutnie nie można na tej podstawie wnioskować, że ustawianie konkursów ma charakter incydentalny i że natrafiono na odosobniony proceder, który ujawnił się tylko w jednej gminie. W rzeczywistości jest zupełnie inaczej, przeważająca liczba naborów na wolne miejsca pracy wygląda bowiem dokładnie tak samo – rozstrzygnięcie jest znane przed opublikowaniem ogłoszenia. Wszystkie osoby zaangażowane w realizację przygotowanego scenariusza działań oraz mające realny wpływ na przebieg wydarzeń doskonale o tym wiedzą i się na to godzą.

Przykładem może być inny medialnie nagłośniony i opisywany przypadek dotyczący wpływania na przebieg postępowań konkursowych w Najwyższej Izbie Kontroli. W tej sprawie, zdaniem prokuratury, doszło do przestępstwa nadużycia władzy z art. 231 §1 kk, a zachowania zostały ocenione jako czyny charakteryzujące się (…) *wysokim stopniem społecznej szkodliwości. Spowodowały one rzeczywistą szkodę w interesie publicznym i prywatnym*[70]. Przedstawiona interpretacja analizowanego zdarzenia pod kątem wykorzystywania władzy i wpływów ściśle koresponduje z wcześniejszymi refleksjami na temat organizacji konkursów, które zostały sformułowane z uwzględnieniem zasad prawidłowego rozumowania, oraz wskazań wiedzy i doświadczenia życiowego. Nie jest to jednak ostateczna i wiążąca ocena rozpatrywanego zagadnienia, gdyż o tym dopiero rozstrzygnie sąd, a ściślej rzecz ujmując – wyznaczony skład sędziowski.

Zupełnie inaczej wyglądają procesy rekrutacyjne w spółkach państwowych oraz innych podmiotach, w których przepisy prawa nie nakładają obowiązku przeprowadzania otwartych postępowań konkursowych na eksponowane, kierownicze stanowiska oraz na pozostałe miejsca pracy. Na podstawie badań i analiz dokumentów oraz informacji jawnoźródłowych można dostrzec powszechnie występujące, powtarzające się praktyki i okoliczności zawłaszczania sektora publicznego. Dzięki arbitralnym i uznaniowym decyzjom intratne posady: prezesa, dyrektora, kierownika, specjalisty otrzymuje **tylko i wyłącznie** wybrana kategoria beneficjentów. Dotyczy to akurat tych instytucji, w których władzę sprawują aktualnie ich partyjni koledzy. Są to najczęściej:

[69] Zob. komunikat CBA z 2 XII 2016 r. w sprawie postępowań konkursowych na stanowiska w urzędzie gminy, https://cba.gov.pl/pl/aktualnosci/3610,Zatrzymani-wojt-sekretarz-i-kontroler-NIK.html [dostęp: 3 II 2018].

[70] Zob. *Prezes NIK z zarzutami. Zdaniem prokuratury doszło do przestępstwa nadużycia władzy przy obsadzaniu stanowisk w Izbie*, wPolityce/pl z 8 września 2017 r., https://wpolityce.pl/kryminal/356851-prezes-nik-z-zarzutami-zdaniem-prokuratury-doszlo-do-przestepstwa-naduzycia-wladzy-przy-obsadzaniu-stanowisk-w-izbie [dostęp: 3 II 2018].

radni, działacze partyjni, byli politycy, członkowie ich rodzin, osoby z nimi powiązane, współpracujące oraz ich znajomi. Co więcej, zjawiskiem powszechnie występującym jest wielofunkcyjność i łączenie stanowisk w zarządach spółek oraz dyrektorskich posad w administracji rządowej lub samorządowej z funkcjami w radach nadzorczych.

Rozpoznane mechanizmy, wzorce postępowania, a przede wszystkim cele przyświecające opisywanym działaniom kadrowym, mają swoją kontynuację w innych obszarach funkcjonalnych. Uprawnienia decyzyjne są wykorzystywane przede wszystkim przy zawieraniu umów ze wskazanymi podmiotami zewnętrznymi oraz przygotowywaniu i realizowaniu czynności związanych z organizacją przetargów i zamówień publicznych. Ale czy ktoś się do tego przyzna? Oczywiście, że nie, bo (…) *sprawowaniu władzy zawsze towarzyszy dyskrecjonalność*[71] i ochrona wiedzy na temat interesów oraz kombinacji.

Zakończenie

Zaprezentowane rozważania oraz przeprowadzone analizy upoważniają do sformułowania wniosku, że szeroko rozumiana korupcja godzi w funkcjonowanie – uczciwe oraz zgodne z zasadami praworządności i sprawiedliwości społecznej – państwa polskiego. Jednym z głównych celów tego artykułu jest usystematyzowanie wiedzy na temat istoty badanego zjawiska, a także uwarunkowań wyznaczających przestrzeń, w której mogą zaistnieć określone praktyki. Takie podejście umożliwia dogłębne poznanie i zrozumienie charakteru określonych zdarzeń i decyzji podejmowanych w procesie zarządzania. Ponadto prowadzi do poszerzenia horyzontów myślowych i właściwej percepcji wzorców zachowań, jakie powszechnie występują w rzeczywistości organizacyjnej. W literaturze przedmiotu dominuje pogląd, że jednoznaczne i precyzyjne zdefiniowanie zjawiska korupcji wraz ze wszystkimi jej cechami i mechanizmami jest zadaniem trudnym[72]. Dlatego też należy najpierw rzetelnie scharakteryzować dane pojęcie, a dopiero w dalszej kolejności wyrażać na konkretny temat merytoryczne oceny, logicznie uzasadnione opinie i sądy wartościujące.

Andzej Cieślik i Łukasz Goczek zwracają uwagę na to, że wraz z przeobrażeniami zachodzącymi we współczesnej gospodarce zmieniają się formy zachowań korupcyjnych[73]. Na podstawie prowadzonych obserwacji i analiz można dojść do wniosku, że najbardziej rozpowszechnione praktyki dotyczą tzw. **legalnych działań korupcyjnych**, które zajmują pozycję dominującą. Nie oznacza to jednak, że są one mniej szkodliwe społecznie i nie stanowią poważnego zagrożenia interesów ekonomicznych państwa. Jest wręcz przeciwnie. Trzeba zgodzić się z poglądem, że korupcja występu-

[71] P. Wiatrowski, *Prawne, ekonomiczne i socjologiczne aspekty korupcji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2008, nr 776, s. 102.

[72] M. Bartoszewicz, *Zagrożenia korupcyjne w polskim samorządzie*, „Rocznik Samorządowy" 2016, t. 5, s. 24.

[73] A. Cieślik, Ł. Goczek, *On the of Corruption Patterns in the Post-Communist Countries*, „*Equilibrium. Quarterly Journal of Economics and Economic Policy*" 2015, nr 1, s. 37.

je nie tylko w sektorze publicznym[74], lecz także w działalności wszystkich podmiotów i organizacji, które działają w obrocie gospodarczym[75]. Nie można jednak zaakceptować takiego toku rozumowania, że istnienie praktyk korupcyjnych odnosi się jedynie do krajów postkomunistycznych, gdyż tego typu zjawiska mają również swoją odsłonę w państwach o ugruntowanej demokracji[76].

Zachowania korupcyjne są najczęściej kojarzone i utożsamiane ze światem polityki oraz sprawowaniem władzy publicznej. Wskazuje się przy tym na związek między korupcją a naciskami politycznymi[77], co jest spostrzeżeniem słusznym. Zdaniem Piotra Solarza w środowisku władzy i administracji publicznej zostały utworzone patologiczne powiązania określane mianem „układ: patron–klient", gdyż (…) *wiążą się z wykorzystywaniem funkcji i publicznych środków finansowych, a także stanowisk w aparacie urzędniczym do gratyfikacji klienteli politycznej*[78]. Jest to bardzo trafna diagnoza rzeczywistości, która diametralnie różni się od twierdzenia, że (…) *państwo stara się przeciwdziałać korupcji poprzez normy prawne i promowanie postaw etycznych*[79].

W najnowszej literaturze przedmiotu pojawia się coraz więcej teoretycznych rozważań na temat możliwych metod i sposobów przeciwdziałania korupcji. Wśród nich wymienia się m.in. potrzebę opracowania strategii antykorupcyjnej, zarządzania przez rzetelność[80], proponuje się przesunięcie zadań związanych ze zwalczaniem korupcji z ABW do CBA[81] oraz zwiększenie swobód gospodarczych obywateli[82]. Zaleca się również wykorzystywanie nowoczesnych technologii informatycznych w nauczaniu zachowań etycznych[83]. Zaznacza się, że wyższe uczelnie jako instytucje odpowiedzialne za kształtowanie postaw młodych ludzi powinny odgrywać doniosłą rolę w procesie edu-

[74] A. Cieślik, Ł. Goczek, *Korupcja, jakość rządzenia a wzrost gospodarczy w krajach transformacji*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2016, nr 5, s. 94.

[75] W.M. Grudzewski, I.K. Hejduk, A. Sankowska, *Korupcja w organizacji*, „Ekonomika i Organizacja Przedsiębiorstwa" 2008, nr 7, s. 5–10.

[76] B. Czepil, *Zjawisko korupcji w demokracji skonsolidowanej. Przypadek Finlandii*, „Przegląd Politologiczny" 2017, nr 2, s. 113–127; P. Grabarz, *Zjawisko korupcji w Polsce i Norwegii – zarys charakterystyki porównawczej*, „Studenckie Zeszyty Naukowe" 2016, nr 29, s. 37–45.

[77] M. Piotrowska, *What Factors Matter for the Evaluation of Relationship between the Perceptions of Corruption and Politicization in Local Administration in Poland*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Ekonomia" 2010, nr 136, s. 138–149.

[78] P. Solarz, *Ekonomiczne i kulturowo-polityczne przyczyny korupcji w Polsce po akcesji do Unii Europejskiej*, „Kwartalnik Naukowy Uczelni Vistula" 2013, nr 4, s. 12.

[79] T. Szewc, *Korupcja: wybrane konsekwencje prawne*, „Organizacja i Zarządzanie" 2015, nr 1, s. 127.

[80] Z. Dobrowolski, *Strategie i metody przeciwdziałania korupcji*, w: *Bezpieczeństwo ekonomiczne państwa. Uwarunkowania, procesy, skutki*, A. Jackiewicz, A. Trzaskowska-Dmoch (red.), Warszawa 2017, s. 122–125.

[81] P. Chodak, *Korupcja – jak ją skutecznie zwalczać*, „Journal of Modern Science" 2017, nr 1, s. 353.

[82] A. Pluskota, *Wpływ wolności gospodarczej na korupcję na przykładzie wybranych państw europejskich*, „Folia Oeconomica Acta Universitatis Lodziensis" 2017, nr 328, s. 161.

[83] E. Stawiarska, J. Machnik-Słomka, *Zastosowanie współczesnych narzędzi informatycznych w nauczaniu w kierunku zachowań etycznych i antykorupcyjnych*, „Organizacja i Zarządzanie" 2016, nr 2, s. 143–156.

kacji obecnych i przyszłych menedżerów w zakresie zachowań etycznych i antykorupcyjnych[84]. Rekomenduje się włączenie do treści nauczania na wyższych uczelniach tzw. Zasad Odpowiedzialnego Kształcenia Menedżerów (ang. *Principles for Responsible Management Education*, PRME)[85]. Nasuwa się jednak ważne pytanie: czy te propozycje rzeczywiście mogą się przyczynić do istotnego ograniczenia skali korupcji w Polsce?

W świetle rozważań zaprezentowanych w artykule warto – tytułem podsumowania – odnieść się do kilku stwierdzeń prezentowanych przez ABW: *Korupcja jest zjawiskiem, które sprzyja nielegalnym mechanizmom podejmowania decyzji kształtujących relacje w przestrzeni publicznej*. *Utrwalone w społeczeństwie zwyczaje korupcyjne są czynnikiem niszczącym struktury państwowe*[86]. Przytoczona opinia wymaga uzupełnienia, ponieważ praktyka dowodzi, że w większości przypadków **korupcja** ma bezpośrednie przełożenie na **legalnie podejmowane decyzje** przez przedstawicieli władzy, tj. zgodnie z przyznanym zakresem kompetencji i uprawnień. Odnośnie do opisywanych zwyczajów dotyczących praktyk kadrowych trzeba powiedzieć, że są one w głównej mierze kreowane i utrwalane przez partie polityczne i panujących włodarzy. Wybrańcy narodu, establishment, nadzwyczajna kasta, towarzystwo salonowe, czyli tzw. grupy trzymające władze, traktują instytucje kontrolowane przez państwo jak swój prywatny folwark i wyłączną własność danej korporacji, co pozostaje w ewidentnej sprzeczności z Konstytucją RP, gdyż: *Rzeczpospolita Polska jest dobrem wspólnym wszystkich obywateli* (art. 1)[87]. A zatem w czyim interesie miałyby być realizowane działania na rzecz zwalczania patologii korupcyjnych i komu miałoby to służyć?

Bartosz Czepil w prawidłowy i logiczny sposób ocenia walkę z korupcją jako (…) *niekończący i autolegitimizujący się proces*[88]. Konieczność przeciwdziałania zjawiskom korupcyjnym jest uzasadniana tym, że pojawiające się nowe formy korupcji, które nigdy się nie kończą, wymuszają stosowanie odmiennych metod i działań antykorupcyjnych. Agnieszka Turska-Kawa twierdzi, że (…) *podmiotem korupcji jest człowiek i to właśnie jego świadomość, wiedza, silna postawa psychologiczna, wewnętrzne kanony uczciwości i rzetelności powinny być punktem wyjścia dla działań antykorupcyjnych*[89]. W nawiązaniu do tych ciekawych refleksji trzeba odpowiedzieć na fundamentalne pytanie: czy wszyscy ludzie mają jednakowe nastawienie do zjawiska korupcji i tożsame zdanie na jego temat?

---

[84] Tamże, s. 144.

[85] E. Pawłowska, K. Skowron, *Wykorzystanie nowoczesnych technologii informatycznych w procesie wdrażania zasad nauczania przeciwko korupcji w szkolnictwie wyższym*, „Zeszyty Naukowe Politechniki Śląskiej. Seria Organizacja i Zarządzanie" 2016, nr 92, s. 256.

[86] *Zwalczanie korupcji*, zakładka „Zadania", www.abw.pl, https://www.abw.gov.pl/pl/zadania/zwalczanie-korupcji/50,Zwalczanie-korupcji.html [dostęp: 9 II 2018].

[87] *Konstytucja Rzeczypospolitej Polskiej*…

[88] B. Czepil, *The "fight against corruption" as a never-ending and self-legitimizing process*, „Studia Socjologiczne" 2016, nr 4, s. 228.

[89] A. Turska-Kawa, *Przeciwdziałanie korupcji – ujęcie wielopłaszczyznowe*, „Political Preferences" 2017, nr 17, s. 110.

Korupcja jest niezwykle pożądaną i cenną wartością dla ludzi układu, którzy dzięki niej zyskują wymierne korzyści, odnoszą spektakularne sukcesy finansowe, mają zapewnione karierę i możliwości rozwoju. Inaczej postrzegają to zjawisko pozostali obywatele, ludzie bez powiązań, koneksji i znajomości, którzy są marginalizowani, blokowani i wyniszczani przez funkcjonujące układy będące immanentną cechą zarządzania i sprawowania władzy w każdej organizacji. Oznacza to, że zależnie od przyjętej perspektywy korupcja będzie odmiennie interpretowana i oceniana – w pozytywnym bądź negatywnym aspekcie. Praktyki korupcyjne zmieniają się wraz z rozwojem sytuacji, ponieważ dostosowują się do nowych realiów, wyzwań współczesności, stąd też przybierają bardziej wyrafinowane, bezpieczne dla uczestników i skryte formy. Niezmienne natomiast od wielu lat pozostają cele, zasady i mechanizmy funkcjonowania układu[90].

Bibliografia:

Bartoszewicz M., *Zagrożenia korupcyjne w polskim samorządzie*, „Rocznik Samorządowy" 2016, t. 5, s. 21–40.

Bojarski J., *Korupcja gospodarcza. Studium z dziedziny polityki kryminalnej*, Toruń 2015, Wydawnictwo Naukowe UMK.

Borowiec P., *Korupcja w III RP – obszary szczególnego występowania*, „Środkowo-europejskie Studia Polityczne" 2007, nr 1, s. 189–208.

Brol M., *Ekonomiczne i instytucjonalne metody przeciwdziałania korupcji*, „Współczesne Problemy Ekonomiczne" 2017, nr 2, s. 57–65.

Burzyński J., Burzyński T., *Ryzyko zachowań korupcyjnych w instytucjach państwowych na przykładzie Służby Celnej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2013, nr 2, s. 217–229.

Chodak P., *Korupcja – jak ją skutecznie zwalczać*, „Journal of Modern Science" 2017, nr 1, s. 339–354.

Chodak P., *Zgoda społeczeństwa na niewielkie przestępstwa korupcyjne*, „Journal of Modern Science" 2013, nr 3, s. 193–209.

Chodorowska A.E., Stopińska J.M., *Korupcja w ochronie zdrowia*, „Journal of ModernScience" 2012, nr 4, s. 163–181.

Chruściel M., *Wojsko jako podatny grunt dla korupcji*, w: *Realizacja działań antykorupcyjnych w resorcie obrony narodowej*, R. Wykurz (red.), Warszawa 2017, Komenda Główna Żandarmerii Wojskowej, s. 7–18.

Cielsielski M., *Zjawiska korupcyjne jako podstawowa kategoria zagrożeń*

[90] W. Walczak, *Źródła zachowań o charakterze korupcyjnym w praktyce zarządzania*, w: *Korupcja w administracji*, M. Myśliwiec, A. Turska-Kawa (red.), Katowice 2016, s. 63–88.

bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP – perspektywa Służby Kontrwywiadu Wojskowego, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 209–218.

Cieślik A., Goczek Ł., *Korupcja, jakość rządzenia a wzrost gospodarczy w krajach transformacji*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2016, nr 5, s. 91–119.

Cieślik A., Goczek Ł., *On the of Corruption Patterns in the Post-Communist Countries,* „Equilibrium. Quarterly Journal of Economics and Economic Policy" 2015, nr 1, s. 33–53.

Czepil B., *The "fight against corruption" as a never-ending and self-legitimizing process*, „Studia Socjologiczne" 2016, nr 4, s. 201–228.

Czepil B., *Zjawisko korupcji w demokracji skonsolidowanej. Przypadek Finlandii*, „Przegląd Politologiczny" 2017, nr 2, s. 113–127.

Dendura K., *Korupcja jako patologia kapitału społecznego*, w: *Zarządzanie bezpieczeństwem w sektorze publicznym i biznesie*, T. Białas, M. Grzybowski, J. Tomaszewski (red.), Gdynia 2009, Wyższa Szkoła Administracji i Biznesu, s. 31–38.

Dobrowolski Z., *Strategie i metody przeciwdziałania korupcji*, w: *Bezpieczeństwo ekonomiczne państwa. Uwarunkowania, procesy, skutki*, A. Jackiewicz, A. Trzaskowska-Dmoch (red.), Warszawa 2017, CeDeWu, s. 113–128.

Durys E., *Układy, znajomości, „haki". Paranoja spiskowa w polskim kinie współczesnym*, w: „Studia Etnologiczne i Antropologiczne" 2016, t. 16, s. 44–54.

Dzietczyk K., *Zjawisko korupcji jako element życia społecznego*, „Seminare. Poszukiwania naukowe" 2016, nr 3, s. 111–121.

Falenta P., *Przestępstwo korupcji – uwarunkowania karnoprawne i społeczne*, „Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu" 2016, nr 1, s. 147–163.

Gintowt-Jankowicz M., *Opinia prawna o projekcie ustawy o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw, druk sejmowy nr 119 z 15 grudnia 2015 r.*, Warszawa 2015, Biuro Analiz Sejmowych.

Goczek Ł., *Przyczyny korupcji i skuteczność strategii antykorupcyjnych*, „Gospodarka Narodowa" 2007, nr 4, s. 33–48.

Golonka A., *Korupcja gospodarcza jako przestępstwo przeciwko zasadom uczciwej konkurencji*, „Czasopismo Prawa Karnego i Nauk Penalnych" 2013, z. 3, s. 51–69.

Grabarz P., *Zjawisko korupcji w Polsce i Norwegii – zarys charakterystyki porównawczej*, „Studenckie Zeszyty Naukowe" 2016, nr 29, s. 37–45.

Grudzewski W.M., Hejduk I.K., Sankowska A., *Korupcja w organizacji*, „Ekonomika i Organizacja Przedsiębiorstwa" 2008, nr 7, s. 5–10.

Gurtowski M., *Niepewność, korupcja i granice podmiotowości w medykalizującym się świecie z perspektywy teorii władzy Michela Croziera i Erharda Friedberga*, „Pogranicze. Polish Borderlands Studies" 2016, nr 2, s. 193–214.

Hussein A., *Mechanizmy korupcjogenne – cztery grzechy główne władz publicznych*, „Przegląd Antykorupcyjny" 2011, nr 1, s. 42–47.

Hussein A., *Obszary zagrożenia korupcją – przegląd badań NIK opublikowanych w 2016 roku*, „Kontrola Państwowa" 2017, nr 5, s. 50–60.

Informacja o wynikach działalności Centralnego Biura Antykorupcyjnego w 2016 r., Centralne Biuro Antykorupcyjne, Warszawa 2017.

Kamiński A.Z., *Korupcja jako symbol instytucjonalnej niewydolności państwa i zagrożenie dla rozwoju polityczno-gospodarczego Polski*, „Zeszyty Centrum im. Adama Smitha" 1997, nr 29, s. 3–32.

Karpiel D., *Przestępczość zorganizowana*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, nr 7, s. 4–21.

Kietliński K., *Korupcja jako naruszenie sprawiedliwości społeczno-gospodarczej oraz zagrożenie dla moralnych podstaw społeczeństwa*, „Problemy Zarządzania" 2010, nr 2, s. 139–147.

Kubiak A., *Działania antykorupcyjne – wybrane przykłady*, „Acta Universitatis Lodziensis Folia Oeconomica" 2013, nr 288, s. 45–57.

Laskowska K., *Rola korupcji w działalności zorganizowanych grup przestępczych*, w: *Oblicza współczesnej przestępczości zorganizowanej*, K. Laskowska (red.), Białystok 2014, Temida 2, s. 143–154.

Maćkowska R., *Informacja w przestrzeni publicznej a zjawisko korupcji i jego postrzeganie*, w: *Public relations w perspektywie naukowej*, A. Adamus-Matuszyńska (red.), Katowice 2016, Wydawnictwo Uniwersytetu Ekonomicznego, s. 116–124.

Matusiak J., *Peryferyjny kapitalizm zależny*, e-book, 2006.

Mapa korupcji. Zwalczanie przestępczości korupcyjnej w Polsce w 2016 r., Warszawa 2017, Centralne Biuro Antykorupcyjne.

Miętek A., *Zasada demokratycznego państwa prawnego w orzecznictwie Trybunału Konstytucyjnego*, „Dialogi Polityczne III RP" 2009, nr 11, s. 75–85.

Nowakowski K., *Zagrożenia etyczne i korupcyjne w mediach*, „Studia Medioznawcze" 2017, nr 2, s. 128–140.

Nowakowski K., *Korupcja a instytucje w gospodarce*, „Ekonomia i Prawo" 2006, nr 1, s. 137–159.

Nowakowski K., *Korupcja jako problem teoretyczny i społeczno-ekonomiczny*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, nr 2, s. 77–94.

Pawłowska E., Skowron K., *Wykorzystanie nowoczesnych technologii informatycznych w procesie wdrażania zasad nauczania przeciwko korupcji w szkolnictwie wyższym*, „Zeszyty Naukowe Politechniki Śląskiej. Seria Organizacja i Zarządzanie" 2016, nr 92, s. 255–267.

Pluskota A., *Czy globalizacja wspiera korupcję?,* „Ekonomia Międzynarodowa" 2017, nr 17, s. 39–48.

Pluskota A., *Wpływ wolności gospodarczej na korupcję na przykładzie wybranych państw europejskich*, „Folia Oeconomica Acta Universitatis Lodziensis" 2017, nr 328, s. 151–162.

Piotrowska M., *What Factors Matter for the Evaluation of Relationship between the Perceptions of Corruption and Politicization in Local Administration in Poland*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Ekonomia" 2010, nr 136, s. 138–149.

Postawy wobec korupcji w samorządzie terytorialnym. Raport z badań w województwie śląskim, A. Turska-Kawa, M. Czaja (red.), Katowice 2015, Fundacja Akademicka IPSO ORDO.

Potulski J., *Penalizacja korupcji w sporcie – uwagi krytyczne*, „Prokuratura i Prawo" 2012, nr 3, s. 67–78.

Raport Agencji Bezpieczeństwa Wewnętrznego: Korupcja w Polsce – próba analizy zjawiska, Warszawa 2004.

Romański M., *Znaczenie zjawiska korupcji dla bezpieczeństwa państw upadłych*, „Roczniki Ekonomii i Zarządzania" 2017, nr 1, s. 25–40.

Rządowy Program Przeciwdziałania Korupcji na lata 2014–2019, Warszawa 2014.

Solarz P., *Ekonomiczne i kulturowo polityczne przyczyny korupcji w Polsce po akcesji do Unii Europejskiej*, „Kwartalnik Naukowy Uczelni Vistula" 2013, nr 4, s. 5–14.

Solarz P., *Korupcja, klientelizm i kapitalizm polityczny jako podstawowe pojęcia w dyskursie o jawności życia publicznego w Polsce*, „Kontrola Państwowa" 2007, nr 3, s. 114–118.

Stachowicz-Stanuch A., Sworowska A., *Definiowanie korupcji w kontekście różnic kulturowych*, „Organizacja i Zarządzanie" 2012, nr 1, s. 97–116.

Stachowicz-Stanuch A., Sworowska A., *Oblicza korupcji: formy i typy zachowań*, „Organizacja i Zarządzanie" 2012, nr 1, s. 117–133.

Stawiarska E., Machnik-Słomka J., *Zastosowanie współczesnych narzędzi informatycznych w nauczaniu w kierunku zachowań etycznych i antykorupcyjnych*, „Organizacja i Zarządzanie" 2016, nr 2, s. 143–156.

Svensson J.*, Osiem pytań na temat korupcji*, „Gospodarka Narodowa" 2006, nr 9, s. 77–106.

Szewc T., *Korupcja: wybrane konsekwencje prawne*, „Organizacja i Zarządzanie" 2015, nr 1, s. 127–144.

Szwajdler P., *The legal aspects of corruption in sport*, „Journal of Education, Health and Sport" 2016, nr 5, s. 445–451.

Tanzler D., *Korupcja jako metafora*, „Roczniki Nauk Społecznych" 2012, nr 4, s. 69–87.

Turska-Kawa A., *Przeciwdziałanie korupcji – ujęcie wielopłaszczyznowe*, „Political Preferences" 2017, nr 17, s. 109–118.

Walczak W., *Działania analityczno-informacyjne identyfikujące mechanizmy korupcyjne w procesach zarządzania*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 55–72.

Walczak W., *Źródła zachowań o charakterze korupcyjnym w praktyce zarządzania*, w: *Korupcja w administracji*, M. Myśliwiec, A. Turska-Kawa (red.), Katowice 2016, Fundacja Akademicka IPSO ORDO, s. 63–88.

Wiatrowski P., *Prawne, ekonomiczne i socjologiczne aspekty korupcji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2008, nr 776, s. 97–111.

Wilk L., *Korupcja w reklamie farmaceutycznej*, „Prokuratura i Prawo" 2011, nr 10, s. 21–36.

Wojtasik W., *Społeczne postrzeganie korupcji politycznej w perspektywie oceny uczciwości władz politycznych*, „Political Preferences" 2017, nr 17, s. 119–128.

Akty prawne:

Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r. (Dz.U z 1997 r. nr 78 poz. 483, ze zm.).

Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j.: Dz.U. z 2017 r. poz. 1993, ze zm.).

Ustawa z dnia 6 czerwca 1997 roku – Kodeks karny (Dz.U. z 1997 r. nr 88 poz. 553, ze zm.).

Ustawa z dnia 27 sierpnia 2009 r. o finansach publicznych (Dz.U. z 2009 r. nr 157 poz. 1240, ze zm.).

Ustawa z dnia 29 stycznia 2004 r. – Prawo zamówień publicznych (t.j.: Dz.U. z 2017 r. poz. 1579, ze zm.).

Ustawa z dnia 30 grudnia 2015 r. o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw (Dz.U. z 2016 r. poz. 34).

Abstrakt

W artykule przedstawiono rozważania i analizy umożliwiające szczegółowe rozpoznanie istoty zjawiska korupcji postrzeganej w kontekście powszechnie stosowanych metod zarządzania i procesów decyzyjnych. Na wstępie wyjaśniono, jak należy rozumieć pojęcie k o r u p c j a, a także scharakteryzowano główne mechanizmy korupcjogenne. W dalszej części pracy korupcja jest analizowana jako ważny element systemu zarządzania. W tym miejscu zwrócono szczególną uwagę na zagrożenia interesów ekonomicznych państwa, a także naruszanie zasad praworządności i sprawiedliwości społecznej. Następnie omówiono przejawy i współczesne formy zachowań korupcyjnych, a także wskazano główne obszary funkcjonalne w zarządzaniu organizacjami, w których najczęściej dochodzi do korupcji. W końcowej części wnikliwie przeanalizowano politykę kadrową jako istotny komponent korupcyjnych praktyk.

Słowa kluczowe: korupcja, mechanizmy korupcjogenne, władza, wpływy, powiązania, praworządność, sprawiedliwość społeczna.

Mateusz Jaremczuk

Współpraca Narodowego Antykorupcyjnego Biura Ukrainy ze służbami specjalnymi innych państw a bezpieczeństwo wewnętrzne Polski

Wstęp

W związku z protestami na Placu Europejskim w Kijowie oraz kryzysem na Krymie i we wschodniej części Ukrainy, które miały miejsce na przełomie lat 2013–2014, władzę stracił dotychczasowy prezydent tego kraju Wiktor Janukowycz. W wyniku tych wydarzeń doszło do wyboru nowych władz na Ukrainie oraz do odwrócenia wektora jej polityki zagranicznej, który do tej pory był skierowany na Rosję. Nowy rząd oraz prezydent zgodnie z oczekiwaniami ukraińskiego narodu rozpoczęli w 2014 r. proces odtwarzania relacji z Zachodem, szczególnie z Unią Europejską i Stanami Zjednoczonymi. Warunkiem poprawy tych relacji było przeprowadzenie przez Ukrainę wielu reform wewnątrzustrojowych, których celem było m.in. ograniczenie nadużyć ze strony władzy i oligarchów[1]. Implikacje kryzysu ukraińskiego, trwającego od listopada 2013 r., mają wpływ także na bezpieczeństwo wewnętrzne Polski. Ponadto granica polsko-ukraińska jest zarazem granicą Ukrainy z Organizacją Paktu Północnoatlantyckiego i Unią Europejską.

Walka z korupcją jest jednym z najistotniejszych wyzwań, przed jakimi stoi nowa władza na Ukrainie. Od poziomu korupcji i zaangażowania władz w jej zwalczanie jest uzależniona pomoc finansowa państw zachodnich dla Ukrainy. Bez wyeliminowania korupcji z życia publicznego ukraińska gospodarka jest skazana na stagnację. Obie te kwestie są niezwykle istotne i od nich zależy poziom dalszego rozwoju Ukrainy. Nowo wybrane władze ukraińskie podjęły się zwalczania korupcji i na wzór państw zachodnich powołały w tym celu służbę specjalną: Narodowe Antykorupcyjne Biuro Ukrainy. Niniejszy artykuł ma na celu określenie wpływu współpracy tego Biura ze służbami specjalnymi innych państw na bezpieczeństwo wewnętrzne Polski.

Problem korupcji na Ukrainie jest szczególnie istotny w kontekście imigracji setek tysięcy obywateli ukraińskich do Polski. Należy zatem określić, w jakim stopniu korupcja destabilizująca państwo ukraińskie wpływa na bezpieczeństwo Polski. Problem korupcji dotyczy bowiem zarówno obywateli, których sytuacja wewnętrzna Ukrainy zmusza do emigracji, jak i państwa ukraińskiego jako całości. Destabilizacja tak dużego kraju leżącego w Europie Środkowo-Wschodniej wpływa na sytuację geopolityczną w regionie. W związku z powyższym zasadne wydaje się stwierdzenie, że państwa Unii Europejskiej (zwłaszcza graniczące z Ukrainą) oraz Stany Zjednoczone jako supermocarstwo dbające o ład międzynarodowy, powinny wspomagać ukraińskie

[1] W. Głowacki, *Rok w którym Europa osiwiała*, „Polska The Times" z 21 listopada 2014 r.

służby zwalczające korupcję, gdyż leży to w ich interesie. Instytucje odpowiedzialne za walkę z korupcją na Ukrainie nie mają doświadczenia w zakresie przyznanych im kompetencji oraz właściwości rzeczowej wskazanych w powołujących je aktach prawnych. Dlatego odpowiednia współpraca z analogicznymi jednostkami innych państw przełoży się na ich efektywność. Jakość tej współpracy będzie oddziaływać w dalszej perspektywie na poprawę lub pogorszenie bezpieczeństwa nie tylko na Ukrainie, lecz także w Polsce.

Korupcja a bezpieczeństwo wewnętrzne

Andrzej Barcikowski w artykule zatytułowanym *Bezpieczeństwo wewnętrzne – różne perspektywy analityczne i doktrynalne*[2] zwraca uwagę na to, że bezpieczeństwo wewnętrzne nie jest osobną dziedziną badawczą. Można je natomiast uznać za pokrewne naukom politycznym oraz prawu konstytucyjnemu, gdyż analizy tego zagadnienia mają przede wszystkim wymiar praktyczny. Zauważa także, że (…) *precyzyjna kategoryzacja, eksplikacja oraz predykcja w dziedzinie bezpieczeństwa wewnętrznego mogą i powinny wpływać na dobór instrumentów i obszarów działania państwa*[3] oraz że bezpieczeństwo wewnętrzne odnosi się do państwa jako całości, a nie do jego poszczególnych elementów. Stanisław Sulowski zaś akcentuje, że bezpieczeństwo nie ma charakteru stałego, a jego pojmowanie jest subiektywne, zwłaszcza w kontekście kulturowym i politycznym[4].

Jednym z czynników wpływających bezpośrednio na bezpieczeństwo wewnętrzne państwa jest k o r u p c j a. Definicja tego zjawiska wskazuje, że dochodzi do niego przy udziale dwóch świadomie działających stron. Jedna z nich wywiera wpływ za pomocą określonych dóbr na drugą, egzekwując w ten sposób określone działanie. Partnerzy dopuszczający się korupcji działają w porozumieniu i dążą do zatajenia zawartej transakcji, aby uniknąć odpowiedzialności. Taką definicję proponuje Piotr Sulowski w artykule *Korupcja zagrożeniem dla bezpieczeństwa wewnętrznego państwa*[5]. Korupcji może się dopuścić także jedna osoba. Dotyczy to przede wszystkim osób sprawujących funkcje publiczne, które przy wykorzystaniu zajmowanego stanowiska mogą defraudować lub przejmować majątek publiczny lub doprowadzać do jego niewłaściwego rozdysponowania. Możliwe jest także dokonanie czynu zabronionego przez osoby niezajmujące stanowisk publicznych, które nie stosują się do obowiązującego prawa i przez wydawanie ekspertyz lub opinii dążą do osiągnięcia zysku[6]. Określenie

[2] A. Barcikowski, *Bezpieczeństwo wewnętrzne – różne perspektywy analityczne i doktrynalne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11, s. 11.

[3] Tamże, s. 11–12.

[4] P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, www.abw.gov.pl/download/1/1756/Majer.pdf [dostęp: 25 VII 2018].

[5] P. Sulowski, *Korupcja zagrożeniem dla bezpieczeństwa wewnętrznego państwa*, „Annales Universitatis Paedagogicae Cracoviensis. Studia Politologica" 2012, nr 8, s. 57–58.

[6] Ł. Szwejkowski, *Korupcja, wybrane zagadnienia*, seria: „Materiały dydaktyczne" nr 87, Legionowo 2013, s. 7–8.

korupcja poza łapownictwem i sprzedajnością dotyczy także nadużywania funkcji, nepotyzmu, faworytyzmu oraz płatnej protekcji. Istotnym czynnikiem charakteryzującym korupcję jest jej niemal nieograniczona wielopostaciowość. Przedmiot korupcji jest kształtowany przez wiele determinantów w zależności od kraju, w jakim występuje, częstotliwość i powszechność oraz czas dokonania czynu zabronionego. Może dotyczyć zarówno krajów wysoko, jak i słabo rozwiniętych, sektora publicznego lub prywatnego, a także organizacji pozarządowych i fundacji[7].

Przy badaniu wpływu korupcji na bezpieczeństwo wewnętrzne państwa, szczególnie w odniesieniu do Ukrainy, jest uzasadnione wskazanie jej rodzajów i wywoływanych przez nią skutków. Niewątpliwie każdy rodzaj korupcji niesie za sobą negatywne konsekwencje dla stanu bezpieczeństwa państwa (zarówno długo-, jak i krótkoterminowe). Korupcję można klasyfikować pod kątem wielu czynników. Na potrzeby niniejszego artykułu przyjęto podział ze względu na sferę działalności państwa – administracyjną, gospodarczą i polityczną. Z uwagi na przenikanie się tych dziedzin także korupcja występuje na kilku płaszczyznach.

Korupcja administracyjna (**urzędnicza**) polega na przyjmowaniu przez pracowników administracji publicznej dodatkowych gratyfikacji uzyskiwanych w sprawach urzędowych za zrealizowanie obowiązku wynikającego z regulaminu danej jednostki organizacyjnej lub za odstąpienie od niego. Skorumpowani urzędnicy w zamian za korzyści osobiste przyczyniają się do powstania przeważnie ekonomicznych strat, które uniemożliwiają prawidłową działalność państwa. Z korupcją urzędniczą często wiąże się **korupcja gospodarcza**. Występuje ona z reguły tam, gdzie są podejmowane decyzje administracyjne, a co za tym idzie – wydaje się pieniądze z budżetu państwa. Polega ona przede wszystkim na przekupstwie i sprzedajności. Wykorzystując te instrumenty, przedsiębiorcy wpływają na urzędników oraz polityków w celu osiągnięcia korzystnych warunków dla swojej działalności. Powoduje to zakłócenia procesów gospodarczych państwa, które mogą hamować rozwój kraju oraz przyczyniać się do spadku produktywności przez ingerencję w działanie rynku. Ponadto paraliżuje prawidłowe funkcjonowanie państwa oraz obniża autorytet instytucji państwowych. **Korupcja polityczna** zaś ma związek z działaniem na rzecz partii politycznych (oraz ich członków), które w sposób nielegalny dążą do zdobycia lub utrzymania władzy. Ten rodzaj korupcji ma szczególny wpływ na funkcjonowanie państwa przez bezpośrednie oddziaływanie na sposób rządzenia, co przekłada się na destabilizację na scenie politycznej. Bardzo często ten rodzaj korupcji wynika z kultury oraz historii państwa, nierzadko bowiem jej funkcjonowaniu towarzyszy społeczne przyzwolenie i uznawanie korupcji za powszechną praktykę[8].

Olgierd Chybiński zwrócił uwagę także na zjawisko **płatnej protekcji**[9] oraz na niebezpieczeństwo związane z jej zakorzenieniem się w społeczeństwie. W wielu państwach przyjęło się, że do załatwienia sprawy w urzędzie trzeba mieć znajomości

[7] P. Sulowski, *Korupcja zagrożeniem dla bezpieczeństwa*…, s. 57.
[8] Tamże, s. 58–64.
[9] O. Chybiński, *Płatna protekcja*, Warszawa 1967, s. 7–8.

bądź należy wręczyć pośrednikowi łapówkę. Ten proceder jest wykorzystywany przez oszustów, którzy nierzadko nie mają nic wspólnego z daną instytucją.

Jako główne implikacje oddziaływania korupcji na bezpieczeństwo wewnętrzne państwa należy wymienić: pomnażanie kosztów funkcjonowania państwa, które w ostateczności muszą zostać pokryte przez obywateli, spowolnienie rozwoju gospodarczego, uzależnienie decyzji politycznych od podmiotów zewnętrznych, spadek atrakcyjności dla inwestorów zagranicznych, obniżenie zaufania obywateli do instytucji państwowych oraz ograniczenie konkurencji w gospodarce. Czynnikiem szczególnie szkodliwym dla państwa jest także to, że poziom korupcji jest wprost proporcjonalny do trudności pozbycia się tego problemu. Wynika to z uzależnienia władz i urzędników od pieniędzy pochodzących z korupcji – im większa jest ta zależność, tym mniejsza jest motywacja do wprowadzenia regulacji prawnych dążących do zwalczenia tego zjawiska[10].

Walka z korupcją na Ukrainie

Jak wspomniano na wstępie, korupcja jest jednym z najpoważniejszych problemów Ukrainy, który skutecznie separuje ten kraj od państw Zachodu. Jednym z powodów wybuchu tzw. Euromajdanu było odstąpienie Wiktora Janukowycza od podpisania umowy stowarzyszeniowej z Unią Europejską. Swoją decyzję ukraiński rząd ogłosił 21 listopada 2013 r.[11] Eksperci wskazują, że gdyby prezydent Wiktor Janukowycz podpisał dokument i zadeklarował chęć współpracy z Unią Europejską, to zobowiązałby się do zreformowania kraju, także pod kątem walki z korupcją. Prezydent będący pod wpływem Rosji oraz grup oligarchów zdecydował się na demonstrację przywiązania do dotychczasowego stylu rządów i odrzucił propozycję Unii Europejskiej[12]. To doprowadziło do buntu dużej części ukraińskiego społeczeństwa, które liczyło na zmiany, zwłaszcza skorumpowanej władzy[13]. Konsekwencją tzw. rewolucji wolności było odsunięcie Janukowycza od władzy. Objęcie rządów przez Petro Poroszenkę oraz zmiana składu rządu w 2014 r. dawały nadzieję na zreformowanie państwa i wyeliminowanie patologii z życia publicznego.

Według „Światowego Barometru Korupcji" opublikowanego przez organizację Transparency International w styczniu 2018 r. Ukraina znajduje się na 130. miejscu pod względem poziomu korupcji wśród 176 państw, które znalazły się w zestawieniu[14]. W sondażu za 2017 r. Ukraina uzyskała 30 na 100 możliwych punktów (im większa liczba punktów, tym mniejszy problem z korupcją i większa transparent-

[10] A. Barcikowski, *Bezpieczeństwo wewnętrzne – różne perspektywy*…, s. 18–19.

[11] W. Konończuk, *Ukraina rezygnuje z podpisania umowy stowarzyszeniowej w Wilnie: przyczyny i implikacje*, https://www.osw.waw.pl/pl/publikacje/analizy/2013-11-27/ukraina-rezygnuje-z-podpisania-umowy-stowarzyszeniowej-w-wilnie [dostęp: 25 VII 2018].

[12] M. Czech, *Kres zbliżenia Ukrainy z Europą: Janukowycz wywrócił stolik*, „Gazeta Wyborcza" z 22 listopada 2013 r.

[13] K. Kwiatkowska, *Mustafa odbije Ukrainę*, „Gazeta Wyborcza" z 29 listopada 2013 r.

[14] *Corruption Perceptions Index 2017*, https://www.transparency.org/news/feature/corruption_perceptions_index_2017 [dostęp: 25 VII 2018].

ność) i znalazła się wśród najbardziej skorumpowanych państw świata. Dla porównania – Polska z 60 punktami znalazła się w zestawieniu na 36. pozycji. Obywatele Ukrainy postrzegają korupcję jako jeden z najistotniejszych problemów państwa (56 proc. ankietowanych)[15]. Ankietowani uznają, że poziom korupcji w ciągu kilku ostatnich lat się nie zmienił (72 proc.), a winnym tego stanu jest przede wszystkim prezydent Petro Poroszenko (60 proc.). Urzędujący prezydent nie cieszy się zaufaniem publicznym (70 proc. respondentów nie ma do niego zaufania). Jedynie 13 proc. biorących udział w ankiecie jest zdania, że władze Ukrainy zmierzają do rozwiązania problemu korupcji. Taka ocena przekłada się na negatywny stosunek do prezydenta. Z raportu wynika też, że spadek poparcia dla aktualnie rządzących powoduje wzrost poparcia wśród partii populistycznych, które tak naprawdę nie są zainteresowane walką z korupcją. Jeśli chodzi o autorefleksję samych Ukraińców odnośnie do korupcji, to sondaż również nie daje nadziei na ewentualne pozytywne zmiany. Co prawda około 33 proc. badanych wskazuje łapownictwo jako jedną z trzech głównych przyczyn niepozwalających na skuteczną walkę z korupcją, ale tylko 25 proc. ankietowanych uważa, że to społeczeństwo jest współodpowiedzialne za taki stan rzeczy. Na szczególną uwagę zasługuje to, że aż 2/3 Ukraińców jest zdania, że korupcja jest integralną częścią ich życia[16].

Mimo że wyniki sondażu dają obraz Ukrainy głęboko pogrążonej w problemach związanych z korupcją, to na przestrzeni ostatnich kilku lat widać subtelną poprawę. W 2012 r. organizacja Transparency International w opublikowanym „Światowym Barometrze Korupcji" przyznała Ukrainie 26 pkt, w 2013 r. – 25 pkt, w 2014 r. – 26 pkt, a w 2015 r. – 27 pkt[17]. Może to świadczyć o tym, że poza 2013 r. tendencja występowania tego zjawiska jest wzrostowa. Warto zaznaczyć, że to właśnie rok 2013 był momentem przełomu w społeczeństwie ukraińskim.

W związku z uzależnieniem przyznania pomocy Ukrainie przez Unię Europejską od podjęcia walki tego kraju z korupcją, podjęto w tym kierunku konkretne działania. Wykorzenienie korupcji z życia publicznego stało się jednym z najważniejszych zadań nowych rządów pod przewodnictwem Arsenija Jaceniuka, a następnie Wołodymira Hrojsmana. W październiku 2014 r. ukraiński parlament uchwalił pakiet ustaw antykorupcyjnych powołujących do życia podmioty, które stały się instytucjonalną podstawą do walki z korupcją: Narodową Agencję ds. Poszukiwania i Rozporządzania Aktywami Pochodzącymi z Przestępstw Korupcyjnych, Narodową Agencję ds. Zapobiegania Korupcji, Wyspecjalizowaną Prokuraturę Antykorupcyjną oraz Narodowe Antykorupcyjne Biuro Ukrainy[18].

Za jeden z przełomowych momentów w ostatnim czasie w walce z korupcją na Ukrainie można uznać ujawnienie deklaracji majątkowych ponad 100 tys. urzędników i polityków, w tym tych najwyższych rangą. System elektronicznych deklaracji

[15] Na pierwszym miejscu wskazano problemy gospodarcze (69% ankietowanych).

[16] V. Rybak, *Ukraine's fight against corruption, explained*, http://euromaidanpress.com/2016/12/16/ukraine-corruption-reform/ [dostęp: 25 VII 2018].

[17] www.transparency.org/cpi [dostęp: 3 I 2018].

[18] P. Kościński, *Problem korupcji na Ukrainie*, https://www.pism.pl/publikacje/biuletyn/nr-3-1445# [dostęp: 25 VII 2018].

majątkowych wywołał poruszenie w społeczeństwie ukraińskim. Okazało się – według obliczeń Reutera – że średnio na członka ukraińskiego rządu przypada prawie 300 tys. dolarów oszczędności w gotówce, przy miesięcznej pensji 200 dolarów. Upublicznienie tych danych spotkało się z wyrażeniem niezadowolenia przez ukraińskich parlamentarzystów[19]. Za sukces w walce z korupcją można uznać także wdrożenie systemu zamówień publicznych ProZorro. Pozwolił on na zachowanie w budżecie tylko w 2016 r. około 320 mln dolarów[20].

Jak informuje Piotr Kościński, powołując się na ukraiński portal Naszi Hroszi, wciąż największym problemem w walce z korupcją na Ukrainie jest nieuczciwość najważniejszych urzędów w państwie, włącznie z sądami. W interesie sędziów i prokuratorów jest utrzymanie stanu obecnego. Dziennik podaje, że spośród około tysiąca osób, którym postawiono zarzuty korupcyjne w okresie między lipcem 2015 r. a czerwcem 2016 r., tylko 3 proc. zostało skazanych prawomocnym wyrokiem. Wartość skonfiskowanego majątku pochodzącego z przestępstw korupcyjnych w latach 2015–2016 wyniosła jedynie 10 tys. dolarów, mimo zakładanego wpływu 368 mln dolarów, co powoduje duże straty w budżecie państwa. Łatwo obliczyć, że wpływ do budżetu był 36,8 tys. razy mniejszy, niż zakładano[21].

Do zjawisk pozytywnych należy zaliczyć rozpoczęcie walki z korupcją przez państwo ukraińskie, które można zaobserwować po wydarzeniach związanych z tzw. Euromajdanem. Trzeba jednak zauważyć, że motywacja – nie tylko rządzących, lecz także całego społeczeństwa – do tej walki jest niewielka. Wydaje się zatem zasadne stwierdzenie, że bez pomocy z zewnątrz Ukraina nie jest w stanie poradzić sobie z tak wielkim problemem. Tę tezę potwierdzają słowa Marii Jarosz, która zjawisko korupcji opisuje zarówno jako przyczynę, jak i skutek niewydolności instytucjonalnej państwa[22].

Narodowe Antykorupcyjne Biuro Ukrainy

W dniu 14 października 2014 r. Rada Najwyższa Ukrainy przyjęła ustawę o Narodowym Antykorupcyjnym Biurze Ukrainy (NABU), która weszła w życie 25 lutego 2015 r.[23] Utworzenie NABU było jednym z wymogów Międzynarodowego Funduszu Walutowego oraz Komisji Europejskiej dotyczących złagodzenia ograniczeń wizowych pomiędzy Unią Europejską a Ukrainą.

W art. 1 wspomnianej ustawy NABU określono jako państwowy organ ścigania, do którego zadań należy: wykrywanie, ściganie, rozpoznawanie i prowadzenie dochodzeń w sprawach związanych z korupcją, a także zapobieganie im, w granicach jego

[19] V. Rybak, *Ukraine's fight against*…

[20] Co-creation of ProZorro, https://www.transparency.org/whatwedo/publication/co_creation_of_prozorro_an_account_of_the_process_and_actors [dostęp: 3 I 2018].

[21] P. Kościński, *Problem korupcji na Ukrainie*…

[22] M. Jarosz, *Władza, przywileje, korupcja*, Warszawa 2004, s. 249.

[23] *Закон України Про Національне антикорупційне бюро України*. Pełna treść dokumentu: http://zakon4.rada.gov.ua/laws/show/1698-18 [dostęp: 4 I 2018].

kompetencji, oraz zapobieganie kolejnym przestępstwom. Artykuł 4 ustawy odnosi się do gwarancji niezależności NABU. Ma ona być zapewniona dzięki zagwarantowanym ustawowo specjalnym procedurom wyboru dyrektora Biura, wyboru pracowników Biura w drodze konkursu, określonym procedurom finansowania Biura, a także dzięki środkom określonym przepisami prawa, które mają na celu zapewnienie bezpieczeństwa pracownikom Biura oraz ich rodzinom. Ustawa w art. 5 stanowi, że maksymalna liczba pracowników Biura nie może przekraczać 700, w tym 200 pracowników personelu wysokiej rangi[24].

W styczniu 2015 r. po raz pierwszy w historii Ukrainy ogłoszono otwarty konkurs na dyrektora agencji państwowej. Spośród 186 kandydatów na stanowisko dyrektora NABU został wybrany Artem Sytnyk[25]. Zdaniem Ruslana Minicha w NABU zatrudniono dobrych, jak na ukraińskie warunki, ekspertów. Pozwoliło to na otwarcie setek spraw dotyczących korupcji. Problemem instytucji jest natomiast uzależnienie jej działania od innych służb. R. Minich jako przykład podaje zależność od Służby Bezpieczeństwa Ukrainy (SBU) w zakresie zakładania podsłuchów oraz uwalnianie przez sądy osób zatrzymanych przez NABU. Zauważa również, że istnieje potrzeba powołania niezależnego sądu antykorupcyjnego jako zupełnie nowej instytucji, która pozwoliłaby na uzupełnienie działań NABU oraz Wyspecjalizowanej Prokuratury Antykorupcyjnej. Ponadto działalność NABU jest zakłócana przez urzędujących polityków, którzy w związku z czynnościami podejmowanymi przez Biuro przestają czuć się bezkarni i starają się przejąć nad nim kontrolę. Wśród części ukraińskich parlamentarzystów popularny jest pomysł przekazania kontroli nad NABU prokuratorowi generalnemu (zależnemu od polityków)[26].

Igor Shevliakov, autor artykułu *Ukraine*[27] odnoszącego się do wyzwań stojących przed instytucjami ukraińskimi w walce z korupcją zaznacza, że NABU nie jest w stanie prawidłowo funkcjonować bez pomocy z zewnątrz. Powstanie Narodowego Antykorupcyjnego Biura Ukrainy jest z pewnością przejawem rozpoczęcia ukraińskiej walki z korupcją, ale zestawienie jego funkcjonowania w teorii z pragmatyzmem jest jednak bezlitosne. Biuro przy pomocy służb innych krajów, szczególnie Federalnego Biura Śledczego (FBI), działa w miarę możliwości niezależnie od władzy. Dużym wyzwaniem jest utrzymanie tej tendencji, jest to bowiem aktualnie jedyna instytucja działająca niezależnie od polityków, co w przypadku walki z korupcją jest warunkiem koniecznym. O ile samo utworzenie Biura można uznać za sukces, o tyle ten sukces będzie bezwartościowy, jeśli Biuro straci niezależność. Walka z korupcją na Ukrainie nie może postępować bez skutecznie działającego NABU. I. Shevliakov dodaje, że pełną świadomość tego mają skorumpowane władze ukraińskie, dlatego próbują wpływać na działanie Biura.

---

[24] *Krajowe Biuro Antykorupcyjne Ukrainy*, „Przegląd Antykorupcyjny" 2016, nr 1, s. 225–227.

[25] https://nabu.gov.ua/en/history-nabu [dostęp: 4 I 2018].

[26] R. Minich, *Ukraine's Fight Against Corruption: Stumble But Not Fall*, http://ukraineworld.org/2017/04/ukraines-fight-against-corruption-stumble-but-not-fall/ [dostęp: 25 VII 2018].

[27] I. Shevliakov, *Ukraine*, w: *Anti-Corruption in Moldova and Ukraine*, A. Sobják (ed.), Warsaw 2015, s. 27–33.

Współpraca Narodowego Antykorupcyjnego Biura Ukrainy ze służbami specjalnymi innych państw

Powstanie NABU było zainicjowane na wyraźne żądanie Zachodu jako jeden z warunków kontynuowania rozmów pomiędzy Unią Europejską a Ukrainą w sprawie złagodzenia polityki wizowej. Jego utworzenie nie oznacza jednak rozwiązania problemu korupcji na Ukrainie. Powstanie Biura jest sygnałem do zmian, ale z biegiem czasu przybywa mu przeciwników. Co istotne, antagoniści Biura wywodzą się z Ukrainy i bardzo często zajmują najważniejsze stanowiska w państwie. Biorąc pod uwagę skalę problemu, jakim jest dla Ukrainy korupcja, konieczne jest uzyskanie poparcia dla działania NABU z zewnątrz. Płynie ono głównie z Zachodu, pomoc oferują Amerykanie, Polacy oraz inne państwa, w których żywotnym interesie jest zahamowanie dalszej destabilizacji Ukrainy.

Stany Zjednoczone jako mocarstwo starają się nie tylko utrzymywać swoją strefę wpływów, lecz także ją poszerzać. Widać to na przykładzie Ukrainy, która po upadku rządów Wiktora Janukowycza stała się partnerem zarówno dla Unii Europejskiej, jak i dla USA. Ukraina jest bezpośrednim sąsiadem NATO, a co za tym idzie – jest państwem ważnym ze względów strategicznych i geopolitycznych. Znajduje się także w kręgu zainteresowań Rosji, przede wszystkim ze względu na to, że do 1991 r. należała do Związku Radzieckiego[28]. Rosja po zajęciu Krymu i zdestabilizowaniu wschodniej części Ukrainy nie zdecydowała się na otwarty konflikt z państwem ukraińskim. Mająca problemy Ukraina jest atrakcyjnym partnerem dla USA, które za pomocą środków finansowych wywierają wpływ na ukraińskie władze, tworząc tym samym strefę buforową pomiędzy NATO a Rosją[29]. Należy zaznaczyć, że takie działania są istotne także dla bezpieczeństwa Polski.

Tylko w ostatnich czterech latach Stany Zjednoczone udzieliły Ukrainie pomocy finansowej oscylującej w granicach dwóch miliardów dolarów. Za prezydentury Baracka Obamy, w marcu 2014 r., Kongres zatwierdził przekazanie temu krajowi miliarda dolarów[30]. Był to okres istotnych zmian na Ukrainie, które dokonywały się przede wszystkim na szczytach władzy, a otrzymane pieniądze miały posłużyć wdrażaniu reform prodemokratycznych i walce z przestępczością. Kolejna kwota – w wysokości 220 mln dolarów, jak podała agencja Reuters – wpłynęła w czerwcu 2016 r.[31] Nastąpiło to dwa miesiące po objęciu urzędu premiera przez Wołodymira Hrojsmana. Joe Beiden, wiceprezydent USA, udzielając informacji o środkach pieniężnych przekazanych Ukrainie, pochwalił także podjęte przez ten kraj reformy. W dniu 12 grudnia

[28] M. Czech, *Rosja bez Ukrainy jak bez ręki. Plan przezbrojenia armii poważnie zagrożony*, „Gazeta Wyborcza" z 23 czerwca 2014 r.

[29] K. Przybyła, *NATO wobec konfliktu na Ukrainie*, „Bezpieczeństwo Narodowe" 2016, nr 37–40, s. 118–120.

[30] J. Weisman, *Congress Approves Aid of $1 Billion for Ukraine*, „The New York Times" z 27 marca 2014 r.

[31] *U.S. to give Ukraine $220 million in new aid: White House*, www.reuters.com [dostęp: 4 I 2018].

2017 r. Blair Guild poinformowała na stronie internetowej telewizji CBS o podpisaniu przez prezydenta Donalda Trumpa nowego budżetu obronnego USA na 2018 r., który zakłada wsparcie Ukrainy kwotą 350 mln dolarów[32]. Potwierdziło się to pośrednio 20 lipca 2018 r., gdy amerykańskie ministerstwo obrony zdecydowało o przekazaniu Ukrainie 200 mln dolarów na cele związane z bezpieczeństwem[33].

Przekazywanie tak dużych sum pieniężnych na przeprowadzanie reform na Ukrainie nie jest dokonywane przez Amerykanów lekkomyślnie. Mając świadomość, jak wielkim problemem w tym kraju jest korupcja i jakie ryzyko niesie oddawanie do dyspozycji tamtejszym urzędnikom tak dużych sum pieniężnych, Amerykanie wpłynęli pośrednio (za pośrednictwem Międzynarodowego Funduszu Walutowego, MFW) na utworzenie NABU. Jednym z najważniejszych partnerów tej organizacji, a także wzorem do naśladowania, było FBI. W styczniu 2016 r. wizytę w Waszyngtonie odbył dyrektor NABU Artem Sytnyk. Zakończyła się ona podpisaniem oficjalnej umowy o współpracy między FBI a NABU. Jak podkreślił Sytnyk[34], szczególnie istotnym aspektem współpracy jest to, że FBI dysponuje instrumentami wykorzystywanymi do śledzenia obiegu dolara, co w przypadku walki z korupcją jest nie do przecenienia. Dyrektor NABU zaznaczył także, że problem korupcji na Ukrainie wykracza poza jej granice, a bez pomocy FBI wykrycie wypływu środków z jego kraju oraz ich zwrot byłyby w znacznym stopniu utrudnione. Umowa ustanowiła współpracę stron w zwalczaniu przestępstw związanych z praniem pieniędzy i odzyskiwaniem mienia, a także pomoc w walce z korupcją ukraińskich urzędników wysokiego szczebla. Ponadto amerykańska agencja zobowiązała się do przekazania ukraińskiej służbie sprzętu ułatwiającego jej funkcjonowanie na odpowiednim poziomie. Sprzęt do digitalizowania dokumentów ofiarowany przez FBI został użyty już w czerwcu 2016 r. podczas afery „Czarnej księgowości" związanej z ukraińską Partią Regionów, na której czele stał Wiktor Janukowycz[35]. Wykorzystanie technik dostarczonych przez Amerykanów znacznie usprawniło pracę ukraińskiej służby[36].

Już w lutym 2016 r. Artem Sytnyk poinformował w wywiadzie radiowym, że do kierowanej przez niego instytucji został przydzielony funkcjonariusz FBI, który będzie odpowiedzialny za współpracę z detektywami NABU oraz za kontrolowanie ich działań pod kątem zgodności ich pracy z amerykańskimi standardami[37]. W maju 2015 r. NABU odwiedził ambasador USA na Ukrainie Geoffrey Pyatt[38], który zwrócił uwagę

[32] *Trump signs National Defense Authorization Act*, www.cbsnews.com [dostęp: 4 I 2018].

[33] https://www.bbc.co.uk/news/world-europe-44909625 [dostęp: 25 VII 2018].

[34] *NACB and FBI will sign memorandum of cooperation*, https://zik.ua/en/news/2016/06/29/nacb_and_fbi_sign_memorandum_on_cooperation_712162 [dostęp: 5 I 2018].

[35] Na temat tej afery zob. https://www.tvn24.pl/wiadomosci-ze-swiata,2/fbi-pomoze-ukrainie-w-sledztwie-ws-paula-manaforta,669904.html (przyp. red.).

[36] *The NABU Director calls upon individuals mentioned in Trepak`s lists to provide their handwriting samples voluntarily*, https://nabu.gov.ua/en/novyny/nabu-director-calls-upon-individuals-mentioned-trepaks-lists-provide-their-handwriting [dostęp: 5 I 2018].

[37] *FBI representative will work together with the NABU detectives*, www.nabu.gov.ua [dostęp: 5 I 2018].

[38] *U.S. Ambassador Marie Yovanovitch visits the NABU*, https://nabu.gov.ua/en/novyny/us-

na rolę, jaką Biuro odgrywa w zmianach zachodzących na Ukrainie. Zaznaczył, że Amerykanie dalej zamierzają wspierać NABU w walce z korupcją, przede wszystkim w zakresie wykonywania nakazów związanych z wysokim ryzykiem, polegających na realizacji czynności w śledztwach, w których pojawiają się duże sumy pieniędzy, a także w które są zamieszani prominentni politycy.

Memorandum o współpracy FBI i NABU weszło oficjalnie w życie 29 czerwca 2016 r. Dwa tygodnie później na Ukrainę przybyli pierwsi funkcjonariusze FBI w celu przeprowadzenia szkolenia dla ukraińskich pracowników Biura[39]. Inauguracyjne szkolenie specjalistyczne trwało 10 dni i objęło m.in. trening taktyczny i praktykę uzbrojenia, metody zatrzymywania przestępców w budynku i samochodzie oraz sposoby przeprowadzania czynności operacyjno-śledczych w pomieszczeniach, w których mogą znajdować się niebezpieczne osoby.

Rok 2017 okazał się owocny dla współpracy NABU z FBI. W czerwcu doszło do zatrzymań w związku z operacją „Bursztyn" prowadzoną przez te struktury[40]. Dzięki współdziałaniu obu instytucji wykryto proceder nielegalnego wydobycia bursztynu na zachodzie Ukrainy oraz zatrzymano urzędników zaangażowanych w tę sprawę, m.in. zastępcę prokuratora regionu. W kręgu podejrzanych pozostaje także ukraiński parlamentarzysta. Szef NABU podkreślił, że operacja nie doszłaby do skutku bez pomocy FBI. Udział osób ze szczytu władzy w przestępczym procederze doprowadził do konfliktu wśród ukraińskich jednostek odpowiedzialnych za walkę z korupcją. Organy, nad którymi politycy sprawują bezpośrednie zwierzchnictwo, przeciwstawiły się sposobowi działania NABU, co uwidoczniło jedynie skalę problemu, z jakim ta organizacja musi się zmagać. Kilka dni po ujawnieniu szczegółów operacji gazeta „Kyiv Post" podała za pośrednictwem agencji Interfax-Ukraine informację o przedłużeniu memorandum o współpracy NABU i FBI o kolejne dwa lata[41]. Strony oświadczyły, że są zadowolone z dotychczasowej współpracy i pragną ją kontynuować.

Operacja „Bursztyn" nie była jedyną operacją prowadzoną w 2017 r. przez NABU przy współpracy z FBI. We wrześniu doszło na Ukrainie do kryzysu instytucji państwowych walczących z korupcją. Narodowe Antykorupcyjne Biuro Ukrainy przy pomocy FBI i Wyspecjalizowanej Prokuratury Antykorupcyjnej wszczęło m.in. postępowanie kontrolne w sprawie ewentualnego nielegalnego wzbogacenia się prokuratora generalnego Ukrainy Jurija Łucenki, a także w sprawie działań korupcyjnych w Służbie Migracyjnej Ukrainy, której kierownictwo miało czerpać zysk z legalizacji pobytu na Ukrainie obywateli innych państw. Sprawę opisał na łamach „The Wall Street Journal" James Marson[42]. Komentator podkreślił, że skuteczność działań antykorupcyjnych

ambassador-marie-yovanovitch-visits-nabu [dostęp: 5 I 2018].

[39] *FBI train Special Forces of Ukraine's National Anti-Corruption Bureau*, https://112.international/politics/rferl-fbi-train-special-forces-of-ukraines-national-anti-corruption-bureau-6984.html [dostęp: 6 I 2018].

[40] *Amber case first joint NABU-FBI operation – Sytnyk*, https://en.interfax.com.ua/news/general/430432.html [dostęp: 6 I 2018].

[41] *NABU, ФБР розширюють співпрацю ще на 2 роки*, www.kyivpost.com [dostęp: 6 I 2018].

[42] J. Marson, *Corruption Battle Roils Ukraine*, „The Wall Steer Journal" z 12 września 2017 r.

na Ukrainie ma ścisły związek ze środkami przekazywanymi dla tego kraju m.in. z MFW czy Banku Światowego.

Do otwartego konfliktu między Służbą Bezpieczeństwa Ukrainy i Prokuraturą Generalną a NABU i Wyspecjalizowaną Prokuraturą Antykorupcyjną doszło w listopadzie 2017 r. Aresztowano wówczas funkcjonariusza NABU, który działał pod przykryciem w sprawie dotyczącej nieprawidłowości w Służbie Migracyjnej Ukrainy. Do zatrzymania doszło na polecenie prokuratora generalnego, który uważał, że NABU działała poza granicami obowiązującego prawa. Sprawa odbiła się szerokim echem na Zachodzie. Głos w sprawie zabrała m.in. przedstawicielka MFW Christine Lagarde, która wyraziła zaniepokojenie wydarzeniami mogącymi powstrzymać rozwój niezależnych instytucji do walki z korupcją na Ukrainie. Bank Światowy oraz Departament Stanu USA wydały oświadczenia w podobnym tonie. Sugerowały, że ograniczenie niezależności NABU może niekorzystnie odbić się na poparciu Ukrainy przez państwa Zachodu na arenie międzynarodowej. Reakcja ukraińskich władz na te wypowiedzi mogła jednak dziwić. Wbrew naciskom postanowiły one złożyć w parlamencie projekt ustawy, który zakładał możliwość odwołania szefa NABU przez złożenie w parlamencie wniosku o wotum nieufności. Ostatecznie projekt nie trafił jednak pod obrady parlamentu. Zdaniem komentatorów prezydent Petro Poroszenko oraz inni najważniejsi politycy ukraińscy są niezadowoleni z tego, że NABU przy współpracy z FBI oraz innymi służbami jest instytucją niezależną, która dokonuje zatrzymań także wśród liczących się polityków lub osób z ich otoczenia (zatrzymano np. syna ministra spraw wewnętrznych)[43]. Komentatorzy podkreślają także, że z powodu nacisków Zachodu prezydent Poroszenko i jego partia nie zdecydują się na gwałtowne ruchy w sprawie zmian w NABU, jednak nie należy się spodziewać owocnej współpracy między NABU a aktualnie wybraną władzą[44].

Współpraca NABU z FBI wydaje się najważniejsza w kontekście rozwoju i dalszego funkcjonowania ukraińskiej służby. Trudno bowiem wyobrazić sobie niezależne funkcjonowanie Biura w realiach ukraińskich bez wsparcia zachodnich służb i organizacji. Współpraca ukraińsko-amerykańska nie jest jednak jedyną, jaką Biuro podjęło.

Kilka miesięcy od powstania Narodowe Antykorupcyjne Biuro Ukrainy rozpoczęło współpracę z jego polskim odpowiednikiem – Centralnym Biurem Antykorupcyjnym. Jak podano w depeszy Polskiej Agencji Prasowej[45], ówczesny premier Ukrainy Arsenij Jaceniuk zaprosił delegację CBA do złożenia wizyty na Ukrainie. Podkreślił, że jego kraj pragnie korzystać z doświadczenia polskiego Biura w walce z korupcją oraz że liczy

[43] T. Vorozkho, *FBI Says Its Support for Anti-corruption Unit Abides by Ukrainian Law*, https://www.voanews.com/a/federal-bureau-investigation-says-support-anti-corruption-unit-abides-by-ukrainian-law/4154225.html [dostęp: 25 VII 2018].

[44] J. Donati, *Feud Thwarts FBI-Backed Anticorruption Efforts in Ukraine*, https://www.wsj.com/articles/ukraine-law-enforcement-feud-threatens-anticorruption-efforts-1512649334 [dostęp: 25 VII 2018].

[45] *Ukraińcy chcą walczyć z korupcją. Będą się wzorować na polskim CBA*, https://wiadomosci.wp.pl/ukraincy-chca-walczyc-z-korupcja-beda-sie-wzorowac-na-polskim-cba-6025267491099265a [dostęp: 7 I 2018].

na pomoc CBA w wybraniu dla Ukrainy najlepszych środków antykorupcyjnych. Spotkanie polskiej delegacji z ukraińskimi władzami odbyło się w maju 2015 r.

Do podpisania oficjalnego memorandum o współpracy między NABU a CBA doszło w maju następnego roku w Warszawie. Było to pierwsze porozumienie zawarte przez ukraińskie Biuro z zagraniczną służbą antykorupcyjną. Podczas wizyty w Warszawie dyrektor NABU podkreślił, że ten wybór jest nieprzypadkowy, a kierowana przez niego instytucja analizowała doświadczenia w walce z korupcją także służb innych krajów, jednak zdecydowano się na skorzystanie z modelu polskiego, stosowanego od 10 lat. Poza podpisaniem dokumentu ustalono m.in. ramy współpracy dotyczącej działań dochodzeniowych, analitycznych, kontrolnych oraz operacyjnych w zakresie przeciwdziałania korupcji[46]. Kolejnym wydarzeniem zacieśniającym współpracę między organizacjami polską i ukraińską było podpisanie w październiku 2017 r. umowy o zapobieganiu zagrożeniom korupcyjnym. Miało to związek z udzieleniem przez polski rząd kredytu dla Ukrainy w wysokości 100 mln euro. Pieniądze mają zostać przeznaczone na uporządkowanie i poprawę infrastruktury przygranicznej po stronie ukraińskiej[47].

Poza służbami amerykańskimi i polskimi NABU podjęło współpracę z instytucjami innych państw. Współpraca ze służbami innych krajów prawdopodobnie nie jest jednak tak rozwinięta, jak z FBI i CBA. Ponadto należy zauważyć, że korupcja ani w Polsce, ani tym bardziej w USA, nigdy nie była na takim poziomie, jak na Ukrainie i nie wszystkie środki wykorzystywane przez polskie i amerykańskie służby w walce z nią mogą być adekwatne do sytuacji w tym kraju. Dyrektor NABU podjął również oficjalną współpracę ze Specjalną Służbą Śledczą Republiki Litewskiej[48] oraz Krajową Dyrekcją Antykorupcyjną Rumunii[49], czyli ze służbami krajów o wyższym wskaźniku poziomu korupcji niż w Polsce.

Pozornie egzotycznym kierunkiem współpracy, jaki ukraińskie Biuro wybrało w ostatnim czasie, jest współdziałanie z Hongkongiem i tamtejszą Niezależną Komisją Przeciw Korupcji. Ta ostatnia instytucja ma przede wszystkim duże doświadczenie, gdyż funkcjonuje od 1974 r., co może mieć dla strony ukraińskiej duży walor edukacyjny. Z pragmatycznego punktu widzenia należy jednak podkreślić, że zgodnie z wiedzą NABU to właśnie do Hongkongu trafiło 15 759 mln dolarów pochodzących z przestępstw korupcyjnych dokonanych na Ukrainie. Aktualnie jest opracowywane dwustronne memorandum na wzór porozumień podpisanych już przez NABU[50].

---

[46] *Memorandum o współpracy polskich i ukraińskich służb antykorupcyjnych*, Forsal.pl, 13 V 2016 r., http://forsal.pl/artykuly/943649,memorandum-o-wspolpracy-polskich-i-ukrainskich-sluzb-antykorupcyjnych.html [dostęp: 7 I 2018].

[47] *Umowa CBA i ukraińskiego NABU*, www.antykorupcja.gov.pl [dostęp: 7 I 2018].

[48] *NABU will strengthen cooperation with the Special Investigation Service of the Republic of Lithuania*, https://nabu.gov.ua/en/novyny/nabu-will-strengthen-cooperation-special-investigation-service-republic-lithuania [dostęp: 7 I 2018].

[49] *NABU and Romania's National Anticorruption Directorate agreed on cooperation and information exchange*, https://nabu.gov.ua/en/novyny/nabu-and-romanias-national-anticorruption-directorate-agreed-cooperation-and-information [dostęp: 7 I 2018].

[50] *NABU will strengthen cooperation with anti-corruption agencies of Hong Kong*, https://nabu.

Należy także odnotować, że NABU współpracuje nie tylko ze służbami innych państw, lecz także z organizacjami międzynarodowymi zajmującymi się walką z przestępczością. Jako jeden z priorytetów Biura określono jego współpracę z Europolem. Dało to możliwość tworzenia z tą instytucją wspólnych zespołów dochodzeniowo-śledczych do walki z przestępstwami transgranicznymi, co jest istotne w przypadku wyprowadzania poza Ukrainę środków pieniężnych, które zgodnie z wiedzą Biura trafiają do 41 krajów[51].

Wpływ działalności Narodowego Antykorupcyjnego Biura Ukrainy na bezpieczeństwo wewnętrzne Polski

Od początku funkcjonowania, tj. od 2015 r., NABU prowadziło 461 postępowań. Ich rezultatem było zatrzymanie 149 osób w związku z przestępstwami mającymi charakter korupcyjny, w których wyniku państwo ukraińskie straciło przeszło 3 mld dolarów. Jest to olbrzymia kwota dla pogrążonej w kryzysie Ukrainy, zważywszy na to, że niemal wszystkie wspomniane przestępstwa są dokonywane przez obywateli tego kraju[52].

Mimo że ukraińskie władze rażąco nieskutecznie prowadzą walkę z korupcją, to od zmian na tej płaszczyźnie będzie zależeć przyszłość Ukrainy. Ma to związek z polityką warunkowości, jaką państwa Zachodu stosują wobec tego kraju. Uzależnienie wypłaty kolejnych środków finansowych na pomoc w odbudowaniu państwa od reform – głównie w zakresie walki z korupcją – wydaje się jedynym skutecznym rozwiązaniem. Walka z patologią, jaką jest korupcja, jest dla Ukrainy jedyną szansą na wyjście z kryzysu. Brak zmian oznaczałby dalsze rozkradanie państwowego majątku przez rządzących, co w rezultacie, przy długotrwałym regresie gospodarczym, mogłoby doprowadzić do upadku tego kraju[53].

Bezpieczeństwo Ukrainy jest ściśle powiązane z bezpieczeństwem Polski. Ewentualne pogłębianie się kryzysu w tym kraju może mieć negatywne skutki dla bezpieczeństwa wewnętrznego państwa polskiego na co najmniej kilku płaszczyznach.

Rok 2017 był rekordowy, jeśli chodzi o ekspansję polskich przedsiębiorstw na Ukrainę. Zgodnie z danymi Głównego Urzędu Statystycznego, tylko w pierwszej połowie 2017 r. wyniósł on 8877 mln złotych, co w porównaniu z analogicznym okresem roku poprzedniego stanowi wzrost o 41 proc. Z raportu GUS wynika, że tendencja wzrostowa eksportu na Ukrainę jest widoczna od 2014 r., czyli od zmiany władzy w tym kraju. Nie można zatem nie zauważyć, że zbiegło się to z rozpoczęciem ukraińskich reform mających na celu przeciwdziałanie korupcji, co przełożyło się na zwiększenie zainteresowania tym krajem przez polskich przedsiębiorców[54].

---

gov.ua/en/novyny/nabu-will-strengthen-cooperation-anti-corruption-agencies-hong-kong [dostęp: 7 I 2018].

[51] *The NABU will cooperate with Europol while investigating cross-border corruption offenses*, https://nabu.gov.ua/en/novyny/nabu-will-cooperate-europol-while-investigating-cross-border-corruption-offenses [dostęp: 7 I 2018].

[52] Zob. www.nabu.gov.ua [dostęp: 7 I 2018].

[53] P. Kościński, *Problem korupcji na Ukrainie*…

[54] *Polska wraca na Ukrainę w wielkim stylu. Eksport wystrzelił*, https://businessinsider.com.pl/

Marcin Lis, redaktor serwisu Money.pl, podał informację, że do końca 2017 r. legalne zatrudnienie znalazły w Polsce 2 mln obywateli Ukrainy, natomiast do końca 2018 r. ta liczba wyniesie około 3 mln[55]. Pośrednią przyczyną tak dużej migracji jest korupcja, która hamuje rozwój państwa i zmusza jego obywateli do szukania pracy za granicą. M. Lis jest zdania, że z punktu widzenia polskiej gospodarki jest to informacja pozytywna. Zauważa jednak, że wraz z napływem tak dużej liczby Ukraińców do Polski pojawia się problem tzw. szarej strefy, czyli nielegalnego zatrudnienia, co niesie zagrożenie bezpieczeństwa ekonomicznego państwa[56]. Przypływ ogromnej liczby obywateli Ukrainy w stosunkowo krótkim okresie zwiększył ryzyko przestępstw dokonywanych przez imigrantów. Należy odnotować, że obywatele Ukrainy coraz częściej dopuszczają się na terytorium Polski przestępstw zagrażających finansom państwa, polegających głównie na wyłudzaniu podatku VAT[57].

Mając na uwadze znaczenie Ukrainy jako dużego kraju pogrążonego w kryzysie, znajdującego się w bezpośrednim sąsiedztwie Polski, należy stwierdzić, że jego przyszłość jest związana z bezpieczeństwem naszego państwa. Powiązania ekonomiczne, liczba obywateli Ukrainy oraz geopolityczne znaczenie tego kraju determinują jego wspieranie w reformach zmierzających do poprawy panującej tam sytuacji. Ponieważ Narodowe Antykorupcyjne Biuro Ukrainy jest aktualnie jedyną niezależną służbą, która może mieć realny wpływ na walkę z korupcją w tym kraju, służby państw Zachodu powinny wspierać tę instytucję. Poza pomocą finansową zachodnie instytucje powinny wpływać przede wszystkim na ukraińskich polityków, którzy wydają się największym problemem w tej walce.

Dzięki wnikliwej analizie materiałów źródłowych udało się potwierdzić tezę, że jakość funkcjonowania NABU jest uzależniona od jego współpracy ze służbami państw zachodnich, a skutek tej współpracy ma bezpośrednie przełożenie na poziom bezpieczeństwa na Ukrainie, co pośrednio wpływa także na bezpieczeństwo wewnętrzne Polski.

Bibliografia:

Barcikowski A., *Bezpieczeństwo wewnętrzne – różne perspektywy analityczne i doktrynalne*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 11, s. 11–21.

Chybiński O., *Płatna protekcja*, Warszawa 1967, Wydawnictwo Prawnicze.

finanse/handel/polski-eksport-na-ukraine-styczen-czerwiec-2017/3gws758 [dostęp: 7 I 2018].

[55] *Za rok w Polsce będzie pracować 3 mln Ukraińców. Ich pensje rosną szybciej niż przeciętne*, https://www.money.pl/gospodarka/unia-europejska/wiadomosci/artykul/ukraincy-pracujacy-w-polsce-pensja-liczba,118,0,2381430.html [dostęp: 7 I 2018].

[56] J. Fryc, *Prezes Forte: Brakuje rąk do pracy, a problem pogłębia szara strefa*, https://businessinsider.com.pl/gielda/wiadomosci/produkcja-mebli-w-polsce-maciej-formanowicz-prezes-forte/nssn1kq [dostęp: 7 I 2018].

[57] *Handel lewymi fakturami*, http://www.antykorupcja.gov.pl/ak/aktualnosci/12627,Handel-lewymi-fakturami-60-mln-strat-skarbu-panstwa.html [dostęp: 7 I 2018].

Czech M., *Kres zbliżenia Ukrainy z Europą: Janukowycz wywrócił stolik*, „Gazeta Wyborcza" z 22 listopada 2013 r.

Czech M., *Rosja bez Ukrainy jak bez ręki. Plan przezbrojenia armii poważnie zagrożony*, „Gazeta Wyborcza" z 23 czerwca 2014 r.

Głowacki W., *Rok w którym Europa osiwiała*, „Polska The Times" z 21 listopada 2014 r.

Jarosz M., *Władza, przywileje, korupcja*, Warszawa 2004, Wydawnictwo Naukowe PWN.

Krajowe Biuro Antykorupcyjne Ukrainy, „Przegląd Antykorupcyjny" 2016, nr 1, s. 220–225.

Kwiatkowska K., *Mustafa odbije Ukrainę*, „Gazeta Wyborcza" z 29 listopada 2013 r.

Marson J., *Corruption Battle Roils Ukraine*, „The Wall Steer Journal" z 12 września 2017 r.

Przybyła K., *NATO wobec konfliktu na Ukrainie,* „Bezpieczeństwo Narodowe" 2016, nr 37–40, s. 117–131.

Shevliakov I., *Ukraine*, w: *Anti-Corruption in Moldova and Ukraine*, A. Sobják (ed.), Warsaw 2015, s. 27–37.

Sulowski P., *Korupcja zagrożeniem dla bezpieczeństwa wewnętrznego państwa*, „Annales Universitatis Paedagogicae Cracoviensis. Studia Politologica" 2012, nr 8, s. 57–81.

Szwejkowski Ł., *Korupcja, wybrane zagadnienia*, seria „Materiały dydaktyczne", nr 87, Legionowo 2013, Centrum Szkolenia Policji.

Weisman J., *Congress Approves Aid of $1 Billion for Ukraine,* „The New York Times" z 27 marca 2014 r.

Źródła internetowe:

www.112.international

www.antykorupcja.gov.pl

www.abw.gov.pl

www.bbc.co.uk

www.businessinsider.com.pl

www.cbsnews.com

www.euromaidanpress.com

www.interfax.com

www.kyivpost.com

www.nabu.gov.ua

www.transparency.org

www.pap.pl

www.pism.pl

www.reuters.com

www.voanews.com

www.wiadomosci.wp.pl

www.wsj.com

www.zakon4.rada.gov.ua

www.zik.ua

Abstrakt

Wydarzenia związane z tzw. Euromajdanem doprowadziły do zmiany władzy na Ukrainie, a w konsekwencji – do zwrócenia się tego kraju w kierunku zachodnim. Nowo wybrane władze zostały zmuszone do podjęcia działań mających na celu uporanie się z problemem, jakim jest korupcja. Był to warunek otrzymania przez Ukrainę pomocy z Unii Europejskiej i Stanów Zjednoczonych. Korupcja jest jednym z głównych powodów stagnacji tego państwa. W 2014 r. utworzono na Ukrainie struktury wyznaczone do walki z korupcją, m.in. Narodowe Antykorupcyjne Biuro Ukrainy. NABU to jedyny niezależny organ działający na terenie państwa ukraińskiego zwalczającą korupcję. Destabilizacja Ukrainy będąca rezultatem łamania prawa przez najwyższej rangi polityków i urzędników niesie za sobą konsekwencje także dla Polski jako jej zachodniego sąsiada oraz dla całego regionu Europy Środkowo-Wschodniej. Spadek bezpieczeństwa na Ukrainie skutkuje m.in. emigracją obywateli tego kraju, głównie do Polski, co przekłada się bezpośrednio na jej bezpieczeństwo wewnętrzne. Wspieranie działalności NABU w walce z korupcją na Ukrainie leży w interesie zarówno Unii Europejskiej, jak i Stanów Zjednoczonych.

Słowa kluczowe: korupcja, bezpieczeństwo wewnętrzne, Polska, Ukraina, służby specjalne.

Krzysztof Izak

Co po Islamskim Państwie Kalifatu? Stan obecny i kierunki rozwoju zagrożeń terrorystycznych

Na wstępie wyjaśnienia wymaga użyta w tytule nazwa „Islamskie Państwo Kalifatu", która może wydawać się nielogiczna lub wręcz błędna od strony semantycznej, jednak jest jak najbardziej właściwa. Jest to jedno z określeń widniejące na dokumentach osobistych, administracyjnych i wojskowych Państwa Islamskiego. W dniu 29 czerwca 2014 r. organizacja Dawlat al-Islamijja fi al-Irak wa asz-Szam – Daisz, (Islamic State of Iraq and Lewant/Szam, ISIL/ISIS, Islamskie Państwo w Iraku i Lewancie) proklamowało utworzenie samozwańczego kalifatu. Od tej pory przestała obowiązywać nazwa Dawlat al-Islamijja fi al-Irak wa asz-Szam, a zamiast niej wprowadzono nazwę Ad-Dawla al-Islamijja (Islamic State, IS, Państwo Islamskie) bez geograficznych odniesień. W ten sposób pojawiły się dwie struktury noszące nazwę „Państwo Islamskie". Jedną była organizacja, drugą – państwo. Mimo to, jakby dla zminimalizowania znaczenia tego wydarzenia i jego następstw, dziennikarze i politycy wciąż używali i nadal stosują akronimy nazwy organizacji sprzed 29 czerwca 2014 r. Po umocnieniu się administracji na szczeblu centralnym i lokalnym (w prowincjach) Państwo Islamskie wydawało tysiące dokumentów. W nagłówkach umieszczano arabski lub angielski napis „Państwo Islamskie" lub „Kalifat", czasami pojawiała się nazwa „Kalifat Państwa Islamskiego" lub „Islamskie Państwo Kalifatu". Ta ostatnia nazwa znalazła się na przykład na paszportach samozwańczego państwa, określanego w literaturze jako „protopaństwo", ponieważ powstałą i rozbudowującą się strukturę polityczno-terytorialną trudno nazwać innym określeniem[1].

W połowie października 2017 r. Syrian Democratic Forces, SDF (Syryjskie Siły Demokratyczne) zdobyły we wschodniej Syrii Ar-Rakkę, stolicę kalifatu. Szturm poprzedziły wielotygodniowe bombardowania, które znacznie osłabiły morale bojowników IS oraz ich zdolności operacyjne. Mimo zapowiedzi polityków i wojskowych państw zachodnich dotyczących zlikwidowania terrorystów w Syrii, kilkuset bojowników opuściło wraz z rodzinami Ar-Rakkę. Zostali oni ewakuowani na mocy tajnego porozumienia zawartego z dowództwem SDF, co pozwoliło zmniejszyć liczbę ofiar zarówno wśród walczących ze sobą stron konfliktu, jak i wśród ludności cywilnej. Z miasta wyjechał kilkukilometrowy konwój pojazdów, z których część podstawili Kurdowie stanowiący trzon SDF. Na samochodach ciężarowych znajdowała się broń, w tym ciężka, oraz duże ilości amunicji i materiałów wybuchowych. Nad konwojem nie powiewały czarne flagi Państwa Islamskiego, dlatego też nie był on atakowany przez samoloty czy przy użyy-

[1] Za nazwaniem reaktywowanego kalifatu „protopaństwem", a nie państwem z przynależnymi mu atrybutami, optuje m.in. A. Wejkszner. Autor wymienia czynniki przemawiające za stosowaniem takiej właśnie terminologii wobec Państwa Islamskiego oraz innych dżihadystycznych protopaństw utworzonych od 1989 r. w świecie muzułmańskim przez różne islamskie organizacje ekstremistyczne. Zob. tenże, *Państwo Islamskie. Narodziny nowego kalifatu?*, Warszawa 2016, s. 41–49.

ciu dronów. Trudno jednak przypuszczać, aby o zdarzeniu nie wiedziało dowództwo sił amerykańskich oraz ich sojusznicy prowadzących operacje powietrzne i specjalne na terenie Syrii. Konwój kierował się do Deir az-Zaur, miasta znajdującego się wówczas pod panowaniem IS (siły syryjskie przejęły je dopiero na początku listopada, ale bojownicy IS kontrolowali jeszcze zachodnią część irackiej prowincji Al-Anbar z miastami Rawa i Al-Kaim). Podobno kilka dni po opuszczeniu Ar-Rakki przez bojowników IS rozpoczęła się obława na uciekinierów. Ta zwłoka wystarczyła, aby rozpierzchli się oni po terenie i próbowali przekroczyć granicę z Turcją. Przemytnicy za przerzut za granicę żądali 600 USD od osoby lub co najmniej 1500 USD od rodziny. Część uciekinierów dostała się w ręce tureckich służb bezpieczeństwa, które wcześniej przymykały oczy na przekraczanie granicy przez *foreign fighters* w przeciwnym kierunku. Teraz bojownicy usiłowali skorzystać z zamieszania i przez Turcję dostać się do krajów swojego zamieszkania w Europie. Nigdy chyba się nie dowiemy, ilu dokładnie bojownikom to się udało. Ale wędrówki ochotników dżihadu do i z Syrii oraz Iraku odbywały się od 2012 r. Według amerykańskiego ośrodka analitycznego The Soufan Center (TSC) od tego czasu w walkach uczestniczyło ok. 40 tys. ochotników niebędących obywatelami Syrii i Iraku oraz państw sąsiednich. Byli to obywatele ponad 100 krajów świata (inne źródła określają tę liczbę na ponad 80). Najwięcej ochotników pochodziło z Tunezji (ponad 6 tys.). W przypadku Europy oddziały kalifatu zasiliło najwięcej bojowników z Federacji Rosyjskiej (prawie 3,5 tys.), następnie z: Francji (ponad 2 tys.), Wielkiej Brytanii i Niemiec (po ok. 1 tys.), Belgii (ok. 500) i Szwecji (ponad 300). Po kilkuset bojowników wyjechało także z Albanii, Bośni, Danii, Hiszpanii i Holandii[2]. Według różnych źródeł w walkach na terenie Syrii i Iraku mogło uczestniczyć łącznie od 100 do 120 tys. dzihadystów. Już w sierpniu 2014 r. szacowano, że IS zrzeszało 80 tys. bojowników, w tym 50 tys. walczących w Syrii i 30 tys. w Iraku. Natomiast według gen. Walerija Gierasimowa, dowódcy rosyjskiej armii, IS dysponowało dobrze dowodzoną i zorganizowaną armią. Na jej czele stali byli oficerowie armii irackiej, a wielu bojowników i dowódców zostało przeszkolonych przez instruktorów z krajów Bliskiego Wschodu. Państwo Islamskie miało ok. 59 tys. ludzi pod bronią, w tym ok. 2800 pochodzących z Rosji, 1500 czołgów i 1200 dział, a sposób działania i taktyka pokazywały, że była to regularna armia, a nie grupa terrorystów. Teraz wracają oni do domów, w większości do Libii, Afganistanu i Azji Południowo-Wschodniej[3]. Znana jest tożsamość ok. 20 osób powiązanych z Polską – obywateli Polski, polskiej narodowości zamieszkałych za granicą oraz cudzoziemców posiadających prawo pobytu w Polsce, którzy przebywali dłuższy lub krótszy czas w strefie konfliktu lub w inny sposób wspierali IS.

W marcu 2016 r. stacja Sky News przekazała informację o posiadaniu karty pamięci zawierającej dane ponad 22 tys. dżihadystów z Państwa Islamskiego. Otrzymała ją od niejakiego Abu Hamida, który wstąpił najpierw do Wolnej Armii Syryjskiej, a następnie do IS. Kartę ukradł Abu Lukmanowi as-Suriemu, szefowi służby wywiadu i bezpieczeń-

[2] http://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf [dostęp: 29 X 2017].

[3] https://wiadomosci.wp.pl/rosyjska-armia-jest-coraz-bardziej-niebezpieczna-to-juz-nie-sa-uprzejme-zielone-ludziki-6203212097816193a [dostęp: 28 XII 2017].

stwa tej organizacji. Z tym łupem zbiegł do Turcji. Na karcie pamięci znajdują się formularze zgłoszeniowe zawierające 23 pytania. Poza imieniem i nazwiskiem kandydaci wpisywali tam m.in. swoje numery telefonów, a także informacje o własnej rodzinie, wykształceniu i doświadczeniu bojowym, a także zakres swej wiedzy na temat szariatu. Podawali również, kto rekomendował ich do Państwa Islamskiego. W formularzu można było także zadeklarować gotowość do wzięcia udziału w szkoleniu na zamachowca samobójcę. Według Sky News część z ujawnionych nazwisk była już wcześniej znana służbom specjalnym, ale nowe dokumenty mogą pomóc w zidentyfikowaniu ekstremistów, o których działalności władze ich krajów dotychczas nie wiedziały. Formularze były wypełnione przez ochotników z 51 państw, w tym z Wielkiej Brytanii, kilku krajów Europy Północnej, USA, Kanady oraz państw Afryki Północnej i Bliskiego Wschodu. O przecieku tajnych danych personalnych bojowników IS poinformował również dziennik „Süddeutsche Zeitung", twierdząc, że wraz z niemieckimi regionalnymi telewizjami publicznymi NDR i WDR uzyskał wgląd w kilkadziesiąt formularzy z danymi na temat niemieckich dżihadystów. Formularze wypełniano przy wjeździe na tereny Syrii opanowane przez IS. Przedstawiciele niemieckich służb poinformowali, że pozyskane dokumenty dotyczą również znanych im obywateli Niemiec, którzy nie zostali osądzeni, ponieważ brakowało dowodów na ich udział w IS. Dokumenty zagranicznych obrońców kalifatu nie zawierały fotografii, w odróżnieniu od formularzy wypełnianych przez miejscowych bojowników pochodzących z Syrii i Iraku.

Według danych European Counter Terrorism Centre, ECTC (Europejskiego Centrum Antyterrorystycznego) z końca czerwca 2017 r. w szeregi Państwa Islamskiego w Iraku i Syrii zaciągnęło się ok. 5 tys. mieszkańców państw UE (inne źródła wskazują liczbę ponad 6 tys. osób), 1650 z nich powróciło do Europy, chociaż te powroty są mniej liczne niż przewidywano. Znaczna część spośród osób powracających do Europy została, według ECTC, zatrzymana bądź jest kontrolowana w krajach, do których przybyli. Wskazano też na konieczność bardzo uważnego śledzenia nie tylko przepływu terrorystów (zaobserwowano również zwiększenie napływu terrorystów do zdestabilizowanych krajów, jak Libia, Somalia i Jemen[4]), lecz także werbowania przez organizacje terrorystyczne kobiet i nieletnich (wzrost ich liczby zaobserwowano w 2017 r.).

Bieżąca sytuacja przypomina tę z przełomu lat 80. i 90. XX w., gdy po zakończeniu wojny w Afganistanie mudżahedini znaleźli się z powrotem w ojczystych krajach (w Afganistanie w latach 80. walczyło ok. 20 tys. cudzoziemców). Zasilili oni wówczas istniejące już radykalne organizacje lub tworzyli nowe i stawali na ich czele. Przykładem takich organizacji są: Abu Sajaf na Filipinach, Dżimah Islamija w Indonezji, Laszkar-e Taiba w Pakistanie, Al-Dżama'at at-Tawhid wa al-Dżihad w Jordanii, Al-Dżama'a al-Islamijja al-Mukatila bi Libija w Libii, Al-Dżama'a al-Islamijja al-Mukatila fi Tunisija w Tunezji oraz Al-Dżama'a al-Islamijja al-Musallaha w Algierii. Wielu afgańskich weteranów walczyło podczas wojny w Bośni i Hercegowinie w latach

[4] https://businessinsider.com.pl/wiadomosci/dzihadysci-w-europie-ilu-wrocilo/ldczlxw [dostęp: 30 VI 2017].

1992–1995 (w wojnie brało udział od 2 do 5 tys. cudzoziemców), a po jej zakończeniu uzyskali oni obywatelstwo tego kraju. Afgańscy weterani brali również udział w krwawej wojnie domowej w Algierii, która wybuchła w 1992 r. i toczyła się niemal do końca lat 90., a jednym z jej skutków było powstanie filii Al-Kaidy w północnej Afryce. O ile bojownicy powracający z Afganistanu do krajów zamieszkania byli witani jak bohaterowie, o tyle *foreign fighters* wracający obecnie z Syrii muszą liczyć się z możliwością aresztowania i postawienia przed sądem za członkostwo w organizacjach terrorystycznych o charakterze zbrojnym i dokonywanie masowych morderstw.

Czasy się zmieniły sytuacja międzynarodowa również, a zagrożenie terrorystyczne, zainicjowane przed laty przez afgańskich weteranów, stało się obecnie niewspółmiernie wysokie w porównaniu do tego sprzed kilkudziesięciu czy nawet kilkunastu lat. Między innymi z tego powodu w państwach UE toczy się spór o powracających dżihadystów. Zamiar ich zlikwidowania jeszcze w Syrii okazał się utopią. CIA stosowała ataki z powietrza i skutecznie prowadziła selektywną eliminację członków Al-Kaidy i związanych z nią organizacji. Dla walczących z Państwem Islamskim nie było to już takie proste. Brytyjski minister obrony zdecydował o zintensyfikowaniu ataków lotniczych w celu wyeliminowania obywateli brytyjskich walczących po stronie organizacji terrorystycznych. Na pytanie, czy nie uważa, że część obywateli brytyjskich powinna móc wrócić do domów, minister odpowiedział, że nie ufa żadnym terrorystom. Nie ma dla niego znaczenia, czy dana osoba pochodzi z Wielkiej Brytanii, czy z innego kraju. Zdaniem ministra jedynie martwy terrorysta nie może zaszkodzić krajowi, w związku z czym żaden z brytyjskich dżihadystów nie ma prawa powrotu do kraju. Współpraca z nimi jest równoznaczna z wydaniem wyroku śmierci na obywateli. Na wyspach pojawiły się głosy, aby wpuścić do kraju osoby przyznające się do współpracy z dżihadystami i wyrażające skruchę. Część Brytyjczyków uważa, że powinny one być osądzone za swoje czyny. Zamiast wyroków śmierci państwo powinno zająć się ich reintegracją[5]. Jednak według opinii innych reintegracja takich ludzi ze społeczeństwami w krajach zamieszkania jest marnowaniem pieniędzy podatników, ponieważ nie ma wielkiej nadziei na ich powrót do normalnego życia. Na temat wątpliwej skuteczności programów deradykalizacyjnych prowadzonych w UE autor pisał już w „Przeglądzie Bezpieczeństwa Wewnęrznego" w artykule zatytułowanym *Ograniczenia i problemy z zwalczaniu terroryzmu i przestępczości imigrantów w Europie*[6].

Nie brakuje też głosów przeciwnych. Według analizy statystycznej norweskiego eksperta Thomasa Hegghammera, ok. 11 proc. osób powracających z dżihadu stanowi zagrożenie terrorystyczne. Ale w przypadku wojny w Syrii, ta liczba jest znacznie mniejsza i wynosi ok. 0,5 proc. Jak dowodzi Charles Lister, ekspert think tanku Brookings, jeśli te szacunki są prawidłowe, to „miękkie podejście" ma większy sens, niż nacisk na zamykanie powracających bojowników do więzień, gdzie mogą ponownie się zradykalizować

[5] http://wolnosc24.pl/2017/12/07/brytyjski-rzad-kazal-wyeliminowac-wlasnych-obywateli-podejrzanych-o-kontakty-z-isis-licencja-na-zabijanie-szokujace-wyznanie-ministra/ [dostęp: 7 XII 2017].

[6] „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 104–137.

i przy okazji zaszczepić ekstremistyczne idee współwięźniom. Programy resocjalizacyjne są prowadzone w kilku krajach Europy, w tym w Niemczech, Holandii i Danii. Podobno część z nich przynosi pozytywne rezultaty, np. w Danii stosuje się „metodę z Aarhus" polegającą na współpracy z lokalnymi meczetami oraz udzielaniu pomocy w znalezieniu pracy i zapewnieniu edukacji. W rezultacie żaden z 16 dżihadystów z Aarhus, którzy od 2013 r. wyjechali do Syrii, a następnie wrócili, nie popełnił dotychczas poważnego przestępstwa i niemal wszyscy mają zatrudnienie lub chodzą do szkoły[7]. Ale to tylko jeden przykład, podczas gdy statystyki dotyczące podobnych programów w innych krajach nie są znane. Tymczasem nawet jeśli spośród 1600 bojowników reemigrujących do krajów UE znajdzie się kilku recydywistów, konsekwencje będą ogromne. Jeszcze z większym zagrożeniem należy się liczyć, biorąc pod uwagę bojowników wracających do krajów spoza UE. Ośrodek TSC opierając się na raportach z 33 państw, ocenił, że między marcem 2016 r. a sierpniem 2017 r. do tych krajów przybyło co najmniej 5600 dżihadystów, m.in. 400 do Rosji, 760 do Arabii Saudyjskiej, 800 do Tunezji i 800 do Turcji. Dlatego większość państw woli stawiać na twarde metody radzenia sobie z problemem, nawet jeśli brakuje dowodów pozwalających na umieszczenie w więzieniach powracających radykałów. W Wielkiej Brytanii takim rozwiązaniem są tzw. TPIMs (Terrorism Preventrion and Investigation Measures) wprowadzone na mocy ustawy w 2011 r., czyli objęcie podejrzanych szczególnym nadzorem. Wedle przepisów władze mogą monitorować działalność tych osób np. za pomocą elektronicznych obrączek i przez nałożenie na nich obowiązku stawiania się w komendzie policji. Problem w tym, że biorąc pod uwagę liczbę ekstremistów, którzy są znani służbom, oraz stałe braki kadrowe wśród służb prowadzących nadzór nad radykałami, także i to podejście nie jest stuprocentowo skuteczne. W Niemczech w 2017 r. kilkakrotnie wzrosła liczba prokuratorskich śledztw związanych z terroryzmem. Wiele z nich dotyczy obywateli Niemiec powracających z Syrii i Iraku. W rezultacie śledczy są przepracowani, a prokuraturze brakuje rąk do pracy. Dlatego proponuje się też inne podejście, a mianowicie pozostawienie w spokoju przynajmniej części powracających do kraju dżihadystów, zwłaszcza tych, którzy wyjechali z naiwności jako nastolatkowie, być może po intensywnym namawianiu, i teraz wracają z poczuciem całkowitego rozczarowania. Tego typu strategię stosuje brytyjski kontrwywiad MI5[8]. Czy jest ona słuszna, pokaże z pewnością niedaleka przyszłość. Francuskie służby poinformowały, że w kraju przebywają już dzieci urodzone na terenach opanowanych przez IS oraz te, które z matkami opuściły Francję w wieku kilku lat. Są one naznaczone traumą wojny, zdarzało się, że czasami były wykorzystywane w działaniach propagandowych, przeszły przeszkolenie w posługiwaniu się bronią, zostały zindoktrynowane, przypatrywały się egzekucjom i same je wykonywały. Filmy z tego rodzaju scenami były umieszczane w cyberprzestrzeni.

[7] http://trybun.org.pl/2017/08/10/dania-w-miejscowosci-aarhus-rusza-program-przytul-terroryste/ [dostęp: 10 VIII 2017].

[8] http://www.bbc.com/news/world-middle-east-41734069 [dostęp: 26 X 2017]; https://wiadomosci.wp.pl/ dzihadysci-wracaja-do-europy-nie-wiadomo-co-z-nimi-zrobic-6180903806875777a [dostęp: 26 X 2017]; https://wiadomosci.wp.pl/czy-terrorysci-moga-byc-resocjalizowani-wielki-spor-o-powracajacych-dzihadystow 6193366738753665a [dostęp: 30 XI 2017].

Obecność w Europie dżihadystów z Państwa Islamskiego stanowi terrorystyczne zagrożenie dla mieszkańców całego kontynentu. Terroryzm będzie narastać wraz z napływem uchodźców i nielegalnych imigrantów nie tylko z Azji, lecz także z państw Afryki. Mimo upadku struktur administracyjnych i zniszczenia sił wojskowych organizacji oraz odzyskania kontroli nad zajmowanymi przez nią terytoriami w Iraku i Syrii, przyszłość obu tych państw stoi pod wielkim znakiem zapytania. W dniu 9 grudnia 2017 r. iracki premier Hajdar al-Abadi ogłosił zwycięstwo nad IS. Był to już kolejny komunikat premiera o pokonaniu tej organizacji. Takie komunikaty pojawiały się kilkakrotnie: po odbiciu z rąk dżihadystów Mosulu, Tel Afar oraz Hawidży, ale walki wciąż trwały. Ostatnia operacja sił irackich w zachodniej części prowincji Al-Anbar oznacza klęskę kalifatu w Iraku, gdyż spowodowała odcięcie oddziałów IS. Zdobywanie pozycji zajmowanych przez dżihadystów wzdłuż syryjsko-irackiej granicy było elementem oczyszczania z IS terytorium prowincji – ostatniej kontrolowanej w Iraku przez tę organizację. Walki w Iraku przyniosły olbrzymie straty. Tylko podczas operacji odbijania Mosulu, trwającej od października 2016 r. do lipca 2017 r., zginęło 23 tys. irackich żołnierzy, a liczba rannych trzykrotnie przekroczyła liczbę zabitych. Życie straciło od 9 do 11 tys. cywilów, straty materialne zaś wyniosły 3 mld USD. Do tego należy doliczyć tony zużytej amunicji oraz tysiące zniszczonej broni i pojazdów[9].

Zwycięstwo militarne nad Państwem Islamskim w bitwie nie oznacza pokonania tej organizacji. Wielu wyższych rangą bojowników i szeregowych żołnierzy przeżyło ostatnie 18 miesięcy walk, w których wyniku utracono prawie całe kontrolowane wcześniej terytorium (w walkach mogło zginąć od 60 do 70 tys. bojowników kalifatu). Najprawdopodobniej członkowie IS przejdą do konspiracji i nadal będą dokonywać ataków. Z pewnością kalifat miał swoich zwolenników wśród mieszkańców odbitych miast, a przede wszystkim wśród byłych oficerów armii irackiej oraz służb wywiadu i bezpieczeństwa z okresu Saddama Husajna. To dzięki nim bojownicy IS odnosili spektakularne zwycięstwa. Bojownicy mają również wielu sympatyków wśród sunnickiej mniejszości w Iraku, mogą zatem liczyć na ich wsparcie i pomoc w kontynuowaniu podziemnej działalności. Przejawem ich aktywności są ataki terrorystyczne organizowane w miastach i dzielnicach zdominowanych przez szyitów. I właśnie ten konflikt sunnicko-szyicki, co prawda o mniejszym natężeniu, ale jednak niosący za sobą wiele zniszczeń i ofiar, naznaczy najbliższą przyszłość tego państwa.

W Syrii sytuacja jest bardziej skomplikowana. Tu oprócz wojsk reżimowych niezwykle aktywne są siły SDF na czele z Kurdami. Ich przeciwnikami są nie tylko bojownicy IS, lecz także Harakat Ahrar asz-Szam al-Islamijja (Islamski Ruch Wolnego Lewantu) i sprzymierzone z nim organizacje oraz Hajat Tahrir asz-Szam (Organizacja Wyzwolenia Lewantu, OWL), czyli dawny Dżabhat an-Nusra li Ahl asz-Szam (Front Obrony Ludu Syryjskiego)[10]. Te dwie organizacje, walczące kiedyś wspólnie przeciw-

[9] http://gpcodziennie.pl/77109-ogromstratwwalceomosul.html [dostęp: 27 XII 2017].

[10] Dawny Dżabhat an-Nusra li Ahl asz-Szam (Front Obrony Ludu Syryjskiego), późniejszy Dżabhat Fateh asz-Szam (Front Podboju Lewantu), będący syryjską filią Al-Kaidy, z którą rzekomo zerwał związki i po połączeniu się z mniejszymi ugrupowaniami 28 stycznia 2017 r. zmienił nazwę

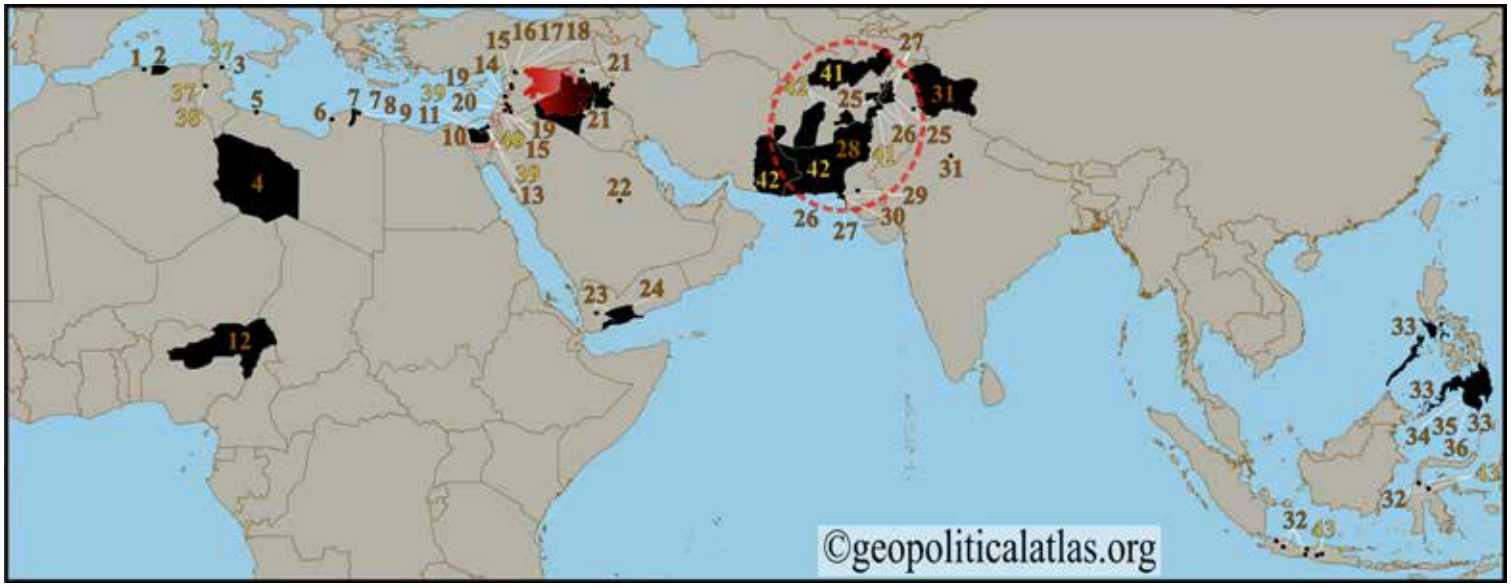
ko siłom reżimowym i Państwa Islamskiego, w ciągu ostatniego roku toczyły między sobą walki, przerywane rozmowami, rozejmami lub prowadzonymi razem operacjami w przypadku pojawienia się zagrożenia ze strony wspólnego wroga. Organizacja Wyzwolenia Lewantu wciąż kontroluje niektóre obszary prowincji Idlib i Hama, bombardowane przez siły rządowe. Do wymienionych ugrupowań należy zaliczyć jeszcze inne, mniejsze, walczące w ostatnich latach w Syrii, tworzące mniej lub bardziej trwałe sojusze. Często pod przykrywką religijnej lub nacjonalistycznej ideologii kryły się zwykłe bandyckie działania. Liczbę tych wszystkich organizacji i grup zbrojnych aktywnych w Syrii i Iraku od 2012 r. szacuje się na 300–800. Tylko w lutym 2016 r. prawie 100 ugrupowań wchodzących w skład Wolnej Armii Syryjskiej i tzw. zbrojnej opozycji zgodziło się na amerykańsko-rosyjskie porozumienie o zawieszeniu broni, niedługo potem zerwane[11]. Trudno zatem uznać, że likwidacja IS w Syrii przyniesie spokój temu krajowi. Podziały etniczno-religijne oraz sprzeczne interesy Rosji, USA i państw zachodnich będą sprzyjały podsycaniu wewnętrznych konfliktów i destabilizacji państwa oraz jego terytorialnemu rozbiciu.

Wciąż aktywne są organizacje sprzymierzone z Państwem Islamskim operujące w zagranicznych wilajetach (prowincjach) kalifatu: na Półwyspie Synaj, w Libii, Nigerii czy Afganistanie. Działają również ugrupowania, których przywódcy w latach 2014–2015 złożyli przysięgę lojalności kalifowi Ibrahimowi (Abu Bakrowi al-Bagdadiemu)[12], a wcześniej były związane z Al-Kaidą lub tworzyły jej filie. Takich organizacji było łącznie ponad 40. Część z nich podzieliła się na skutek wewnętrznych sporów dotyczących opowiedzenia się po stronie Al-Kaidy lub ISIS/IS, skonfliktowanych ze sobą od 2013 r. Ta zmiana sojuszy była początkowo mało czytelna. Dopiero analiza informacji zamieszczanych przez poszczególne ugrupowania w cyberprzestrzeni pozwoliła na identyfikację organizacji, które „zdradziły" Al-Kaidę (zob. mapa 1 i wykaz organizacji). Warto wspomnieć, że na początku września 2014 r. Ajman az-Zawahiri ogłosił powstanie Al-Dżama'at Kaidat al-Dżihad al-Karrah al-Hindijah (Wspólnota Bazy Dżihadu Subkontynentu Indyjskiego). Miesiąc potem grupa Al-Ansar-ut Tauhid fi Bilad al-Hind (Zwolennicy Jedności Boga w Indiach) opublikowała oficjalne oświadczenie, w którym zadeklarowała lojalność wobec Państwa Islamskiego. Wezwała również do ataków na przebywających w Indiach obywateli państw zachodnich. Zamachy miały być odwetem za działania międzynarodowej koalicji przeciwko Państwu Islamskiemu.

na Organizację Wyzwolenie Lewantu, zob. M. Weiss, H. Hassan*, ISIS. Wewnątrz armii terroru*, Warszawa 2015, s. 281–326; https://alshahidwitness.com/ identifying-hts-syria-revolution/ [dostęp: 6 VI 2017].

[11] https://www.polskieradio.pl/5/3/Artykul/1587568,Syria-100-ugrupowan-opozycji-przystapi-do-rozejmu [dostęp: 26 II 2016].

[12] Więcej na temat kalifa Ibrahima zob. S. Laurent, E. Kaniowska, *Kalifat terroru. Kulisy działania Państwa Islamskiego*, Warszawa 2015, s. 109–125; J. Warrick, *Czarne flagi. Geneza Państwa Islamskiego*, Warszawa 2017, s. 356–377.



Mapa 1. Muzułmańskie organizacje ekstremistyczne sprzymierzone z Państwem Islamskim (poniżej zamieszczono wykaz organizacji zaznaczonych na mapie).

Źródło: https://intelcenter.com/maps/is-affiliates-map.html#gs.mm1jPv0 [dostęp: 4 III 2016].

Legenda:

- Obszary kontrolowane przez Państwo Islamskie Iraku i Lewantu (ISIS)
- 37 — Obszary, na których działają oddziały Państwa Islamskiego
- 1 — Grupy deklarujące sojusz z Państwem Islamskim
- Grupy deklarujące wsparcie dla Państwa Islamskiego
- Sojusze strategiczne, taktyczne i polityczne

Wykaz organizacji zaznaczonych na mapie

Obok nazwy organizacji podano datę złożenia przysięgi lojalności (arab. *baja*) wobec kalifa Abu Bakra al-Bagdadiego lub datę jej ogłoszenia – źródło: https://intelcenter.com/maps/is-affiliates-map.html#gs.mm1jPv0 [dostęp: 4 III 2016].

SOJUSZE IDEOLOGICZNE I MARKETINGOWE

Grupy deklarujące sojusz – data

1. Kataib al-Huda bi al-Maghrib al-Islami (Batalion Hudy w Islamskim Maghrebie) – 30 VI 2014 r.
2. Dżund al-Khilafah fi Ard al-Dżazira (Armia Kalifatu w Algierii) – 14 IX 2014 r.
3. Dżund al-Khilafah fi Tunisijja (Armia Kalifatu w Tunezji) – 30 III 2015 r.
4. Wilajat al-Fezzan (Gubernatorstwo/Okręg Fezzanu) – 27 IX 2014 r.
5. Khilafah fi Tarabulus (Kalifat Trypolisu) – brak daty.
6. Mudżahidin fi Libijja (Mudżahedini Libijscy) – 10 XI 2014 r.
7. Wilajat Barka (Gubernatorstwo/Okręg Barka) – 5 X 2014 r.
8. Al-Madżlis asz-Szura asz-Szabab al-Muslimin (Rada Doradcza Młodzieży Muzułmańskiej) – 3 X 2014 (poparcie wyraziła 22 VI 2014 r.).
9. Al-Dżama'at al-Dżihad fi ad-Derna (Grupa Dżihadu w Dernie) – 8 XI 2014 r.
10. Al-Ansar Bait al-Makdis (Obrońcy Jerozolimy) – 10 XI 2014 r.
11. Dżund al-Khilafah fi Ard al-Kinana (Armia Kalifatu w Krainie Kołcznu – Górny Egipt) – 20 IX 2014 r.
12. Boko Haram (zachodnia cywilizacja jest zakazana) – 7 III 2015 r.
13. As-Salafijja Dżihadijja Ittihad fi al-Kaida (Salaficcy Dżihadyści Zjednoczeni z Al-Kaidą) – 11 II 2014 r.
14. Liwa Ahrar Ahl as-Sunnah fi al-Baalbek (Brygada Wyzwolenia Ludności Sunnickiej w Baalbeku) – 11 II 2014 r.
15. Liwa al-Faruk (Brygada Faruka) – 12 XI 2014 r.
16. Al-Dżama'at al-Imam Bukhari (Grupa Imama Buchariego) – 29 X 2014 r.
17. Ahrar asz-Szam fi al-Aleppo (Wyzwolenie Lewantu w Aleppo) – 5 X 2014 r.
18. Dżama'at Ansar al-Islam fi as-Surijja (Grupa Obrońców Islamu w Syrii) – 8 I 2015 r.
19. Liwa Szuhada al-*Jarmuk* (Brygada Męczenników Jarmuka) – 29 IV 2015 r.
20. Liwa Fadżr al-Islam (Brygada Świtu Islamu) – 20 VI 2014 r.
21. Ansar al-Islam fi al-Irak (Zwolennicy Islamu w Iraku) – 25 VIII 2014 r.
22. Mudżahidin fi al-Dżazirat al-Arab (Mudżahedini Półwyspu Arabskiego) – 10 XI 2014 r.
23. Ansar asz-Szaria (Zwolennicy Szariatu) – 11 II 2015 r.
24. Mudżahidin fi al-Jemen (Mudżahedini Jemenu) – 10 XI 2014 r.

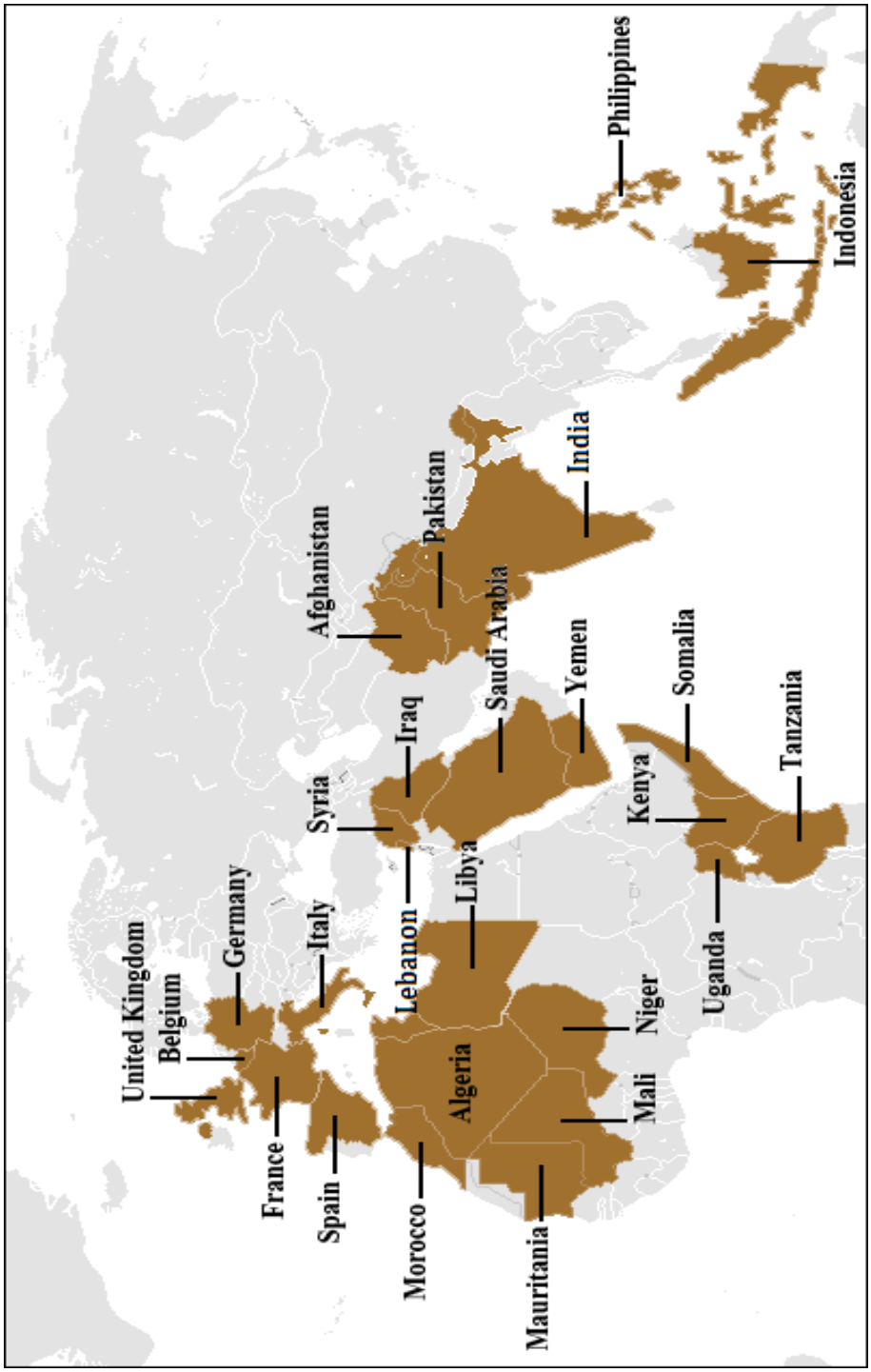
25. Al-Alama al-Liwa al-Islamijja fi al-Churasan (Bohaterowie Islamskiej Brygady Chorasanu) – 30 IX 2014 r.
26. Kataib at-Tawhid (Batalion Jedności) – 27 IX 2014 r.
27. Tehrik-e Taliban Pakistan (Ruch Pakistańskich Talibów) – 13 X 2014 r.
28. Szura-e Churasan (Rada Chorasanu) – 10 I 2015 r.
29. Tehrik-e Khilafah wa al-Dżihad (Ruch Kalifatu i Dżihadu) – 10 VII 2014 r.
30. Tehrik-e Khilafah (Ruch Kalifatu) – 9 VII 2014 r.
31. Ansar at-Tawhid fi Ard al-Hind (Zwolennicy Jedności Boga w Indiach) – 4 X 2014 r.
32. Mudżahidin Indonesia Timur (Mudżahedini Indonezji Wschodniej) – 3 VI 2014 r.
33. Bangsamoro Islamic Freedom Fighters (Islamscy Bojownicy o Wolność Bangsamoro) – 13 VIII 2014 r.
34. Abu Sajaf (Ojciec Miecza) – 23 VII 2014 r.
35. Ansar al-Khilafah fi Ard al-Filipino (Zwolennicy Kalifatu na Filipinach) – 12 VIII 2014 r.
36. Bangsamoro Justice Movement (Ruch Sprawiedliwości Bangsamoro) – 11 IX 2014 r.

WSPARCIE IDEOLOGICZNE I MARKETINGOWE

Grupy deklarujące wsparcie – data

1. Ansar asz-Szaria fi Tunisijja (Zwolennicy Szariatu w Tunezji) – 5 VII 2014 r.
2. Kataib Okba Ibn Nafi (Batalion Okby Ibn Nafiego) – 14 IX 2014 r.
3. Mudżahidin al-Madżlis asz-Szura fi Bajt al-Makdis (Mudżahedini Rady Doradczej Jerozolimy) – 2 II 2014 r.
4. Sons of Call for Tawhid and Jihad (Synowie Wzywają do Jedności i Dżihadu).
5. Ozbekiston Islomiy Harakati (Islamski Ruch Uzbekistanu) – 26 IX 2014 r.
6. Dżundallah (Armia Boga) – 17 XI 2014 r.
7. Dżimah Anszarut Tawhid (Wspólnota Zwolenników Jedności Boga) – 18 VII 2014 r.

Po stronie Al-Kaidy pozostały organizacje mające w swojej nazwie mają słowo „Al-Kaida" oraz somalijski Harakat asz-Szabab al-Mudżahidin – aby wymienić te najważniejsze (mapa 2). W dalszej części artykułu dokonano krótkiej charakterystyki aktywności tych ugrupowań w obliczu rosnącej w siłę konkurencji ze strony ISIS/IS i jego sojuszniczych organizacji.



Mapa 2. Sieć Al-Kaidy.

Źródło: https://en.wikipedia.org/wiki/Al-Qaeda [dostęp: 4 III 2016].

Ideologiczne podziały na osi Al-Kaida–IS są bardziej skomplikowane i, według autora, będą wywierać wpływ na bezpieczeństwo wielu państw świata. Dlatego też warto poświęcić im więcej uwagi. Marc Sageman w książce *Sieci terroru*[13] definiuje i opisuje koncepcje bliskiego i dalekiego wroga oraz lokalnego i globalnego salafickiego dżihadu w wykonaniu Al-Kaidy[14]. Ta rozbieżność strategii walki miała zwolenników i przeciwników, co musiało doprowadzić do istotnych rozłamów pomiędzy rozmaitymi radykalnymi ugrupowaniami związanymi z organizacją Osamy bin Ladena. Część z nich była zainteresowana raczej działalnością i osiąganiem celów o zasięgu lokalnym, na przykład zdobyciem wpływów we własnym regionie lub państwie i ich utrzymaniem. Mimo że część muzułmańskich teologów przyjęła koncepcję prowadzenia globalnego dżihadu, za którą optował Bin Laden, to jednak większość radykalnych uczonych religijnych pozostała przy konieczności obrony terytoriów muzułmańskich przed obcą ingerencją. Duże rozbieżności istniały również w traktowaniu szyitów. Przywódcy Al-Kaidy byli na przykład przeciwni strategii Abu Musaba az-Zarkawiego prowadzenia dżihadu zakładającego przede wszystkim rozpętanie w Iraku wojny domowej pomiędzy sunnitami i szyitami. Uważali, że priorytetem jest skoncentrowanie się na walce przeciw Amerykanom i ich sojusznikom. Dla ISIS/IS szyici są naturalnym wrogiem, którego należy zniszczyć. Al-Kaidę zaś charakteryzowała wrogość wobec USA i Izraela, co zostało ogłoszone w fatwie wydanej 23 sierpnia 1996 r. wypowiadającej wojnę „Amerykanom okupującym Ziemię Dwóch Świętych Miejsc" i potwierdzone 23 lutego 1998 r. przez utworzenie Światowego Frontu Islamskiego na rzecz Dżihadu przeciwko Żydom i Krzyżowcom.

Po śmierci Osamy bin Ladena 2 maja 2011 r. jego następca Ajman az-Zawahiri postanowił skoncentrować się na bliskich wrogach, zwłaszcza prozachodnich reżimach w regionach Afryki Północnej i Bliskiego Wschodu. Z dokumentacji znalezionej w pakistańskiej kryjówce Bin Ladena wynikało, że różnice zdań pomiędzy nim i jego następcą co do priorytetowych celów ataków terrorystycznych były znaczne. Podczas gdy Bin Laden był gotów atakować Amerykanów na ich własnym terytorium, Az-Zawahiri odrzucał takie rozwiązanie, twierdząc, że terytorium USA jest zbyt dobrze chronione.

Państwo Islamskie broniło terytoriów Iraku i Syrii i rozszerzało nad nimi kontrolę, a jednocześnie nie wahało się uderzać wszędzie tam, gdzie było to możliwe. Dysponowało bowiem większym zapleczem finansowo-logistycznym, militarnym, możliwościami operacyjnymi i propagandowo-rekrutacyjnymi niż Al-Kaida. Ajman az-Zawahiri zdecydowanie odrzucał jakąkolwiek formę uzurpowanego kalifatu lub próby narzucenia zwierzchnictwa i utworzenia kalifatu przy użyciu siły, zwłaszcza w kontekście działań podejmowanych przez Państwo Islamskie. Tym samym proponował restytucję kalifatu przez ewolucję, a nie rewolucję. Jednocześnie zdecydowanie potępiał terror stosowany przez bojowników IS wobec muzułmanów zamieszkujących

[13] M. Sageman, *Sieci terroru*, Kraków 2008.
[14] Tamże, s. 21–74.

obszary w Iraku i Syrii kontrolowane przez samozwańczy kalifat. W odróżnieniu od Państwa Islamskiego Bin Laden i Az-Zawahiri wspominali o idei kalifatu w perspektywie długoterminowej i traktowali je bardziej w kategoriach czynnika mobilizującego, aniżeli zadania możliwego do zrealizowania w najbliższych latach. Warto przy tym zwrócić uwagę na wyraźną różnicę między horyzontem czasowym strategii Al-Kaidy a czasem, w jakim zwykle planują instytucje polityczne i gospodarcze Zachodu. Cele krótkookresowe powinny być w założeniach Al-Kaidy osiągane kolejno w ciągu kilkudziesięciu lat, podczas gdy długookresowy zamiar ustanowienia kalifatu może zająć 50–100 lat[15]. Artur Wejkszner, jeden z badaczy tej problematyki, również stara się odpowiedzieć na pytanie, kiedy powstanie kalifat Al-Kaidy, i podaje różne scenariusze[16]. Nic bowiem nie stoi na przeszkodzie, aby istniały dwa kalifaty. W X i XI wieku istniały przecież obok siebie nawet trzy kalifaty: Abbasydów ze stolicą w Bagdadzie, Fatymidów ze stolicą w Kairze i kordobański Umajjadów.

Terrorystyczna rywalizacja pomiędzy Państwem Islamskim i Al-Kaidą[17]

Ogłoszenie powstania Państwa Islamskiego w czerwcu 2014 r. jako bytu terytorialnego i organizacji salafickiego globalnego dżihadu oznaczało zmianę na mapie terroryzmu islamskiego, z którym USA i sojusznicy prowadzą wojnę od ponad 15 lat. Państwo Islamskie pozbawiło Al-Kaidę miana najważniejszej organizacji terrorystycznej na świecie, zagospodarowując ideologiczną i logistyczną próżnię powstałą wraz z utratą znaczenia przez Al-Kaidę. Państwo Islamskie przejęło również większość jej wpływów, sponsorów oraz członków. Wykazało się ponadto większą dynamiką działań, większą brutalnością oraz większymi zdolnościami operacyjnymi. Proklamowanie kalifatu doprowadziło do konfrontacji IS z Al-Kaidą i sporu o pieniądze, bojowników, prestiż i popularność. Ta rywalizacja w znacznym stopniu wynika z osobistych animozji pomiędzy przywódcami obu struktur i przybiera bardzo różne formy, np. walki w Syrii pomiędzy IS a Dżabhat an-Nusra li Ahl asz-Szam i jej późniejszymi wcieleniami (OWL) i koalicjantami, przekazywanie sprzecznych informacji dotyczących autorstwa przeprowadzonych zamachów, konkurencja o wpływy, mordowanie liderów strony przeciwnej czy wzajemne dyskredytowanie się w mediach[18].W wyniku tej rywalizacji Al-Kaida straciła monopol na przewodzenie ruchowi dzihadystycznemu, wykorzystywanie cyberprzestrzeni do komunikacji, propagandy, indokrynacji i werbunku co spowodowało obniżenie jej atrakcyjności wśród islamskich organizacji ekstremistycznych oraz ograniczenie jej wpływów.

[15] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Warszawa 2017, s. 174–175.

[16] A. Wejkszner, *Globalna sieć Al-Kaidy. Nowe państwo islamskie?*, Warszawa 2017, s. 332–342.

[17] Informacje dotyczące wydarzeń w krajach Afryki i Azji zawarte w tej części artykułu pochodzą z mediów elektronicznych. Wymieniono jedynie najbardziej istotne dla treści opracowania.

[18] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*…, s. 206.

Poza Al-Kaidą i Państwem Islamskim działają również inne islamskie ugrupowania ekstremistyczne. Ich aktywność wywołuje niekiedy głębokie różnice między stanowiskami władz państwowych. Przykładem jest ruch Al-Ichwan al-Muslimin (Bracia Muzułmanie). Podobnie jak Państwo Islamskie oraz Al-Kaida jest to organizacja transgraniczna, działająca w wielu krajach muzułmańskich oraz w Europie (organizacje powiązane z Braćmi Muzułmanami istnieją często jako samodzielne struktury). Bracia Muzułmanie są obecnie uznawani za organizację terrorystyczną przez kilka państw islamskich: Egipt, Arabię Saudyjską oraz Zjednoczone Emiraty Arabskie. Inne kraje zezwalają na działalność tego ruchu lub go tolerują. Zjednoczone Emiraty Arabskie na swojej liście organizacji terrorystycznych umieściły również większość instytucji i ugrupowań powiązanych z Braćmi Muzułmanami, działających autonomicznie w Europie, uznawanych przez niektóre rządy krajów UE za reprezentację społeczności muzułmańskiej. Arabia Saudyjska oficjalnie zwalczała Państwo Islamskie, ale nieoficjalnie wspierała jej finansowo i militarnie.

Większość organizacji terrorystycznych jest inspirowanych ideologią salafick[19]. Salafici z założenia odrzucają demokrację i proces wyborczy jako niezgodny z szariatem**.** Odrzucają też świeckie ustawodawstwo jako niezgodne z *Koranem* i dążą do wprowadzenia prawa koranicznego jako jedynego źródła prawa. Ugrupowania salafickie jednak nie tworzą jednolitego bloku w świecie muzułmańskim, mają różne powiązania międzynarodowe (przeważnie z rywalizującymi między sobą Katarem i Arabią Saudyjską), a czasem – mimo swoich poglądów na demokrację i wybory – uczestniczą w wyborach (np. w Egipcie). Wahhabizm będący w istocie jedną z odmian salafizmu jest fundamentem ideologiczno-religijnym Arabii Saudyjskiej. To właśnie dzięki pieniądzom królestwa ta niegdyś marginalna grupa wewnątrz islamu zdołała dokonać ekspansji w ostatnich dekadach XX wieku i na początku obecnego stulecia, stanowiąc fundament zarówno dla Al-Kaidy, jak i Państwa Islamskiego.

Oprócz Bliskiego Wschodu główną areną aktywności i rywalizacji ugrupowań dżihadystycznych jest Afryka Północna obejmująca kraje Sahary i Sahelu, w których od drugiej połowy 2014 r. zwiększały się wpływy IS. Państwo Islamskie poniosło wiele dotkliwych klęsk w Syrii i Iraku, a i w Afryce jego pozycja znacznie osłabła. Utraciło ono kontrolę nad opanowanymi wcześniej terytoriami, na przykład w Libii,

[19] *Salafijja* – nurt religijno-społeczny i polityczny w islamie odwołujący się do pierwszego pokolenia muzułmanów (arab. *as-salaf as-salih* – szlachetni przodkowie). Wywodzi się z przekonania, że tylko bardzo ścisłe przestrzeganie ustalonych już dogmatów, przedstawianych jako zasady ustanowione raz na zawsze przez proroka Muhammada w wyniku objawienia, może zwrócić islamowi pozycję pierwszej siły w świecie, utraconej z powodu odejścia od nauki *Koranu*. Ideologia została stworzona na przełomie wieków XIX i XX przez Dżamala ad-Dina al-Afghaniego, Muhammada Abduha i Raszida Ridę. Postuluje ona powrót do rygorystycznie rozumianego prawa i wychwala ścisłą ortopraksję (ubieranie się na wzór proroka Muhammada, noszenie długiej brody, spanie na prawym boku na macie itp.). Fatwy formułowane zgodnie z zasadami *salafijji* są bardzo rygorystyczne, odwołują się jedynie do nakazów świętego tekstu *Koranu* i sunny. Pomijają przy tym społeczny kontekst europejski, często demonizowany w zestawieniu z normami obowiązującymi w świecie islamu. *Salafijja* dzieli się na kwietystyczną, polityczną i dżihadystyczną.

gdzie od lipca 2017 r. nie panuje już nad środkową częścią wybrzeża (Wilajet Syrta IS) i przy granicy z Tunezją, wciąż jednak ma zdolności do przeprowadzenia zamachów terrorystycznych. Na północy Afryki jedną z najważniejszych struktur terrorystycznych jest Tanzim al-Kaida bi Bilad al-Maghrib al-Islami (Organizacja Al-Kaidy w Krajach Islamskiego Maghrebu, OAKIM) powiązana z Al-Kaidą. W wyniku dezintegracji Republiki Mali w 2012 r. OAKIM, wykorzystując rebelię Tuaregów, opanowała prawie całe północne terytorium państwa, w tym główne miasta: Timbuktu i Gao. W ten sposób Al-Kaida Islamskiego Maghrebu zdołała stworzyć islamistyczny organizm państwowy w Afryce. Wprowadzono nową administrację kierującą się radykalną interpretacją *Koranu*, niszczono zabytkowe budowle (mauzolea), stare dokumenty oraz obiekty sztuki plemiennej[20]. Przywódca organizacji Abdel Malek Drukdel alias Abu Musab Abdel Wadu nakazał spowolnienie tempa zmian i ekspansji, aby nie zrazić do organizacji miejscowej ludności oraz nie sprowokować obcej interwencji. Jedną ze słabości nowego islamistycznego państwa była rywalizacja wewnętrzna pomiędzy przywódcami. Poza OAKIM działały tu inne ugrupowania. Jednym z nich było Ansar ad-Din (Obrońcy Wiary) oparte na zradykalizowanych religijnie Tuaregach, które przejęło kontrolę nad regionem Kidal, drugim – Dżama'at at-Tawhid wa al-Dżihad fi Gharbi Ifrikija (Mouvement pour l'Unicité et le Jihad en Afrique de l'Ouest, MUJAO, Grupa Jedności i Dżihadu w Zachodniej Afryce) z siedzibą w Gao, w skład którego weszli Sahrawijczycy (rdzenna ludność Sahary Zachodniej reprezentowana polityczne od lat przez Front Polisario), lokalni Arabowie oraz Songhajowie (członkowie jednego z największych plemion w północnym Mali). Jeden z liderów OAKIM Mochtar Belmochtar, skłócony z Drukdelem, pod koniec 2012 r. założył własne ugrupowanie o nazwie Katibat al-Mulassamin (Zamaskowana Brygada), zwane również Muwaka'un bi ad-Dima (Podpisani Krwią). Po rozpoczęciu interwencji Francji w Mali 16 stycznia 2013 r. ta organizacja przypuściła atak na pole gazowe Ajn Amenas, porywając ponad 800 pracujących tam osób, w tym 132 cudzoziemców. Według terrorystów był to odwet za francuskie bombardowania pozycji dżihadystów w Mali. Po czterech dniach oblężenia i szturmie algierskiej jednostki specjalnej uwolniono zakładników, jednak 39 z nich poniosło śmierć. Po tym ataku Belmochtar stał się jednym z najbardziej poszukiwanych terrorystów. W dniu 22 sierpnia 2013 r. przywódca MUJAO Ahmed at-Tilemsi i Belmochtar połączyli swoje ugrupowania i utworzyli organizację Al-Murabitun (Strażnicy). O tę fuzję wnioskował przywódca Al-Kaidy Ajman az-Zawahiri. Na czele Strażników stanął Egipcjanin Abu Bakr an-Nasri. Po jego śmierci w kwietniu 2014 r. przywództwo nad grupą objął Ahmed

[20] W sierpniu 2016 r. przed Międzynarodowym Trybunałem Karnym w Hadze stanął Ahmed al-Faki al-Mahdi, przywódca Ansar ad-Din, oskarżony o dokonanie zniszczenia średniowiecznych zabytków w Timbuktu, wpisanych na listę światowego dziedzictwa UNESCO, co jest traktowane jako zbrodnia wojenna. Al-Mahdi przyznał się do winy. Powiedział, że wydał rozkaz zniszczenia dziewięciu mauzoleów z XI i XII wieku oraz XV-wiecznego meczetu Sidi Jahia. We wrześniu 2016 r. został skazany na 9 lat więzienia i karę finansową w wysokości 2,7 mln euro, http://www.tvp.info/27101180/dzihadysta-skazany-na-zniszczenie-zabytkow-w-timbuktu-kierowaly-mna-zle-duchy [dostęp: 27 IX 2017].

at-Tilemsi, na co Belmochtar wyraził zgodę. W grudniu 2014 r. zginął również At-Tilemsi. Pod nieobecność Belmochtara liderem ogłosił się samozwańczo jeden z zastępców At-Tilemsiego Adnan Abu Walid as-Sahrawi. Belmochtar nie uznał nowego przywódcy. W maju 2015 r. As-Sahrawi zadeklarował sojusz organizacji z Państwem Islamskim, jednak kilka dni później Belmochtar wydał oświadczenie, w którym zanegował ważność sojuszu z IS, oskarżył tę organizację o zabijanie niewinnych muzułmanów, zadeklarował również wierność Ajmanowi az-Zawahiriemu, przywódcy Al-Kaidy. Libijskie władze poinformowały 14 czerwca 2015 r., że Belmochtar zginął w Libii podczas amerykańskich nalotów. Nie dostarczono jednak żadnych pewnych dowodów. W styczniu 2016 r. Departament Stanu USA usunął nazwisko Belmochtara z listy terrorystów, za których wyznaczono nagrodę.

Mimo aktywnych działań sił francuskich i oddziałów Mission Multidimensionnelle Intégrée des Nations Unies pour la Stabilisation au Mali, MINUSMA (Wielowymiarowej Zintegrowanej Misji Stabilizacyjnej ONZ w Mali), OAKIM wciąż stwarza poważne zagrożenie. W dniu 20 listopada 2015 r. terroryści dokonali ataku na hotel Radisson Blu w stolicy Republiki Mali Bamako, w którym zginęło 21 osób. W ataku na hotel Splendid w Wagadugu stolicy Burkina Faso, przeprowadzonym przez OAKIM 15–16 stycznia 2016 r., życie straciło 30 osób, a 56 zostało rannych, natomiast 13 marca tego samego roku ta organizacja ostrzelała turystów w kurorcie Grand -Bassam niedaleko Abidżanu, stolicy Wybrzeża Kości Słoniowej, powodując śmierć 19 osób. Dnia 18 czerwca 2017 r. zaatakowano ośrodek „Le Campement" w Dougourakoro na przedmieściach Bamako, gdzie wzięto 36 zakładników. Zostali oni uwolnieni w wyniku akcji sił specjalnych, podczas której śmierć poniosło trzech napastników. Dwa miesiące później (13 sierpnia) bojownicy OAKIM zaatakowali gości restauracji i hotelu w Wagadugu, zabijając 18 osób i raniąc 22. Poza tym terroryści atakują żołnierzy sił rządowych Mali i MINUSMA. Dżihadyści wykorzystują to, że wojska tych państw słabo kontrolują granice pomiędzy Mali, Nigrem i Burkiną Faso. Dżamel Okaha, przywódca saharyjskich struktur OAKIM, Ijad Ag Ghali, lider Ansar ad-Din, oraz Amadu Koufa, założyciel Front de Libération du Macina (Frontu Wyzwolenia Masiny)[21] utworzyli 2 marca 2017 r. organizację o nazwie Dżama'at Nusra al-Islam wa al-Muslimin (Stowarzyszenie Obrońców Islamu i Muzułmanów). Saharyjskie struktury Al-Kaidy pozostały lojalne wobec Az-Zawahiriego, jednak w lipcu 2014 r.

[21] Do Frontu Wyzwolenia Masiny należą przede wszystkim przedstawiciele pasterskiego plemienia Fulanów (Peul), sympatyzujący z Ansar ad-Din. Oprócz radykalnego imama Amadu Koufy na czele grupy stanął Sulejman Keita. Bazy organizacji znajdują się w Mali i na Wybrzeżu Kości Słoniowej, gdzie aresztowano siedmiu członków grupy, którzy przygotowywali zamach w stolicy Mali. W 2015 r. i 2016 r. ugrupowanie organizowało ataki na przedstawicieli malijskich sił bezpieczeństwa i obiekty międzynarodowe w Bamako oraz w regionie Mopti. W dniu 7 sierpnia 2015 r. przeprowadziło atak na hotel Byblos w Sevare, w którym mieszkali członkowie misji ONZ. Siły bezpieczeństwa odbiły obiekt dopiero następnego dnia. Zginęło co najmniej 13 osób, w tym pięciu pracowników ONZ i czterech żołnierzy. Zabito również czterech terrorystów, a siedmiu aresztowano, https://www.timesofisrael.com/mali-arrests-suspected-mastermind-of-hotel-terror-attack/ [dostęp: 25 IV 2016].

doszło do rozłamu w OAKIM w rejonie Kabyli w północnej Algierii. Grupa pod przywództwem wpływowego lidera tej organizacji Abdel Maleka Guriego złożyła przysięgę wierności kalifowi Ibrahimowi, przyjmując nazwę Dżund al-Khilafa fi Ard al-Dżazira (Armia/Żołnierze Kalifatu w Algierii). Ta organizacja porwała i zamordowała francuskiego przewodnika Hervé Gourdela, to zaś spowodowało wytropienie i zlikwidowanie Guriego przez wojsko algierskie. W lutym 2016 r. grupa zamordowała trzech algierskich żołnierzy. Rebelia Tuaregów w Republice Mali w 2012 r. została pozytywnie przyjęta przez część ich pobratymców z Ahaggaru we wschodniej Algierii i z libijskiego miasta Ghat, którzy utworzyli organizację Mouvement des Fils du Sahara pour la Justice Islamique, MFSJI (Ruch Synów Sahary na rzecz Sprawiedliwości Islamskiej). Bojownicy tej organizacji planowali uderzenia na miasta Hassi Messaoud i Dżanet we wschodniej Algierii. Celem ataków przeprowadzanych na północy Algierii są służby bezpieczeństwa państwa. W lutym 2017 r. trzech policjantów zostało rannych w Konstantynie, a trzech następnych zginęło w Tiaret w sierpniu tego samego roku. Obawiając się poważnego ataku terrorystycznego na początku września 2017 r., władze Algierii podniosły poziom zagrożenia do najwyższego w strategicznych miejscach cywilnych i wojskowych, w tym wzdłuż granicy państwa[22].

Znacznie lepiej wiedzie się Państwu Islamskiemu w Libii, gdzie wciąż daleko jest do stabilizacji. Już w kwietniu 2014 r. w nadmorskiej Dernie powstał 800-osobowy oddział islamistów wierny IS, wzmocniony następnie przez 300 Libijczyków z Katibat al-Battar (Brygady Al-Battar), walczącej dotychczas w syryjskich szeregach Państwa Islamskiego. W październiku 2014 r. te oddziały opanowały Dernę, a Al-Baghdadi wysłał do Libii Jemeńczyka Abu al-Baraa al-Azdiego oraz swojego zastępcę Abu Nabila al-Anbariego, byłego generała armii Saddama Husajna. Abu al-Baraa al-Azdi został emirem utworzonego w Libii nowego emiratu Państwa Islamskiego o nazwie Wilajet al-Barqa (Cyrenajka), natomiast zadaniem Abu Nabil al-Anbari było ugruntowanie wpływów organizacji w tym rejonie, przy jednoczesnym zmniejszeniu wpływów Al-Kaidy i innych ugrupowań. W lutym 2015 r. libijski odłam IS wzmocnił się finansowo po zdobyciu Syrty i okolicznych pól naftowych. W maju 2017 r. powiązana z Al-Kaidą libijska organizacja Ansar asz-Szaria (Zwolennicy Szariatu) podjęła decyzję o samorozwiązaniu. Powodem tego miały być straty w ludziach i śmierć najważniejszych dowódców. Ugrupowanie, które próbowało umocnić się we wschodniej Libii, było zwalczane zarówno przez oddziały samozwańczej Libijskiej Armii Narodowej dowodzonej przez gen. Chalifę Haftara, jak i przez jednostki pozostające pod kontrolą Rządu Porozumienia Narodowego. Przedstawiciele ugrupowania wezwali wszystkie radykalne siły islamu w Libii do zjednoczenia się w ramach jednolitego frontu. Ansar asz-Szaria miało na koncie kilka spektakularnych akcji, przede wszystkim zamach na budynek konsulatu oraz komórkę CIA w Bengazi (11 września 2012 r.). Śmierć poniosło wówczas czterech Amerykanów: ambasador Christopher Stevens, pracownik konsulatu

[22] Szerzej na temat konfliktu w Republice Mali zob. K. Danielewicz, *Terroryzm w Afryce. Geneza oraz przebieg konfliktu w Mali w latach 2012–2014*, Oświęcim 2016, s. 82–151.

Sean Smith oraz agenci CIA: Tyrone S. Woods i Glen Doherty. Dnia 27 stycznia 2015 r. zdetonowano samochód-pułapkę przed wejściem do luksusowego hotelu Corinthia w Trypolisie, do którego następnie wtargnęła grupa uzbrojonych i zamaskowanych napastników, strzelając do znajdujących się w holu osób. Po wkroczeniu policji terroryści zdetonowali pasy z ładunkami wybuchowymi. W ataku zginęło 11 osób, w tym sześciu cudzoziemców. Prawdopodobnie ci sami sprawcy 10 dni wcześniej zaatakowali ambasadę Algierii w Trypolisie, raniąc trzech strażników. W opublikowanym w internecie oświadczeniu odpowiedzialność za zamach wzięli bojownicy deklarujący przynależność do Państwa Islamskiego. Akcja miała być formą odwetu za Abu Anasa al-Libiego, jednego z organizatorów zamachów na ambasady USA w Kenii i Tanzanii (7 sierpnia 1998 r.), który zmarł w amerykańskim więzieniu[23]. Dżihadyści działający w imieniu IS zaatakowali 23 sierpnia 2017 r. w rejonie Al-Dżufra na zachodzie Libii żołnierzy gen. Haftara. Dziewięciu żołnierzom wziętym do niewoli ścięto głowy. Zamordowano także dwóch cywilów. W lutym 2015 r. podobny los spotkał 21 egipskich Koptów pracujących w Libii. Egzekucji, która została sfilmowana, dokonano na plaży przy jednym z hoteli w Syrcie. Ciała ofiar tej zbrodni odnaleziono pod koniec września 2017 r. Natomiast libijskie, malijskie i algierskie organizacje, które są powiązane z Al-Kaidą, utworzyły Radę tej organizacji w Afryce. W jej skład weszły: Katibat al-Kaida (Brygada Al-Kaidy) w Syrcie, Katibat al-Kaka ibn Amr (Brygada Al-Kaka ibn Amra) we wschodniej Libii, OAKIM i Muwaka'un bi ad-Dima w Mali, a także kilka mniejszych grup z Libii i Algierii, w tym powiązanych z OAKIM.

Organizacje o nazwie Ansar asz-Szaria były i są nadal obecne również w innych krajach Afryki Północnej: w Egipcie, Maroku, Mauretanii i Tunezji. Nie deklarowały one swojej przynależności ani do Al-Kaidy, ani do Państwa Islamskiego, działają natomiast na szczeblu lokalnym. Tunezyjska Ansar asz-Szaria wykazywała dużą aktywność operacyjną. Po rewolucji w 2011 r. salafici początkowo działali legalnie, korzystając z parasola ochronnego islamistycznego rządu kierowanego przez tunezyjski odłam Braci Muzułmanów, znany jako Hizb an-Nahda (Partia Odrodzenia). Część ugrupowań salafickich próbowała nawet tworzyć partie polityczne, większość jednak z góry odrzucała demokrację. Ansar asz-Szaria była odpowiedzialna za inspirowanie ataku kilkutysięcznego tłumu na ambasadę USA w Tunisie 14 września 2012 r. w reakcji na upublicznienie amerykańskiego filmu *Innocence of Muslims* (*Niewinność muzułmanów*)[24], uważanego za obrazę islamu. Podczas tych wydarzeń zginęły cztery osoby, a wiele odniosło rany. Islamistyczne władze Tunezji zdelegalizowały Ansar asz-Szaria dopiero po masowych demonstracjach zorganizowanych przez tę organiza-

[23] Abu Anas al-Libi został schwytany w Trypolisie w październiku 2013 r. przez amerykańskie siły specjalne i przewieziony do USA. Zmarł w szpitalu z powodu ciężkiej choroby w oczekiwaniu na proces.

[24] Niezależny film amerykański określany jako antyislamski. Udostępnienie jego fragmentów w serwisie internetowym YouTube wywołało we wrześniu 2012 r. falę oburzenia w niektórych krajach zamieszkanych przez muzułmanów. Twórca filmu ukrywa się pod pseudonimem Sam Bacile, https://pl.wikipedia.org/wiki/Innocence_of_Muslims [dostęp: 20 VI 2018] – przyp. red.

cję po zamachach w lutym i lipcu 2013 r. na dwóch lewicowych polityków opozycji. Po tej decyzji jej członkowie zaczęli prowadzić zakonspirowaną działalność, ale organizacja nie odzyskała już dawnej pozycji. Jej miejsce zajęła Katibat Okba ibn Nafi (Brygada Okby ibn Nafiego)[25], która powstała w grudniu 2012 r. z inicjatywy lidera OAKIM Abdela Maleka Drukdela. Jej przywódcą został Chalid Chaieb alias Lukman Abu Sachr W styczniu 2014 r. stanął on na czele zdelegalizowanej Ansar asz-Szaria. We wrześniu 2014 r. jedna z frakcji Brygady Okby ibn Nafiego podporządkowała się IS (znowu po przywództwem Abu Sachra), podczas gdy pozostali bojownicy zachowali wierność OAKIM i działali na terenie Tunezji i Libii. W lipcu 2014 r. Abu Sahr odbył spotkanie z Mochtarem Belmochtarem w celu przeprowadzenia wspólnych ataków wymierzonych w infrastrukturę turystyczną i obiekty rządowe w Tunezji. Na początku marca następnego roku tunezyjscy ekstremiści poinformowali o powstaniu nowej organizacji – Dżund al-Khilafa fi Tunis (Armia/Żołnierze Kalifatu w Tunisie). Podporządkowała się ona Państwu Islamskiemu zaraz po apelu IS skierowanym do Tunezyjczyków, aby wstępowali w szeregi sił kalifatu. W dniu 29 lipca 2013 r. bojownicy Brygady Okby ibn Nafiego i OAKIM atakowali przez wiele godzin posterunek wojskowy w masywie Chambi w zachodniej Tunezji, zabijając 8 żołnierzy. Rok później (16 lipca) zginęło tutaj kolejnych 15 żołnierzy, a 20 zostało rannych. Tunezyjskie i algierskie siły bezpieczeństwa prowadziły operację antyterrorystyczną po obu stronach granicy. Do marca 2016 r. dżihadyści atakowali żołnierzy, funkcjonariuszy policji i sił bezpieczeństwa w różnych regionach Tunezji[26], jednak do najkrwawszych zamachów w tym kraju doszło w 2015 r. Ich celem byli zachodni turyści: w ataku na Muzeum Bardo w Tunisie, przeprowadzonym 18 marca, zastrzelono 24 osoby, a ok. 50 zostało rannych; 26 czerwca w Susie śmierć poniosło 36 osób, a 39 odniosło rany; 24 listopada terrorysta powiązany z Państwem Islamskim wysadził się w powietrze podczas próby wejścia do autobusu z funkcjonariuszami ochrony prezydenta. W tym zamachu śmierć poniosło 13 osób, a 20 zostało rannych.

Od czasu gdy egipskie siły pod dowództwem gen. Abd al-Fattaha as-Sisiego (obecnie prezydenta Egiptu) obaliły w 2013 r. prezydenta Muhammada Mursiego związanego z Bractwem Muzułmańskim, ugrupowania ekstremistyczne w Egipcie nasiliły ataki na siły zbrojne i policję, głównie na półwyspie Synaj. W atakach na Synaju zginęło kilkudziesięciu żołnierzy i policjantów. Właśnie na tym półwyspie Państwo Islamskie zdołało stworzyć silną komórkę. W listopadzie 2014 r. przysięgę wierności kalifowi Abu Bakrowi al-Bagdadiemu złożyła grupa Ansar Bajt al-Makdis (Obrońcy Jerozolimy), która powstała w 2011 r. Powołała ona Wilajet Synaj i działa od tej pory

[25] Nazwa odwołuje się do legendarnego zdobywcy, generała, który wyruszył na podbój Afryki Północnej. W 672 r. wzniósł on najstarszą arabską budowlę w Afryce Północnej – zachowany do dziś meczet w Kairuanie, mieście uznawanym przez Arabów za czwarte święte miejsce po Mekce Medynie i Jerozolimie. Okba (Ukba) ibn Nafi zginął w 683 r. na terytorium obecnej Algierii w bitwie ze zjednoczonymi siłami berberyjskimi dowodzonymi przez Kusajlę (Kosejlę), zob. E. Szymański, *Tradycje i legendy ludów Afryki Północnej*, Kraków 1994, s. 63–66.

[26] https://fr.wikipedia.org/wiki/Bataille_de_Chaambi [dostęp: 12 V 2017].

jako Państwo Islamskie zwane też Państwem Synaj. Po stronie IS opowiedziało się też ugrupowanie Adżnad Misr (Żołnierze Egiptu) założone w 2013 r. Choć te grupy nie kontrolują żadnego terytorium, to do chwili obecnej są bardzo aktywne, organizując często krwawe zamachy na cele znajdujące się głównie, choć nie tylko, na Synaju. Celem są przede wszystkim żołnierze i funkcjonariusze publiczni Egiptu, Koptowie oraz turyści. Bojownicy IS silnie zaznaczyli swoją obecność w okolicach miasta Rafah na obrzeżach Asz-Szajch Zuwajjid i w rejonie największego miasta na Synaju, Al-Arisz. W dniu 31 października 2015 r. doprowadzili również do katastrofy samolotu rosyjskich linii lotniczych Metrolet z turystami wracającymi do kraju z Szarm el-Szejk. W katastrofie śmierć poniosły 224 osoby. W 2017 r. w Wielki Piątek zaatakowali koptyjskie kościoły w mieście Tanta w Delcie Nilu i w Aleksandrii, zabijając co najmniej 45 osób. W dniu 27 maja tego samego roku Państwo Islamskie przyznało się do ostrzelania dzień wcześniej autokaru przewożącego koptyjskich pielgrzymów w prowincji Al-Minja. W tym ataku śmierć poniosło 26 osób, a 25 zostało rannych. Jednak do najtragiczniejszego zamachu doszło 24 listopada 2017 r., gdy grupa ok. 30 terrorystów otworzyła ogień do ludzi modlących się w meczecie w miejscowości Ar-Rawda niedaleko Al-Arisz. W ataku zginęło 305 osób. Była to największa masakra w nowożytnej historii Egiptu.

Z Al-Kaidą ściśle jest związany somalijski Harakat asz-Szabab al-Mudżahidin (Ruch Młodych Mudżahedinów), znany pod krótszą nazwą Asz-Szabab, który w latach 2007–2010 zdołał opanować większość terytorium Somalii wraz ze stolicą Mogadiszu. Po interwencji sił kenijskich w 2011 r. ugrupowanie zostało wyparte z większości zajmowanego terytorium i obecnie działa w rozproszeniu, jednak nie straciło możliwości operacyjnych, jeżeli chodzi o zamachy terrorystyczne, i to nie tylko w Somalii, lecz także w sąsiedniej Kenii[27]. Asz-Szabab zadeklarowała lojalność wobec Al-Kaidy dopiero w 2012 r. W 2014 r. frakcja na czele z Abdulem Kaderem Mohammedem, dowódcą operacji zagranicznych, oraz Mohamedem Sandherem opowiedziała się za współpracą z IS. We wrześniu 2014 r. amerykański dron zlikwidował lidera organizacji Ahmeda Abdi Godane. Po jego śmierci przywództwo nad organizacją objął Ahmed Omar alias Abu Ubaidah, alias Ahmed Dirije, a jego zastępcami zostali Muchtar Robow alias Abu Mansur i Mahad Karate alias Mahad Warsame Kalej. Do pomocy mieli Komitet Doradczy (*Szura Medżlis*) złożony z 10 doświadczonych bojowników. Celem Komitetu jest nadzór nad różnymi dziedzinami aktywności grupy: operacyjną, polityczną, propagandową i religijną. W skład struktur organizacji wchodzą jednostki: bezpieczeństwa wewnętrznego, organizująca zamachy za granicą (przede wszystkim

[27] Przed inwazją wojsk kenijskich w Somalii w Asz-Szabab doszło do podziału na opcję nacjonalistyczną (reprezentowaną przez Hasana Dahira Awejsa), która optowała wyłącznie za walką o władzę w Somalii, a opcją Ahmeda Abdi Godane opowiadającą się za utworzeniem kalifatu w Afryce Wschodniej. Po śmierci Abdi Godane w 2014 r. frakcja narodowa na czele z Ahmedem Omarem i Muchtarem Robow zyskała przewagę, nadając ton działalności organizacji, https://ctc.usma.edu/posts/the-life-and-death-of-al-shabab-leader-ahmed-godane [dostęp: 3 X 2014]; Y. Olomojobi, *Frontiers of Jihad. Radical islam in Africa*, Ibadan 2015, s. 161–165.

w Kenii) i odpowiedzialna za bojowników z innych państw (*muhadżirun*), głównie z Kenii, Tanzanii, Sudanu oraz za Somalijczyków, którzy przyjechali z państw zachodnich. W ciągu ostatnich lat zmalało zainteresowanie radykałów spoza Somalii wstępowaniem do struktur tej organizacji, do czego przyczyniła się popularność innych, bardziej dostępnych frontów walki, w tym przede wszystkim w Iraku i Syrii. W dniu 13 sierpniu 2017 r. Robow, na mocy amnestii, oddał się w ręce sił rządowych, a na początku grudnia tego samego roku w wyniku nalotu amerykańskiego drona został zlikwidowany Mahad Karate.

Asz-Szabab jest znany m.in. z krwawych zamachów w Kenii (tu filią Asz-Szabab jest Centrum Młodzieży Muzułmańskiej „Al-Hidżra"), gdzie od wkroczenia sił kenijskich do Somalii w październiku 2011 r. do końca 2014 r. jego członkowie przeprowadzili ok. 140 zamachów. Między innymi 21 września 2013 r. grupa zamaskowanych i uzbrojonych napastników wtargnęła do galerii handlowej Westgate w Nairobi, biorąc zakładników i zabijając osoby niebędące muzułmanami. Do czasu odbicia obiektu 24 września zginęło 71 osób, a 175 zostało rannych. Był to odwet za działania wojsk kenijskich w Somalii. Dnia 21 listopada 2014 r. 50 km od miasta Mandera leżącego w pobliżu granicy z Somalią i Etiopią terroryści uprowadzili autobus z ok. 60 pasażerami. Oddzielili muzułmanów od niemuzułmanów, których było 28, nakazali tym ostatnim wejść ponownie do pojazdu, zastrzelili ich, a nstępnie zbiegli do Somalii. Do podobnego zamachu doszło w grudniu 2015 r. w wiosce El Wak, również w pobliżu granicy, ale wówczas muzułmanie obronili chrześcijan, nie dając się od nich oddzielić. W zamachu zginęły dwie osoby. Wcześniej tego samego roku (2 kwietnia) czterej uzbrojeni bojownicy Asz-Szabab wtargnęli do budynku uniwersytetu w Garissie na wschodzie kraju i zabili strażników pilnujących bramy wjazdowej. Napastnicy początkowo strzelali na oślep, a następnie rozpoczęli selekcję – wypuszczali muzułmańskich studentów, a na chrześcijanach dokonywali egzekucji. Liczba ofiar wyniosła 148 osób. Po około 20 godzinach oblężenia terroryści zostali zastrzeleni. W dniach 6 i 25 października 2016 r. terroryści zaatakowali dwukrotnie w mieście Mandera. W obu zamachach śmierć poniosło 18 osób, a wiele zostało rannych.

Asz-Szabab wciąż kontroluje część terenów w południowej i środkowej Somalii. W Mogadiszu współpracownicy organizacji pobierają od przedsiębiorców podatek rewolucyjny. Każdego miesiąca w stolicy dochodzi przeciętnie do dwóch eksplozji. Asz-Szabab przeprowadza zamachy na polityków i biznesmenów, porywa pracowników misji humanitarnych, podkłada miny i atakuje hotele oraz żołnierzy African Union Mission in Somalia, AMISOM, np. 30 lipca 2017 r. w zasadzce zorganizowanej przez Asz-Szabab zginęło 24 żołnierzy. Do ataku doszło kilka godzin po wybuchu samochodu pułapki w Mogadiszu, w którym śmierć poniosło pięć osób, a 13 zostało rannych. Dnia 14 grudnia 2017 r. ubrany w policyjny mundur napastnik przedostał się na teren szkoły policyjnej w Mogadiszu i zdetonował bombę, którą miał na sobie. W zamachu śmierć poniosło 18 funkcjonariuszy, a 15 cywilów odniosło rany. Liczba ofiar mogłaby być znacznie większa, gdyby napastnik zdołał zdetonować ładunek w tłumie policjantów przygotowujących się na placu do apelu. Do najbardziej krwawego zamachu

przeprowadzonego przez Asz-Szabab na hotel i targowisko w stolicy kraju, uznanego za jeden z najkrwawszych w historii, doszło 14 października 2017 r. Do ataku użyto dwóch ciężarówek wypełnionych materiałami wybuchowymi. Jedna z eksplozji okazała się szczególnie tragiczna, ponieważ ciężarówkę z bombą postawiono tuż przy cysternie z benzyną. Detonacja wywołała potężny pożar. W obu zamachach zginęło 512 osób, a 295 zostało rannych. 165 osób nie udało się zidentyfikować i zostały one pochowane we wspólnej mogile. Od momentu tego zdarzenia Stany Zjednoczone zwiększyły częstotliwość lotniczych ataków na bojowników Asz-Szabab. W dniu 13 listopada 2017 r. Pentagon potwierdził zabicie w ciągu czterech dni ponad 40 dżihadystów należących do tej organizacji i do Państwa Islamskiego. W kolejnej operacji przeciwko Asz-Szabab, przeprowadzonej 21 listopada tego samego roku przez amerykańską armię, zlikwidowano ponad 100 bojowników. Według raportu ONZ aktywność dżihadystów w Somalii w 2017 r. znacznie wzrosła.

Równie krwawa jak Asz-Szabab jest nigeryjska organizacja Dżama'at Ahl al-Sunna li ad-Dawa wa al-Dżihad (Stowarzyszenie Ludności Sunnickiej na rzecz Działalności Misyjnej i Dżihadu), znana jako Boko Haram (Zachodnia cywilizacja jest zakazana). We wrześniu 2014 r. ogłosiła ona powołanie własnego kalifatu. Na początku 2015 r. jej lider Abubakar Szekau przyjął zwierzchność IS, tworząc oficjalnie w kwietniu tego samego roku Zachodnioafrykańską Prowincję Państwa Islamskiego, znaną jako Prowincja Sudanu Zachodniego (Wilajet Gharbi Ifriqijja). Państwo Islamskie chciało przejąć kontrolę nad Boko Haram, dlatego dążyło do osłabienia pozycji Szekau. Wynikało to z jego sprzeciwu wobec planów kalifa Abu Bakra al-Bagdadiego rozszerzenia działalności Boko Haram poza Niger i Kamerun w ramach idei globalnego dżihadu oraz powierzenia przywództwa nad grupą organowi kolegialnemu (arab. *madżlis asz-szura*). W skład tego organu mieliby wejść m.in. wyznaczeni przez szefa IS Mamman Nur i Abubakar Adam Kambara, co pozbawiłoby Szekau jednoosobowego dowództwa nad Boko Haram. Zmniejszaniu jego wpływów sprzyjał także zarządzony przez Al-Bagdadiego podział bojowników Boko Haram na trzy zgrupowania, które zostały dyslokowane do północnego Kamerunu, w okolice jeziora Czad oraz do wschodniego Nigru. Zadaniem Szekau miało być koordynowanie działań, głównie w północnej Nigerii. Spory pomiędzy liderami dotyczące zakresu terytorialnego działania oraz podziału kompetencji doprowadziły m.in. do opuszczenia Boko Haram przez Dżama'atu Ansarul Muslimina fi Biladis Sudan (Stowarzyszenie Obrońców Muzułmanów w Krainie Czarnych). Przywódca tej siostrzanej organizacji Khalid al-Barnawi nawiązał współpracę z Organizacją Al-Kaidy w Krajach Islamskiego Maghrebu.

Do 2015 r. organizacja Boko Haram niemal przejęła kontrolę nad trzema stanami w północno-wschodniej Nigerii: Borno, Jobe i Adamawą. Po Państwie Islamskim jest to najbardziej zbrodnicza organizacja, której działalność spowodowała śmierć ponad 20 tys. ludzi i zmusiła do ucieczki z zagrożonych terenów ok. 2 mln mieszkańców. Według różnych źródeł siłę zbrojną organizacji szacowano w 2015 r. na 4–30 tys. bojowników. Zasłynęła ona m.in. z uprowadzenia w nocy z 14 na 15 kwietnia 2014 r. 276 dziewcząt z internatu w szkole w Chibok. Sprawa porwania była najgłośniejsza,

ale nie jedyna. Kilka miesięcy później dżihadyści porwali 300 uczniów i kolejne 100 dzieci i kobiet w miejscowości Damasak, o czym media już milczały. Uprowadzenie dziewcząt z Chibok sprawiło, że opinia publiczna z niepokojem patrzyła na Nigerię. Przez media społecznościowe przeszła kampania „Zwróćcie nasze dziewczynki". Przyłączyła się do niej nawet pierwsza dama USA Michelle Obama. Miało to wywrzeć presję na nigeryjskie siły, aby odnalazły dzieci. Jednak mimo obietnic afrykańskich polityków i upływu trzech lat od tamtego zdarzenia, wiele dziewcząt z Chibok nadal jest w rękach porywczy. Wolność odzyskały te, które zdołały same uciec. W maju 2017 r. w wyniku porozumienia z władzami Nigerii uwolniono 82 dziewczynki w zamian za wypuszczenie z więzień członków Boko Haram. Według Amnesty International od początku 2014 r. do kwietnia 2015 r. Boko Haram porwało co najmniej 2 tys. kobiet i dzieci, które są wykorzystywane jako seksualne niewolnice i pomoce kuchenne, jako karta przetargowa w negocjacjach mających doprowadzić do zwolnienia więźniów oraz do przeprowadzenia zamachów samobójczych. W 2015 r. do takich ataków w Nigerii, Kamerunie i Czadzie zmuszono 44 dzieci (w 2014 r. – czworo). Kilkoro z nich miało zaledwie osiem lat. Łączna liczba zamachów samobójczych dokonanych w tych trzech krajach oraz w Nigrze przez Boko Haram oraz jej siostrzaną organizację z północnego Kamerunu wzrosła z 32 w 2014 r. do 151 w 2015 r. Zwiększyła się również liczba dziewcząt i kobiet biorących udział w tych atakach. Boko Haram jest organizacją mającą największy na świecie odsetek dzieci i kobiet wśród zamachowców[28]. Od 1 stycznia do 16 sierpnia 2017 r. zabito 83 dzieci (w tym 55 dziewczynek) przez zdetonowanie ładunków wybuchowych przytwierdzonych do ich ciał. Większość z dzieci miała mniej niż 15 lat. Zazwyczaj terroryści umieszczają ładunek wybuchowy na ciele dziecka, pozostawiają dzieci w zatłoczonym miejscu publicznym, na zatłoczonych bazarach i dworcach, a następnie zdalnie powodują wybuch. Do jednej z dziewczynek dodatkowo przyklejono taśmą niemowlę. Kilkorgu dzieciom udało się przedostać na posterunek policji, gdzie zdjęto z nich i zabezpieczono ładunki wybuchowe. W marcu 2015 r. nastolatka, której udało się udaremnić zamach, powiedziała, że jest jedną z 276 uczennic ze szkoły w Chibok porwanych przez Boko Haram w 2014 r.

Władze Nigerii kilkakrotnie informowały o śmierci lidera Boko Haram Abubakara Szekau. Nowym przywódcą miał zostać Abu Musab al-Barnawi. O tej decyzji poinformowano 2 sierpnia 2016 r. w tygodniku dżihadystów „Al-Naba" („Wieść"), jednak dwa dni później Szekau ogłosił, że nadal jest przywódcą organizacji. W dniu 27 czerwca 2017 r. w internecie został opublikowany film z wypowiedzią Szekau o tym, że jest on odpowiedzialny za porwanie nigeryjskiej policjantki. Skrytykował również władze kraju za propagowanie fałszywych informacji o zlikwidowaniu jego organizacji.

Terrorystyczna działalność Boko Haram doprowadziła do całkowitego zniszczenia 900 szkół (część z nich została spalona) oraz do zamknięcia dwukrotnie większej liczby tych placówek. Ponad 600 nauczycieli i pracowników szkolnych zostało zabi-

[28] https://kobieta.wp.pl/horror-ktorego-swiat-nie-chce-dostrzec-w-2017-roku-boko-haram-wysadzilo-w-powietrze-55-dziewczynek-6158590054090881a [dostęp: 24 VIII 2017]; https://wiadomosci.wp.pl/zamach-w-maiduguri-zabitych-10-osob-wielu-rannych-6188198088788097a [dostęp: 16 XI 2017].

tych, a 19 tys. zmuszono do ucieczki[29]. Do tego trzeba dodać setki zamordowanych lub porwanych uczniów i tysiące rannych osób. Od kiedy islamiści w Nigerii zostali zepchnięci przez koalicyjne siły Nigerii, Czadu, Nigru i Kamerunu do defensywy, ich celem pozostają cywile. Dzięki sukcesom militarnym nigeryjska armia oswobodziła w ostatnich miesiącach setki porwanych. Z raportu UNICEF i londyńskiej fundacji International Alert wynika, że kobiety i nastolatki powracające do wiosek są traktowane z podejrzliwością lub wręcz odrzucane. Ofiary gwałtów nierzadko są w ciąży i noszą dziecko dżihadysty. Lokalna społeczność obawia się też, że porywacze zaszczepili im radykalne idee. W kwietniu 2016 r. pojawiły się informacje, że członkowie lub sympatycy Boko Haram pochodzący z Senegalu mogą przeprowadzić ataki na plażach Włoch, Francji i Hiszpanii. W październiku 2017 r. rozpoczął się pierwszy z procesów przeciwko 2300 osobom oskarżonym o działalność w Boko Haram. Wśród nich znajduje się Khalid Barnawi oskarżony o porwanie i zamordowanie 10 cudzoziemców.

Na przełomie lat 2015 i 2016 Tanzim al-Kaida fi Dżazirat al-Arab (Organizacja Al-Kaidy na Półwyspie Arabskim, OAKPA) utworzyła własny emirat. Ta organizacja jest uznawana za najgroźniejszą gałąź Al-Kaidy, działała w Jemenie od dawna, jednak za rządów prezydenta Abd Rabbuha Mansura Hadiego oraz jego poprzednika Alego Abdullaha Saleha jej możliwości operacyjne były ograniczone. Było to spowodowane amerykańskimi uderzeniami z powietrza oraz atakami szkolonych przez siły USA żołnierzy rządu w Sanie, które zepchnęły OAKPA do defensywy. Tak było do stycznia 2015 r., kiedy to szyiccy rebelianci z ruchu Husi zmusili Hadiego do ucieczki ze stolicy, a w ślad za nim – do wycofania z kraju amerykańskich żołnierzy. Za sprawą interwencji Arabii Saudyjskiej (w marcu 2015 r.) konflikt wkrótce stał się kolejną areną saudyjsko-irańskiej rywalizacji w regionie, co doprowadziło do eskalacji sporu i humanitarnej katastrofy. Podczas gdy walki między Husi i siłami rządu skupiały się w południowo-zachodniej, najgęściej zaludnionej, części kraju, na wschodzie OAKPA skorzystała z chaosu i przejmowała kolejne miejscowości, często opuszczone przez żołnierzy reżimu. Budowała tutaj swoje struktury, niekiedy przy cichej akceptacji miejscowej ludności, która uważała, że sytuacja była bardziej stabilna niż w wyzwolonych przez siły rządowe częściach Jemenu, a rządy inne niż Al-Kaidy mogły być dużo gorsze. Niemal od samego początku funkcjonowania w tej części Bliskiego Wschodu OAKPA stosowała taktykę zbliżoną do tego, co robiło Państwo Islamskie – zajmowała określony teren, kontrolowała i wykorzystywała jego potencjał społeczno-ekonomiczny oraz podporządkowywała sobie zamieszkałą tam ludność. OAKPA wyróżniała się na tle innych struktur Al-Kaidy tym, że przenosiła swoje działania do Europy. W tym miejscu należy zwrócić uwagę na coraz powszechniejszą tendencję tworzenia przez islamskie organizacje terrorystyczne w punktach zapalnych struktur quasi-państwowych.

W 2016 r. OAKPA sprawowała kontrolę nad 10 miejscowościami. Mimo że władzę sprawuje przez lokalnych popleczników, a nie pod szyldem Al-Kaidy, rządy

[29] https://wiadomosci.wp.pl/pala-szkoly-porywaja-dzieci-morduja-nauczycieli-krwawa-kampania-fanatykow-boko-haram-6025269939212929a [dostęp: 22 IV 2016].

ekstremistów są bezwzględne i niewiele różnią się od stylu rządów ich ideologicznych rywali z Państwa Islamskiego. Podobnie jak IS w Syrii i Iraku OAKPA pobierała podatki i czerpała zyski z pól naftowych i rafinerii. Majątek organizacji w tym najuboższym państwie Bliskiego Wschodu szacowano na 100 milionów dolarów. OAKPA wykorzystała pustkę pozostawioną przez władze i dzięki temu stała się silniejsza niż kiedykolwiek wcześniej. Nie pierwszy raz dżihadyści z Jemenu skorzystali z szansy, aby zwiększyć swoje wpływy.

Przez długie miesiące sukcesy Al-Kaidy pozostawały głównie w cieniu walk Husi z reżimem oraz wojny w Syrii. Kilka miesięcy po tym jak terroryści z OAKPA, bracia Said i Cherif Kouachi, dokonali w styczniu 2015 r. zamachu na redakcję „Charlie Hebdo" w Paryżu[30], Amerykanie przeprowadzili 12 czerwca 2015 r. w Mukalli w prowincji Hadramaut atak przy użyciu drona. Zlikwidowano wówczas kilka najważniejszych postaci organizacji, włącznie z jej przywódcą i numerem dwa w całej Al-Kaidzie – Nasirem al-Wuhajszim. Warto nadmienić, że to nadmorskie miasto zostało zdobyte przez bojowników Al-Kaidy w kwietniu 2015 r. po dwóch tygodniach walk. Od początku 2016 r. USA zintensyfikowały swoją kampanię uderzeń z powietrza. W wyniku jednego z nalotów na obiekt OAKPA w Mukalli zginęło 50 dżihadystów. Jednak w porównaniu z walką z Państwem Islamskim liczba ataków przeprowadzanych przez Amerykanów w Jemenie była niewielka. Za każdym razem USA i siły jemeńskie potrafiły odebrać terrorystom ich zdobycze, ale nigdy nie były w stanie zupełnie ich pokonać[31]. W kwietniu 2017 r. przywódca OAKPA Kasim al-Rajmi wydał oświadczenie, w którym poinformował, że jego organizacja będzie walczyć z szyickim ruchem Husi oraz jest gotowa rozpocząć, pod pewnymi warunkami, negocjacje z prezydentem Mansurem Hadim. Na początku sierpnia 2017 r. żołnierze jemeńscy wspierani przez doradców z ZEA rozpoczęli operację przeciwko OAKPA w kontrolowanej przez tę organizację części prowincji Szabwa.

Od drugiej połowy 2014 r. Państwo Islamskie próbowało budować swoje przyczółki na terenie Afganistanu. Islamski Ruch Uzbekistanu działający na pograniczu afgańsko-pakistańskim podporządkował się kalifowi Ibrahimowi, natomiast wśród talibów doszło do rozłamu, rywalizacji w skuteczności przeprowadzanych zamachów oraz do wzajemnych mordów. Przywódcą afgańsko-pakistańskich oddziałów Państwa Islamskiego został emir Hafiz Said Khan. Postawiono przed nim zadanie utworzenia Wilajetu Chorasanu na ziemiach Afganistanu, Pakistanu i Azji Centralnej[32]. Khan został zabity 26 lipca 2016 r., a jego następca Abdul Hasib – w maju 2017 r. Większość bojowników działających na tym terenie rekrutowała się z pakistańskiego Tehrik-e Taliban Pakistan (Ruchu Pakistań-

[30] G. Kepel, *Terror we Francji. Geneza francuskiego dżihadu*, Warszawa 2017, s. 239–265.

[31] A. Wejkszner, *Globalna sieć sieć Al-Kaidy*…, s.146–148; tenże, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010, s. 249–252.

[32] W Syrii działał również Batalion Chorasan, zwany Batalionem Wilków, dowodzony przez Muhsina al-Fadhliego, działacza Al-Kaidy. Kierowana przez niego organizacja współpracowała z jemeńskim konstruktorem bomb Ibrahimem al-Asirim, członkiem OAKPA. Celem Batalionu Chorasan było organizowanie zamachów terrorystycznych na Zachodzie, B. Hall, *ISIS. Państwo Islamskie*, Warszawa 2015, s. 201–204.

skich Talibów). Najbardziej aktywnie działa w prowincjach Badachszan, Kunduz, Farah, Farjab oraz na wschodzie kraju – w prowincjach Logar, Paktika, a szczególnie w Nangarhar. Zaobserwowano również zwiększoną rekrutację młodych ludzi i byłych talibów w szeregi IS. Lokalni dowódcy IS wypłacali swym żołnierzom znacznie wyższy żołd niż talibowie, co przyciągało rekrutów. W 2015 r. do Państwa Islamskiego przyłączyła się Hizb-e Islami (Partia Islamska) Gulbuddina Hekmatiara. Na początku czerwca 2015 r. jej lider zadeklarował, że wspólnie z IS zamierza walczyć w Afganistanie z ruchem talibów. Jednak to talibowie zwyciężyli w tej rywalizacji. Obecnie wydają się kontrolować 40 proc. powierzchni kraju i przynajmniej raz w tygodniu przeprowadzają ataki terrorystyczne na obiekty rządowe, bazary i centra handlowe, siedziby zagranicznych instytucji, szyickie placówki kulturalne, siły policyjne, wojskowe oraz służby bezpieczeństwa państwa.

Zwierzchność Państwa Islamskiego przyjęły również: filipińska Abu Sajaf (Ojciec Miecza) oraz indonezyjskie Dżimah Islamijja (Wspólnota Muzułmańska), i Dżimah Anszorut Tawhid (Grupa Zwolenników Jedności Boga). W tej ostatniej organizacji doszło na tym tle do rozłamu, w wyniku czego powstało Dżimah Anszorut Szariah (Stowarzyszenie Zwolenników Szariatu). Na Filipinach bojownicy Abu Sajaf, już pod sztandarami IS, zdobyli 22 maja 2017 r. dwustutysięczne miasto Marawi na wyspie Mindanao. Stało się to po tym, gdy siły rządowe próbowały aresztować przywódcę organizacji Isnilona Hapilona, który przybył do miasta na leczenie. Bojownicy Abu Sajaf dowodzeni przez Mahmuda Ahmada alias Abu Handzalah i wspierani przez grupę Maute (te siły szacowano na ponad 300 osób) wyparli wojsko, zabijali chrześcijan i wzięli do niewoli ponad 200 zakładników. Walki o miasto trwały pięć miesięcy. Dnia 23 października 2017 r. minister obrony Filipin zakomunikował zakończenie działań bojowych oraz zlikwidowanie islamistów. Zginęli Mahmud Ahmad i Hapilon. Z Marawi i z jego regionu uciekło prawie 500 tys. ludzi, a w walkach śmierć poniosło ponad 800 osób, w tym dżihadyści, cywile i wojskowi. Najbliższa przyszłość pokaże, czy dżihadyści zostali pokonani, ponieważ Abu Sajaf – aktywna od 1991 r. – ma niezwykłą zdolność do odradzania się, rekrutowania kolejnych bojowników i stwarzania nowego zagrożenia.

Popularność idei głoszonych przez Państwo Islamskie oraz spadek znaczenia Al-Kaidy spowodował, że IS zyskała na znaczeniu głównie wśród muzułmańskich ugrupowań terrorystycznych. Zagospodarowała również zaplecze finansowe i militarne Al-Kaidy oraz jej zasoby ludzkie, stając się największą, najbogatszą i najgroźniejszą organizacją terrorystyczną na świecie. Restytucja kalifatu miała głębokie przesłanie polityczne, ideologiczne i religijne ze względu na jego znaczenie w tradycji muzułmańskiej. W związku z tym obecnemu pokoleniu dżihadystów walczącemu o rozwój i utrzymanie kalifatu trudno będzie pogodzić się z jego upadkiem, do którego przyczyniły się w znacznym stopniu siły znienawidzonego przez ekstremistów Zachodu. Znowu odżyła pamięć o czasach kolonialnych i dominacji Wielkiej Brytanii i Francji na Bliskim Wschodzie. Oprócz tych państw oraz Stanów Zjednoczonych pojawił się też nowy agresor – Rosja. Zdrajcami i wrogami pozostają władze w Syrii i Iraku, szyici i Kurdowie, którzy muszą mieć na uwadze to, że będą obiektami ataków

terrorystycznych. Państwo Islamskie jako hybrydowa struktura terrorystyczna o światowym zasięgu wciąż będzie stanowić szczególnie groźne wyzwanie dla policji i służb specjalnych wielu państw. Ich funkcjonariusze muszą liczyć się z nieprzejednaną wrogością, fanatyzmem, pogardą dla śmierci i okrucieństwem. Pod znakiem zapytania stoi dalsza konfrontacja między IS i Al-Kaidą. Nie można wykluczyć scenariusza, że konflikt zostanie zastąpiony formą porozumienia lub nawet współpracy np. w ramach organizowania i przeprowadzania zamachów terrorystycznych. Taki jednostkowy przykład zaistniał w styczniu 2015 r. w Paryżu, gdy bracia Said i Cherif Kouachi, związani z Al-Kaidą, przeprowadzili atak na redakcję tygodnika „Charlie Hebdo", a Amedy Coulibaly – współdziałający z nimi i deklarujący swoją przynależność do IS – przeprowadził zamach na żydowski supermarket.

Do unormowania relacji pomiędzy IS i Al-Kaidą może doprowadzić zmarginalizowanie znaczenia IS i śmierć kalifa Abu Bakra al-Bagdadiego. Zmiany w kierownictwie Al-Kaidy też mogą przyczynić się do poprawy stosunków między obu organizacjami. Wydaje się, że w najbliższym czasie ster w tym ugrupowaniu przejmie 28-letni Hamza bin Laden, syn Osamy i jego trzeciej żony Saudyjki Hajriji Sabar, nazywany „księciem dżihadu". Może on zostać nową twarzą odmienionej Al-Kaidy. W sierpniu 2015 r. Hamza bin Laden po raz pierwszy wystąpił w nagraniu razem z Ajmanem az-Zawahirim, które ukazało się w cyberprzestrzeni. Wezwał wówczas wiernych do prowadzenia dżihadu w Waszyngtonie, Londynie, Paryżu i Tel Awiwie. Potem występował jeszcze trzy razy, gorliwie zachęcając do kolejnych ataków, dokonywanych przede wszystkim przez „samotne wilki", oraz do pomszczenia swojego ojca. W sierpniu 2016 r. w internecie pojawiło się kolejne nagranie, w którym wzywał do zmiany reżimu w Arabii Saudyjskiej, rządzonej przez „wielkich kryminalistów i złodziei" oraz amerykańskich agentów. Według niego władze w tym kraju muszą być zastąpione przez nowy rząd, który bardziej sprawiedliwie będzie rozdzielał dochody z ropy naftowej oraz będzie aktywizował obywateli do dżihadu. Jednak prawdziwym grzechem Saudów jest, według niego, ich postawa w Jemenie, gdzie od marca 2015 r. toczą krwawą wojnę przeciwko szyickim rebeliantom z ruchu Husi. Hamza oskarżył Rijad o sprzyjanie szyitom i zwalczanie dżihadystów sprzymierzonych z Al-Kaidą, co stanowi (…) *podwójną zdradę przeciw muzułmanom w Jemenie*[33]. Mimo że źródłem charyzmy Hamzy jest niewątpliwie jego nazwisko (Osama bin Laden był organizatorem największego zamachu terrorystycznego w historii), Hamza ma własną koncepcję dżihadu. Jest przeciwny spektakularnym, długo przygotowywanym zamachom, które mogą zostać wykryte przez służby specjalne. Podobnie jak Państwo Islamskie, wzywa do atakowania Amerykanów, Europejczyków oraz prozachodnich muzułmanów gdziekolwiek się znajdują, każdą dostępna bronią. W odróżnieniu od Az-Zawahiriego nie krytykował kalifatu, co po upadku IS może przyczynić się do zwiększenia liczby jego zwolenników i pozwoli odnowić szeregi Al-Kaidy lub organizacji wyrosłej na jej fundamencie[34]. Zdając sobie sprawę z nowego zagrożenia, na przełomie września i października 2017 r. 40 operatorów

[33] https://wiadomosci.wp.pl/syn-osamy-bin-ladena-nowym-liderem-al-kaidy-hamza-wzywa-do-walki-6029048256705665a [dostęp: 23 VIII 2017].

[34] M. Urzędowska, *Powrót Al-Kaidy i Ben Ladena*, „Gazeta Wyborcza" z 2 listopada 2017 r.

brytyjskiej SAS przybyło do Syrii, gdzie ma przebywać Hamza, aby go wytropić i zabić[35]. Jak do tej pory – bezskutecznie. Pojawienie się w mediach tej informacji może przysporzyć młodemu Bin Ladenowi dodatkowych sojuszników.

Bibliografia:

Danielewicz K., *Terroryzm w Afryce. Geneza oraz przebieg konfliktu w Mali w latach 2012–2014*, Oświęcim 2016, Napoleon V.

Hall B., *ISIS. Państwo Islamskie*, Warszawa 2015, Muza.

Kepel G., *Terror we Francji. Geneza francuskiego dżihadu*, Warszawa 2017, Dialog.

Laurent S., Kaniowska E., *Kalifat terroru. Kulisy działania Państwa Islamskiego*, Warszawa 2015, W.A.B.

Olomojobi Y., *Frontiers of Jihad. Radical islam in Africa*, Ibadan 2015, Safari Books.

Sageman M., *Sieci terroru*, Kraków 2008, Wydawnictwo Uniwersytetu Jagiellońskiego.

Szymański E., *Tradycje i legendy ludów Afryki Północnej*, Kraków 1994, Nomos.

Urzędowska M., *Powrót Al-Kaidy i Ben Ladena*, „Gazeta Wyborcza" z 2 listopada 2017 r.

Warrick J., *Czarne flagi. Geneza Państwa Islamskiego*, Warszawa 2017, W.A.B.

Weiss M., Hassan H., *ISIS. Wewnątrz armii terroru*, Warszawa 2015, Burda Publishing Polska.

Wejkszner A., *Globalna sieć Al-Kaidy. Nowe państwo islamskie?*, Warszawa 2017, Difin.

Wejkszner A., *Państwo Islamskie. Narodziny nowego kalifatu?*, Warszawa 2016, Difin.

Wojciechowski S., Osiewicz P., *Zrozumieć współczesny terroryzm*, Warszawa 2017, Difin.

Abstrakt

Zwycięstwo militarne nad Państwem Islamskim nie oznacza pokonania tej organizacji terrorystycznej. Najprawdopodobniej jej członkowie przejdą do konspiracji i nadal będą przeprowadzać ataki. Wciąż aktywne są organizacje sprzymierzone z Państwem Islamskim operujące w zagranicznych wilajetach (prowincjach) kalifatu: na Półwyspie Synaj, w Libii, Nigerii oraz Afganistanie. Działają również ugrupowania, których przywódcy w latach 2014–2015 złożyli przysięgę lojalności kalifowi Ibrahimowi

[35] http://www.dailymail.co.uk/news/article-4938874/SAS-begin-mission-kill-capture-Osama-Bin-Laden-s-son.html [dostęp: 6 X 2017].

(Abu Bakrowi al-Bagdadiemu), a wcześniej były związane z Al-Kaidą lub tworzyły jej filie. Takich organizacji jest łącznie ponad 40. Część z nich podzieliła się na skutek wewnętrznych sporów dotyczących opowiedzenia się po jednej ze stron: Al-Kaidy lub ISIS/IS – organizacji skonfliktowanych ze sobą od 2013 r.

Oprócz Bliskiego Wschodu główną areną aktywności i rywalizacji ugrupowań dżihadystycznych jest Afryka Północna obejmująca kraje Sahary i Sahelu, gdzie od drugiej połowy 2014 r. zwiększały się wpływy Państwa Islamskiego. Chociaż IS poniosło dotkliwą klęskę w Syrii i Iraku, to w Afryce, pomimo osłabienia jego pozycji, zachowało zdolności operacyjne do przeprowadzenia zamachów terrorystycznych. Skutki terrorystycznej aktywności Państwa Islamskiego i innych organizacji z nim powiązanych lub działających pod własnym szyldem (np. ruch talibów w Afganistanie) były tragiczne. Najbardziej krwawy był rok 2014. Na całym świecie zginęło wówczas 32 858 osób. Dla porównania: w 2016 r. zginęły 25 673 osoby, czyli prawie o 22 proc. mniej niż w 2014 r. Nie zmienia się przy tym lista krajów najbardziej zagrożonych terrorem. Pierwsza piątka to Irak, Nigeria, Afganistan, Syria i Pakistan. To w tych krajach zabito aż 75 proc. wszystkich ofiar.

Bezpieczeństwo w Europie może w najbliższym czasie ulec znacznemu pogorszeniu. Propaganda dżihadystyczna wciąż trafia na podatny grunt i będzie bardziej skuteczna, gdy oczekiwania imigrantów coraz bardziej będą się rozmijać z rzeczywistością, a postawy roszczeniowe zamienią się w gniew. Będą temu sprzyjać deportacje osób, które z różnych względów utraciły prawo pobytu w Europie, w tym z powodu popełnionych przestępstw kryminalnych, oraz zaostrzanie prawa azylowego i warunków przyznawania zasiłków, co zapowiedziały m.in. Dania, Austria, Niemcy i Francja – ze względu na zacieranie się granic miedzy uchodźcami a imigrantami ekonomicznymi.

Do zwiększenia zagrożenia może dojść w wyniku poprawienia relacji między IS i Al-Kaidą spowodowanej m.in. śmiercią Abu Bakra al-Bagdadiego. Zmiany w kierownictwie Al-Kaidy też mogą przyczynić się do poprawy stosunków między obu organizacjami. Wydaje się, że w najbliższym czasie ster w tym ugrupowaniu przejmie 28-letni Hamza bin Laden, syn Osamy, nazywany „księciem dżihadu". W odróżnieniu od obecnego lidera Al-Kaidy Ajmana az-Zawahiriego, nie krytykował on kalifatu, co po upadku IS może przysporzyć mu zwolenników i spowodować odnowienie szeregów Al-Kaidy lub organizacji wyrosłej na jej fundamencie.

Słowa kluczowe: Al-Kaida, ataki terrorystyczne, Bliski Wschód, Państwo Islamskie, salafici, talibowie, wahhabizm.

Danuta Gibas-Krzak

Terroryzm na Bałkanach. Geneza – nurty – prognozy

Wprowadzenie

Chociaż w nauce istnieje ponad dwieście definicji terroryzmu, to jednak trudno byłoby wyodrębnić tę najwłaściwszą, oddającą precyzyjnie podejmowaną problematykę oraz tłumaczącą w sposób właściwy specyfikę ładu międzynarodowego w epoce globalizacji. Nie zmienia to jednak tego, że współczesny terroryzm jest zjawiskiem zarówno politycznym, jak i społecznym, a jego geneza tkwi w skomplikowanych procesach zachodzących w społeczeństwach. Wielu badaczy uważa, że lepiej jest określać różne odmiany terroryzmu, niż próbować formułować jedną definicję. W ramach tego paradygmatu można mówić o terroryzmie państwowym, etnicznym czy międzynarodowym. W nauce stosuje się także pojęcie zagrożenie asymetryczne, które odnosi się do badań nad wojną i konfliktami[1]. Trudno zaprzeczyć, że terroryzm – postrzegany często jako nieselektywny i bezsensowny – jest w istocie bardzo świadomym i planowym zastosowaniem przemocy[2]. Brak jednej typologii, oddającej naturę tego zjawiska, sprawia, że badacze dokonują kolejnych prób systematyzacji terroryzmu, przyjmując podział na założenia doktrynalne i cele ideologiczne. Powszechnie stosowanym terminem jest terroryzm międzynarodowy rozumiany jako stosowanie siły lub groźby jej użycia przez jednostki lub grupy osób przeciw osobom, miejscom lub rzeczom naruszającym prawo międzynarodowe, z zamiarem wywołania stanu zastraszenia grupy społecznej (etnicznej), społeczeństwa, narodu lub społeczności międzynarodowej dla osiągnięcia celów politycznych. Po zimnej wojnie szczególnie niebezpieczne są: współpraca poszczególnych organizacji terrorystycznych w zakresie szkolenia i dawania schronienia komandom terrorystycznym, wspólne działanie oraz sięganie do metod terrorystycznych przez walczące o wyzwolenie narody i grupy polityczne, etniczne oraz ruchy religijne. Niepokój budzi prowadzenie akcji o charakterze terrorystycznym przez służby specjalne, a także współpraca grup terrorystycznych ze strukturami przestępczości zorganizowanej oraz wspólne ich działania ze służbami specjalnymi[3].

Działania terrorystyczne były od wieków stosowane jako skuteczne narzędzie walki zarówno przeciw silniejszemu przeciwnikowi, jak i własnemu społeczeństwu, u jego podstaw bowiem występuje zastraszenie podmiotu, który był poddany działaniom terrorystycznym.

Jak każde zjawisko społeczno-polityczne, tak i terroryzm ewoluował na przestrzeni wieków, przybierając różne formy, aż w końcu stał się przekleństwem naszych

[1] R. Borkowski, *Terroryzm ponowoczesny. Studium z antropologii polityki*, Toruń 2007, s. 43.
[2] B. Hoffman, *Oblicza terroryzmu*, Warszawa 1999, s. 175.
[3] *Encyklopedia Politologii*, t. 5, M. Żmigrodzki (red.), Zakamycze 2002, s. 365.

czasów. W epoce globalizacji terroryzm to głównie brutalne akty – akcje i operacje prowadzone przez organizacje powiązane ideologicznie i religijnie z islamem. Mimo skomplikowanej typologii omawianego zjawiska, w perspektywie historycznej można wymienić następujące nurty terroryzmu:

– terroryzm anarchistyczny XIX w. i początku XX w.,
– terroryzm lewacki lat 60. i 80. XX w.,
– terroryzm prawicowy końca XX w. i początku XXI w.,
– terroryzm ponowoczesny, religijny, globalny[4].

Mniej znane są inne aspekty działalności terrorystycznej, obserwowane zwłaszcza w południowo-wschodniej części Starego Kontynentu. W żadnym z pozostałych regionów Europy nie znajdzie się tak szerokiego spektrum różnych form terroryzmu, co niewątpliwie stanowi o wyjątkowości tego obszaru zarówno dla historyków, politologów, jak i przedstawicieli innych nauk. Na przestrzeni przeszło stu lat Bałkany były areną działalności różnych organizacji wywrotowych oraz licznych zamachów terrorystycznych, które miały decydujący wpływ na dzieje świata. Za sprawą Gavrilo Principa i jego towarzyszy, wywodzących się z małej organizacji terrorystycznej „Młoda Bośnia", doszło do zamachu w Sarajewie i zabicia arcyksięcia Franciszka Ferdynanda. To z kolei stało się bezpośrednią przyczyną wybuchu Wielkiej Wojny 1914–1918. Kilkanaście lat wcześniej na obszarze Bałkanów rozpoczęli działalność macedońscy rewolucjoniści spod znaku Wewnętrznej Macedońskiej Organizacji Rewolucyjnej (WMRO), którzy z determinacją walczyli początkowo z panowaniem tureckim, a w późniejszych latach swoje działania skierowali przeciwko Jugosławii. Praktycznie zupełnie niezbadane pozostaje w polskiej (a także światowej) historiografii zjawisko terroru poustaszowskiego i poczetnickiego. Dużo lepiej natomiast został opisany związek terroryzmu pochodzenia bałkańskiego z organizacjami współczesnej odmiany islamskiego terroru. Wydaje się jednak, że ten problem w odniesieniu do Bałkanów jest niedostrzegany lub marginalizowany przez decydentów politycznych, zwłaszcza w Europie Zachodniej[5].

W tym kontekście jest ważne, aby specyficzny terroryzm bałkański został poddany odrębnym badaniom, przede wszystkim o charakterze heurystycznym, z zastosowaniem – w szerokim zakresie – metod: analizy, syntezy oraz porównawczej. Metoda analizy pozwala na przetworzenie materiału badawczego. Posługując się nią, dąży się do rozłożenia opisywanych wydarzeń na zbiór pojedynczych, szczególnych cech i elementów zdarzeń. Metoda syntezy pozwala na sformułowanie twierdzeń o charakterze ogólnym, w tym uogólnienie szczegółowych danych badanego materiału. Użycie tej metody badawczej jest niezbędne podczas zamykania kolejnych etapów badań i procesu uzasadnienia sądów i ocen. Częste stosowanie syntezy wiąże się z użyciem metody indukcyjnej pozwalającej na prowadzenie tzw. wnioskowania uogólniającego (wnioskowanie indukcyjne). Ta metoda wymaga przeprowadzenia badań opartych na

[4] R. Borkowski, *Terroryzm ponowoczesny*…, s. 49.
[5] Zob. *Terrorism in the Balkans in the 20th and 21st century*, D. Gibas-Krzak (ed.), Torun 2018.

faktach, które stanowią podstawę naukowego wnioskowania. Zastosowanie metody porównawczej pozwala śledzić sposób i formy działań terrorystycznych w różnych epokach, państwach i regionach. Można wówczas stwierdzić, na ile badane wydarzenie było specyficzne, a co było w nim typowego. Ta metoda umożliwia stosowanie różnego rodzaju analogii dotyczących zwykle porównywania danych pochodzących z różnych terenów, państw czy regionów. Metoda porównawcza służy także uzasadnieniu słuszności określonej tezy. Dzięki jej zastosowaniu dokonuje się ważnych uogólnień, które są rezultatem wnioskowania porównawczego. Biorąc pod uwagę zastosowanie powyższych metod, celem niniejszego artykułu jest sklasyfikowanie odmian terroryzmu występującego na Bałkanach, umiejscowienie w czasie jego początków, przedstawienie rozwoju oraz rozważenie charakteru współczesnego oblicza tego terroryzmu. Za pomocne uznano postawienie pytań badawczych:

1. Jaka jest geneza zjawiska terroryzmu na Bałkanach?
2. Jak przebiegała ewolucja terroryzmu bałkańskiego?
3. Jakie czynniki decydowały o rozwoju działalności terrorystycznej w tej części Europy?
4. W jakim stopniu rozpad komunistycznej Jugosławii wpłynął na polaryzację stosunków narodowościowych i kształtowanie się radykalnych ruchów religijnych związanych z islamskim terroryzmem?
5. Czy rzeczywiście Bałkany są miejscem azylu dla terroryzmu motywowanego fundamentalizmem religijnym?

Główna hipoteza postawiona w artykule brzmi: Bałkany ze względu na warunki geograficzne (naturalne) stwarzają znakomitą możliwość rozwoju baz i obozów treningowych dla terrorystów powiązanych z globalnym dżihadem. Stanowi to zagrożenie bezpieczeństwa Europy i jej demokratycznych społeczeństw z powodu prawdopodobieństwa wzniecenia konfliktu nie tylko lokalnego, lecz także mającego szeroki zakres, na skalę międzynarodową.

Odmiany terroryzmu na Bałkanach w wiekach XIX i XX

Historia terroryzmu na Bałkanach jest związana z kształtowaniem się ruchów narodowowyzwoleńczych w tej części Europy. Narody bałkańskie posługiwały się metodami terrorystycznymi niemal od początku zmagań z tureckim najeźdźcą, co miało im pomóc w odzyskaniu niepodległości. Za jednego z prekursorów terroryzmu w tym regionie trzeba uznać powstałą w 1893 r. Wewnętrzną Macedońską Organizację Rewolucyjną, która dążąc do wyzwolenia ludności zamieszkałej na ziemiach słowiańskich, stosowała metody terrorystyczne. Tę niechlubną kartę zapisały zwłaszcza napawające grozą działania macedońskich „szwadronów śmierci" dokonujące bezwzględnych mordów i spektakularnych ataków na bogatych członków rodzin tureckich. To ugrupowanie zorganizowało w 1903 r. największe w dziejach narodu macedońskiego po-

wstanie zwane ilindeńskim[6]. Separatyści macedońscy włączyli się aktywnie również w proces rozbijania Królestwa Jugosławii w dwudziestoleciu międzywojennym, a ich sojusznikami zostali członkowie chorwackiego ruchu Ustasza. W 1934 r. w Marsylii macedońscy i chorwaccy ekstremiści dokonali zamachu, w którym śmierć ponieśli: Aleksander I Karađorđević, król Jugosławii, oraz Louis Barthou, francuski minister spraw zagranicznych. Ustasze, często będący egzemplifikacją ruchów stosujących metody terrorystyczne[7], byli znani także z przeprowadzanych w Belgradzie i Zagrzebiu zamachów, w latach 30. XX w. próbowali m.in. wzniecić powstanie w okolicach miasta Zadar i regionach Banija oraz Kordun, którego celem było oderwanie Chorwacji od Królestwa Jugosławii[8].

W międzywojennej Rumunii działalność terrorystyczną przypisywano organizacji politycznej pod nazwą Żelazna Gwardia. Została ona założona w lipcu 1927 r. jako Legion Archanioła Michała[9] i w momencie utworzenia była jedynie grupą secesjonistyczną z Ligi Obrony Narodowo-Chrześcijańskiej (Liga Apărări Naţional Creşine, LANC) funkcjonującą na terenie Mołdawii od początku lat 20. XX w. Wkrótce jednak terror i akcja bezpośrednia stały się istotnymi elementami walki tej organizacji. „Komanda śmierci" LANC dokonywały ataków na urzędników państwowych wysokiego szczebla (m.in. zamordowały premiera) oraz niszczyły obiekty użyteczności publicznej[10]. Nie można bowiem zapominać, że Bałkany były widownią różnorodnych nurtów i form terroryzmu. Zabójstwa polityczne, które można zakwalifikować jako akty terroru politycznego, były także dość częstym zjawiskiem w dziejach międzywojennej Jugosławii oraz Bułgarii. Po metody terrorystyczne sięgały również radzieckie służby specjalne kontrolujące Komintern i partie komunistyczne państw bałkańskich. Ich członkowie, zwłaszcza w pierwszych latach po zakończeniu Wielkiej Wojny, stosowali na szeroką skalą terror indywidualny, który miał być pierwszą fazą rewolucji proletariackiej. Liczne zamachy często były nieudane, jak ten na bułgarskiego cara Borysa III na przełęczy Arabakonak. Nie była to pierwsza, i notabene – nie ostatnia, porażka zarówno Kominternu, jak i bolszewickich służb specjalnych, jednak skutkowała tym, że władze na Kremlu zostały zmuszone, przynajmniej częściowo, do porzucenia idei o przeniesieniu działań rewolucyjnych na inne kraje[11].

---

[6] T. Wasilewski, *Historia Bułgarii*, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1988, s. 207; Z. Klejn, *Bułgaria. Szkice z dziejów najnowszych*, Pułtusk 2005, s. 54 oraz w wielu miejscach.

[7] D. Trifunović, *Threat to international security – terrorism in South East Europe*, w: *Służby specjalne w systemie bezpieczeństwa państwa. Przeszłość – teraźniejszość – przyszłość. Materiały i studia*, t. 2, A. Krzak, D. Gibas-Krzak (red.), Szczecin 2012, s. 279.

[8] J. Wilamowski, K. Szczepanik, *Ustasze i separatyzm chorwacki*, „Przegląd Historyczny" 1983, z. 1, s. 82–90.

[9] N.M. Nagy Talavera, *The Green Shirts and the Others. A history of fascism in Hungary and Romania*, Iaşi 2001, s. 370.

[10] A. Dubicki, *Terror as a method of fighting of the Iron Guard*, w: *Terrorism in the Balkans in the 20th*..., s. 52–60.

[11] A. Krzak, *Active intelligence service (terrorism) of the Comintern and Soviet secret service in Bulgaria in the 1920s – case study*, w: *Terrorism in the Balkans in the 20th*..., s. 36–48.

W okresie II wojny światowej w skomplikowanej sytuacji, jaka miała miejsce na ziemiach okupowanej Jugosławii, doszło do zinstytucjonalizowania terroru jako formy ludobójczej eksterminacji. Była ona stosowana przede wszystkim przez władze Niezależnego Państwa Chorwackiego (Nezavisna Hrvatska Drzava, NDH) i ich sojuszników. Powołanie do życia w 1941 r. marionetkowego państwa kierowanego przez ustaszy stanowiło realizację idei o państwie chorwackim, o które wcześniej walczono za pomocą metod terrorystycznych. Terror państwowy został skierowany nie tylko przeciw Serbom, Żydom czy Romom, lecz także przeciw Chorwatom będącym oponentami rządów Ante Pavelicia. Należy jednak pamiętać, że II wojna światowa na Bałkanach była okresem powszechnego terroru państwowego, stosowanego przez władze okupacyjne oraz rządy kolaborujące z państwami Osi.

Po zakończeniu II wojny światowej komunistyczne władze Jugosławii, Albanii, Bułgarii i Grecji prowadziły przez kilka kolejnych lat intensywne działania, w tym akcje terrorystyczne, w celu wyeliminowania przeciwników politycznych. Jugosławia wybrała opcję pozablokową, nie uchroniło to jej jednak przed atakami ze strony światowej opinii publicznej, która krytykowała ją za wspieranie międzynarodowego terroryzmu. Jugosławia bowiem czerpała znaczne zyski z handlu bronią dostarczaną do krajów Trzeciego Świata i w ten sposób zarabiała ok. 700 mln rocznie[12]. Kolejnym przykładem wspomagania działań terrorystycznych miało być udzielenie przez komunistyczne władze schronienia m.in. sławnemu terroryście Carlosowi, członkom organizacji Baader-Meinhof oraz Abu Abbasowi z Frontu Wyzwolenia Palestyny, znanemu z porwania w 1985 r. włoskiego statku wycieczkowego MS Achille Lauro. Nie można zapominać, że w Jugosławii w latach 80. XX w. istniały bazy szkoleniowe palestyńskich i libańskich terrorystów. W Wojwodinie do końca 1984 r. wyszkolono na kursach wywiadowczych ponad 800 osób, w tym również członków ruchów narodowowyzwoleńczych i organizacji terrorystycznych z państw Trzeciego Świata[13]. W latach 1945–1990 służby specjalne Jugosławii dokonywały ataków na przedstawicieli antyjugosłowiańskiej emigracji, zabijając 73 osoby[14]. Źródła serbskie podają, że Josip Broz Tito i kanclerz Niemiec Willy Brandt zawarli tajne porozumienie, dzięki któremu było możliwe dokonywanie zabójstw jugosłowiańskich dysydentów na terenie Niemiec. Jednym z zabójców na zlecenie miał być Željko Ražnatović, ps. „Arkan", przyszły dowódca serbskich oddziałów paramilitarnych znanych ze zbrodni wojennych popełnionych w czasie wojny domowej związanej z rozpadem komunistycznej Jugosławii[15]. W 1981 r. w Niemczech Zachodnich odbył się proces trzech jugosłowiańskich agentów tajnej policji. Zostali oni skazani na wieloletnie

[12] I. Lučić, *Bosnia and Herzegovina and terrorism*, „National security and the future" 2001, nr 3–4, s. 117.

[13] Tamże, s. 115.

[14] *Emigrant Croats who were victims of federal terror after 1945*, „Slobodna Dalmacija" z 15 sierpnia 2000 r., s. 10.

[15] M. Lopušina, *Tajne srpske policije i zloupotrebe*, w: *Służby specjalne w systemie bezpieczeństwa*…, s. 213.

więzienie za planowanie i przygotowanie zabójstw jugosłowiańskich (chorwackich) emigrantów[16]. O działalność terrorystyczną są podejrzewani także serbscy politycy, na czele z nieżyjącym, byłym prezydentem Slobodanem Miloševiciem. Za jego rządów doszło do bliskiej współpracy policji i służb specjalnych ze środowiskiem przestępczym, a najbardziej dramatycznym przykładem tej współpracy było zabójstwo premiera Serbii Zorana Đinđicia w 2003 r.[17]

Chorwackie środowisko dysydenckie odpłaciło komunistycznej władzy atakami terrorystycznymi. Nurty ekstremistyczne jugosłowiańskiej emigracji przygotowały w latach 1946–1985 przeszło 400 ataków terrorystycznych w kraju i za granicą, w których śmierć poniosły 102 osoby, a 330 zostało rannych. Celem utworzonej w 1961 r. organizacji Hrvatsko revolucionarno bratstvo (HRB) było wywołanie powstania w Jugosławii i uzyskanie przez Chorwację niepodległości. HRB dokonała 120 ataków, powodując śmierć 53 osób oraz raniąc 118. Terroryści z HRB przygotowali także zamach na Josipa Broz Tito (1976 r.), atak na jugosłowiański klub w Paryżu (1966 r.), ambasadę Jugosławii w Niemczech (1966 r.) oraz napad na wicekonsula Jugosławii w Lyonie (1969 r.). Część członków HRB weszła w skład grupy terrorystycznej związanej z ruchem ustaszy, która w 1972 r. podczas spotkań konspiracyjnych w Austrii przygotowywała zbrojne powstanie mające na celu wyzwolenie Chorwacji[18].

Nurt terroryzmu islamskiego na Bałkanach

Początki terroryzmu muzułmańskiego zazwyczaj są utożsamiane ze średniowieczną sektą asasynów posługujących się metodami skrytobójczymi oraz terrorem. Po pierwszej wojnie światowej powstała w Egipcie nacjonalistyczno-religijna organizacja Al-Ichwan al-Muslimin (Bracia Muzułmanie). Jej celem był powrót do tradycji prawdziwego, czyli wczesnego, islamu oraz wyzwolenie świata muzułmańskiego od cywilizacji zachodniej, która niosła za sobą demoralizację prawdziwego wyznawcy i w konsekwencji jego upadek. Członkowie Braci Muzułmanów nadali zasadzie fundamentalizmu islamskiego ramy instytucjonalne. Głosili dżihad pojmowany, tylko początkowo, jako metodę pokojowego upowszechniania zasad religijnych. Jednak z czasem dżihad przekształcił się i przybrał formę działalności terrorystycznej, stosowanej przez prawie wszystkie organizacje fundamentalistyczne, ekstremistyczne i terrorystyczne[19].

Na Bałkanach terroryzm związany z ekstremalnymi nurtami islamu ujawnił się dopiero wraz z rozpadem Jugosławii i walką, jaką stoczyły skonfliktowane narody i narodowości tego państwa w czasie wojny domowej (1992–1995), i zakorzenił się na tym terenie. W okresie zimnej wojny społeczeństwo Jugosławii nie ulegało prawie

[16] I. Lučić, *Bosnia and Herzegovina*…, s. 117. Zob. M. Doder, *Jugoslavenska neprijateljska emigracja*, Zagreb 1989.

[17] M. Lopušina, *Tajne srpske policije*…, s. 214–220.

[18] D. Trifunović, *Threat to international security*…, s. 279.

[19] K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, s. 7. Zob. J. Hauziński, *Asasyni. Legendarni zabójcy w czasach krucjat*, Poznań 2016.

żadnym wpływom radykalnych zasad islamu. W 1971 r. muzułmanie uzyskali w Jugosławii status odrębnej narodowości, lecz ich dość powierzchowna religijność miała świecki charakter. Bezpośrednim impulsem do wzrostu zaangażowania religijnego miejscowych wyznawców islamu stało się dopiero zwycięstwo rewolucji Chomeiniego[20]. W latach 70. XX w. Alija Izetbegović, przyszły prezydent Bośni i Hercegowiny, wezwał muzułmanów do stosowania „Islamskiej Deklaracji", inicjując w ten sposób rozwój ruchu islamistycznego[21]. Współcześnie terroryzm związany z ekstremalnymi nurtami islamu wiąże się z obecnością fundamentalistów muzułmańskich i wzrostem ich wpływów w tym regionie.

Ważnym aspektem dominacji wyznawców islamu stał się wzbudzający liczne polemiki udział muzułmańskich najemników w wojnie domowej. Przypuszcza się, że w Bośni i Hercegowinie walczyło od 1500 do 3500 ochotników, zwanych „wojownikami Boga (Allaha)". Niektóre statystyki wskazują, że na początku 1995 r. ich liczba mogła dochodzić nawet do 20 tys. Pierwsi najemnicy zostali zwerbowani w 1992 r. przez wicepremiera sarajewskiego rządu Muhameda Čengicia, wysłanego do Turcji z zadaniem zdobycia broni, amunicji oraz zebrania najemników. „Wojownicy Boga" przybyli z krajów muzułmańskich: Arabii Saudyjskiej, Pakistanu, Turcji, Algierii, Afganistanu, Egiptu, Sudanu, Iranu, Syrii. Wielu z nich było weteranami wojny w Afganistanie bądź należało do różnych organizacji terrorystycznych: Al-Kaidy, Islamskiej Grupy Zbrojnej, Hezbollahu, Hamasu, Gama El-Islamiji. Walczyli oni w imię Allaha, a ich celem stało się szerzenie idei panislamizmu na terenie Bośni i Hercegowiny, chociaż część z nich pobierała znaczne kwoty pieniędzy[22]. Islamscy fundamentaliści popełnili w szeregach armii bośniackiej wiele zbrodni wojennych. Jak poinformował w raporcie z 1993 r. specjalny obserwator ONZ Tadeusz Mazowiecki, mudżahedini działający w rejonie Jablanicy wypędzali i mordowali tych mieszkańców, którzy nie byli muzułmanami. Szczególną brutalnością wyróżniała się 7 Brygada 3 Korpusu (El Dżihad). Jej członkowie chełpili się popełnieniem wielu zbrodni wojennych. Bataliony Zelena Legija i Gerila oraz jednostka muzułmańska z miasta Tešanj – Al Mudžahedin były znane z mordowania wziętych do niewoli przeciwników, szczególnie Serbów, którym odcinano głowy[23]. Do Międzynarodowego Trybunału Karnego dla byłej Jugosławii (International Criminal Tribunal for the former Yugoslavia, ICTY) wpłynęły oskarżenia m.in. przeciwko dowódcom 3 Korpusu – Enverovi Hadžihasanoviciovi i Mehmedowi Alagiciowi, którym zarzucono popełnienie zbrodni wojennych[24]. Na zaję-

[20] N. Beloff, *Tito's flawed legacy. Yugoslavia and the West: 1939–84,* London 1985, s. 216.

[21] W opublikowanej w 1970 r. *Islamskiej Deklaracji* A. Izetbegović zawarł idee budowy bałkańskiego państwa muzułmańskiego, I. Aralica, *Što sam rekao o Bosni,* Zagreb 1995, s. 88.

[22] D. Džamić, *Psi rata na Balkanu. Strani plaćenici u ratnim sukobima na prostorima bivše Jugoslavije*, Beograd 2001, s. 204–207.

[23] Tamże, s. 209.

[24] Wbrew szablonowym poglądom, że zbrodniarzami wojennymi w wojnie jugosłowiańskiej pod koniec XX wieku byli przede wszystkim Serbowie, także przedstawiciele narodowości i religii muzułmańskiej (oraz Chorwaci) zostali postawieni w stan oskarżenia jako winni aktów barbarzyńskich i zbrodni, które zostały popełniane w czasie tego krwawego i brutalnego konfliktu.

tych terenach starali się wprowadzić surowe zasady religijne i obyczajowe, zmuszając mieszkańców do życia zgodnie z regułami szariatu (m.in. dziewczynom zabroniono pod groźbą kary chodzenia w krótkich sukienkach, a starszym kobietom obowiązkowo nakazano nosić hidżab[25]).

Bałkański dżihad rozwijał się dzięki znacznemu wsparciu państw muzułmańskich. W latach 1992–1995 Iran przekazał władzom w Sarajewie pomoc finansową oraz logistyczną[26]. W sprawozdaniu Kongresu USA ze stycznia 1997 r. podkreślono, że irańscy Strażnicy Rewolucji integrowali się z bośniackimi strukturami wojskowymi. Irański wywiad (Vezarat-e Ettela'at va Amniat-e Keshvar, VEVAK) zorganizował na terytorium całego kraju siatki agencyjne, a Irańczycy kontrolowali dużą część tamtejszego aparatu bezpieczeństwa. Narzędziem islamizacji stały się służby specjalne (np. Muslimanska Obaveštajna Služba, MOS), które w czasie wojny utrzymywały związki z Osamą bin Ladenem i Al-Kaidą oraz z arabskimi organizacjami wspierającymi dżihad. Przykładem tego są kontakty m.in. z Tvaik Grupa stanowiącą, według niemieckiej służby wywiadu BND, przykrycie dla wywiadu saudyjskiego (oficjalnie zajmowała się ona wynajmem samochodów w Europie). MOS wydawała bośniackie paszporty członkom organizacji terrorystycznych, którzy brali udział w walkach na Bałkanach. Bośniaccy dyplomaci sprzedawali paszporty nawet pospolitym przestępcom, a ich koszt miał wynosić do 500 dolarów za jeden dokument[27]. W maju 1992 r. powstał zespół Ševe, w którego skład weszli byli oficerowie wywiadu jugosłowiańskiego zajmujący się zwalczaniem wewnętrznych przeciwników. Na jego czele stanął Nedžad Ugljen, od wiosny 1994 r. odpowiedzialny za osobistą ochronę Izetbegovicia[28]. Z działalnością tego zespołu był również związany Enver Mujezinović, były major jugosłowiańskiego kontrwywiadu. Grupa przeprowadzała ataki terrorystyczne na serbską i chorwacką ludność, których dokonywali snajperzy zwerbowani wcześniej do służby w Sarajewie. Ataki na cywilów – Serbów i Chorwatów – miały ich zmusić do opuszczenia miasta[29]. Ševe zajmował się także eliminowaniem wrogów politycznych[30]. Latem 1993 r. muzułmańskie siły specjalne zleciły dokonanie zamachu na Fikreta Abdicia. Okazał się on niewygodny, gdyż występował przeciwko legitymizacji prezydentury Izetbegovicia i głosił, że to on – zgodnie z wynikiem wyborów – powinien sprawować tę funkcję. Postulował porozumienie się z Serbami i Chorwatami i rozwijanie współpracy gospodarczej z nimi, ostro krytykował fanatyzm religijny i nieustępliwość w kontynuowaniu wojny domowej, która, jego zdaniem, dawno mogła być zakończona. Zamach na Abdicia przygotowany za wiedzą Izetbegovicia, nie zakończył się powodzeniem, a pięciu zamachowców szkolonych przez irański wywiad zostało aresztowanych przez chorwacką policję[31].

---

[25] D. Džamić, *Psi rata na Balkanu*…, s. 208–209.

[26] Tamże, s. 81.

[27] D.P. Šindler, *Nesveti teror. Bosna, Al Kaida i uspon globalnog džihada,* Beograd 2009*,* s. 145–147.

[28] J. Elsässer, *Jak dżihad przybył do Europy. Wojownicy Boga i tajne służby na Bałkanach*, Warszawa 2007, s. 130–131.

[29] D.P. Šindler, *Nesveti teror. Bosna*..., s. 158–159.

[30] Tamże.

[31] Tamże, s. 203–204.

Po podpisaniu porozumień w Dayton (1995 r.) Izetbegović publicznie oddał hołd mudżahedinom, chwaląc ich za wierność jego idei oraz męstwo. Nie podjął on też żadnych kroków, aby zapobiec powstawaniu sekt wahhabickich, będących często schronieniem dla grup terrorystycznych związanych z Al-Kaidą. Po zakończeniu wojny domowej elity polityczne pomagały mudżahedinom znaleźć zatrudnienie, przede wszystkim w policji i armii[32]. Byli wśród nich także wahhabici głoszący hasła reformowania islamu w radykalnym kierunku. W tym okresie dochodziło także do licznych incydentów na tle islamizacji społeczeństwa i zamykania meczetów, których imamowie nie zgadzali się na głoszenie fundamentalistycznych poglądów. Z czasem konflikty zaczęły przeradzać się w akty terrorystyczne. Zdaniem ekspertów Al-Kaida miała co najmniej dwie bazy w Bośni i Hercegowinie, w których byli szkoleni terroryści. Na czele jednej z grup szkoleniowych stał Algierczyk Abu Al Mali, dowódca El Mudżahid, który został aresztowany, gdy jechał do Stambułu. Okazało się, że posługiwał się on bośniackim paszportem. Nie można pominąć informacji, że czterech spośród siedmiu terrorystów odpowiedzialnych za ataki z 11 września walczyło na terytorium Bośni i Hercegowiny oraz miało obywatelstwo tego kraju. Istnieją przypuszczenia, że przebywał tam również Muhamed Atta, najbardziej znany zamachowiec, który został zwerbowany przez członka Al-Kaidy, Muhammeda Hadara Zammara, obywatela Niemiec, uczestnika bośniackiego dżihadu[33].

Policja i służby bezpieczeństwa Bośni i Hercegowiny nadal podejmują wiele akcji mających na celu zwalczenie terroryzmu związanego z islamskimi ekstremistami. Jedna z największych operacji została przeprowadzona w nocy z 1 na 2 lutego 2010 r. we wsi Gornja Maoča[34] między Tuzlą a Brčko, w której działała wspólnota mudżahedinów założona przez członków oddziału El Mudżahid. W wyniku podjętej akcji aresztowano członków sekty wahhabitów, na czele z przywódcą Nusretem Imamoviciem. Imamović, instruowany przez Bin Ladena, przedstawiał w internecie swoje skrajne poglądy, które miały usprawiedliwić podejmowane akty terrorystyczne. W siedzibie sekty znaleziono broń oraz materiały propagandowe w języku arabskim[35]. Śledztwo wykazało, że bośniaccy wahhabici współpracowali z podobną sektą w Nowym Pazarze. Zdaniem serbskich władz aresztowani brali udział w planowaniu ataków terrorystycznych w Europie Zachodniej, m.in. zamachu bombowego podczas pogrzebu papieża Jana Pawła II[36].

Chociaż po 1995 r. działalność mudżahedinów na Bałkanach uległa osłabieniu, nie można jednak bagatelizować tego zjawiska. Na przełomie wieków XX i XXI do-

[32] A. Wejkszner, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010, s. 215–216 oraz w wielu miejscach.

[33] A. Krzak, *Niebezpieczeństwo terroryzmu dla państw narodowych na Bałkanach*, w: *Problemy bezpieczeństwa wewnętrznego i bezpieczeństwa międzynarodowego*, K.M. Księżopolski (red.), Warszawa 2009, s. 439 oraz w wielu miejscach.

[34] *Długie brody i krótkie spodnie*, http://mojesarajevo.blogspot.com/ [dostęp: 12 IV 2018].

[35] D. Halimović, *Vehabije u BiH: Od Bočinje do Maoče*, http://www.slobodnaevropa.org/ [dostęp: 12 IV 2018].

[36] Tamże.

szło do odradzania się na Bałkanach sieci terrorystycznej związanej z muzułmańskim fundamentalizmem. Już w 1996 r., kiedy odnotowano mniejszą aktywność mudżahedinów, zaczęła działać nowa grupa uderzeniowa terrorystów samobójców, złożona z młodych obywateli Bośni i Hercegowiny, o jasnych włosach i jasnych oczach. Były to osoby naśladujące terrorystów z Bliskiego Wschodu, wyszkolone w operowaniu materiałami wybuchowymi oraz prowadzeniu samobójczych misji. Liderzy Al-Kaidy postanowili rekrutować nowych terrorystów spośród Słowian, tworząc „białą" Al-Kaidę, która jest trudniejsza do zidentyfikowania ze względu na europejski wygląd jej członków[37]. W połowie 2003 r. radykalni islamistyczni liderzy przyjęli plan „Bałkany 2020" autorstwa Ajmana az-Zawahiriego[38], w którym Bałkany stanowią jedno z centrów islamskiego terroryzmu w Europie i jednocześnie odgrywają najważniejszą rolę w strategii Al-Kaidy przyjętej do 2020 r. Na Bałkanach, przede wszystkim w Bośni i Hercegowinie, Kosowie, Sandżaku i Chorwacji, nadal powstają centra służące rekrutowaniu terrorystów. Środki finansowe na ich działalność pochodzą przede wszystkim z handlu narkotykami[39]. Zebranie grupy „białej" Al-Kaidy i przygotowanie jej członków do uderzeń terrorystycznych służyłoby wzmocnieniu akcji przeprowadzanych w Europie Zachodniej. Do końca 2004 r. przygotowano do ataków ok. 200 terrorystów w wieku 20–25 lat. Instruktaż odbywał się w krajach islamskich, a za ich naukę płacił oddział Al-Kaidy odpowiedzialny za Bałkany i Europę. Terroryści zostali rozmieszczeni głównie na terytorium Macedonii i Kosowa. W 2005 r. szkolenie samobójców było kontynuowane na północy Albanii i w Kosowie, werbowano tam m.in. kobiety wybrane spośród wdów, które na wojnie straciły wszystkich bliskich, łatwo więc stawały się ofiarami manipulacji prowadzonej przez organizacje terrorystyczne.

Wielu ekspertów i naukowców uważa, że ortodoksyjni wyznawcy islamu zaczęli adaptować się w tych regionach i państwach, gdzie ich do tej pory nie było: w Bośni i Hercegowinie, Kosowie, Serbii, Chorwacji, a ostatnio pojawili się w Bułgarii. Za szerzenie wahhabizmu jest odpowiedzialna Liga Świata Muzułmańskiego, a szczególnie jej agenda – Światowa Rada Meczetów. Ta ostatnia finansuje budowę świątyń muzułmańskich na Bałkanach. W Kosowie często powstają one na miejscu spalonych cerkwi, a np. w stolicy tego quasi-państwa[40] w 2008 r. otwierano co miesiąc nowe ośrodki islamskiego kultu religijnego[41]. Problem spornej prowincji ma szerszy wymiar, zarówno etniczny, jak i religijny, jest on bowiem związany ze społecznością muzułmańską na Starym Kontynencie. Młode albańskie elity mieszkające w Kosowie uznają Serbów za wrogów, często głoszą hasła wzywające do wyeliminowania tej „obcej"

[37] M. Drecun, *Alahovi ratnici*, Beograd 2008, s. 305–310.

[38] Y. Bodansky, *Osama bin Laden człowiek, który wypowiedział wojnę Ameryce*, Warszawa 2001, s. 95.

[39] M. Drecun, *Alahovi ratnici*…, s. 6–9, 304–305.

[40] W dniu 17 lutego 2008 r. Kosowo formalnie ogłosiło niepodległość, ten akt nie został jednak uznany przez Serbię. Niezależności Kosowa nie popierają m.in. Rosja, Hiszpania, Cypr, Rumunia, Grecja i Słowacja, opowiadając się za przynależnością spornego terytorium do Serbii, E. Bujwid-Kurek, *Serbia w nowej przestrzeni ustrojowej: dzieje, ustrój, konstytucja*, Kraków 2012, s. 94.

[41] K. Izak, *Leksykon organizacji i ruchów*…, s. 522.

nacji. Silne związki tego quasi-państwa z terroryzmem islamskim datują się od czasu funkcjonowania Armii Wyzwolenia Kosowa (Ushtria Çlivimtare e Kosovës, UÇK), organizacji albańskiej, której celem było doprowadzenie do niepodległości Kosowa i utworzenie Wielkiej Albanii. Pod koniec XX w. jej członkowie wielokrotnie dokonywali fizycznej likwidacji obywateli narodowości serbskiej (głównie przedstawicieli administracji, funkcjonariuszy instytucji oraz służb bezpieczeństwa), a także kolaborantów albańskich opowiadających się za koegzystencją z innymi narodowościami zamieszkującymi Kosowo[42]. Najazdy UÇK na miejscowości zasiedlone przez Serbów były wspierane przez ochotnicze jednostki bojowników z Bośni i Hercegowiny, co spowodowało eskalację napięć etnicznych i potęgowało starcia zbrojne i akty terrorystyczne[43]. Zabójstwa i napady miały na celu zarówno zmuszenie mniejszości serbskiej do opuszczenia Kosowa, jak i prowokowanie oddziałów armii jugosłowiańskiej i milicji broniących porządku w prowincji do występowania przeciw Serbom. Od 1997 r. UÇK podjęła regularną walkę z Serbami, zajmując 30 proc. rejonu Drenicy w Kosowie. Do 1998 r. państwa zachodnie uznawały UÇK za organizację terrorystyczną, lecz wkrótce zmieniły swój stosunek do niej, co wynikało przede wszystkim z poparcia udzielonego tej formacji przez USA. W związku z rosnącym zaangażowaniem USA w konflikt w Kosowie w lutym 1998 r. Departament Stanu usunął UÇK z listy organizacji terrorystycznych, gdyż stała się ona pożądanym sprzymierzeńcem w walce z rządami Slobodana Miloševicia[44]. Narastające animozje pomiędzy Serbami a Albańczykami doprowadziły do wybuchu otwartej walki zbrojnej, której eskalacja stała się w 1999 r. przyczyną interwencji militarnej NATO i utworzenia w spornej prowincji międzynarodowego protektoratu ONZ. Działania podejmowane przez społeczność międzynarodową nie rozwiązały jednak omawianego konfliktu. Podczas walk UÇK stała się konglomeratem rożnych grup zbrojnych mających na celu utworzenie Wielkiej Albanii. W jej skład weszły jednostki finansowane przez służby wywiadowcze: amerykańskie, niemieckie, brytyjskie i chorwackie. Akcje policji i służb wywiadowczych skierowane przeciwko muzułmańskim radykałom często przynoszą aresztowania, konfiskatę broni i amunicji. W ocenie służb specjalnych Kosowo (podobnie jak Bośnia i Hercegowina) staje się obszarem, z którego są werbowani terroryści walczący w szeregach Państwa Islamskiego oraz na różnych frontach dżihadu prowadzonego przez fundamentalistów. Przypuszcza się, że to oni biorą udział w zamachach na ludność cywilną w Europie Zachodniej[45].

[42] S. Schwartz, *Kosovo: Background to a War*, London 2000, s. 137–143.

[43] T. Arbuckle, *Unhealthy climate in Kosovo as guerillas gear up for a summer confrontation*, „Jane's International Defense Review" 1999, nr 2, s. 60. Serbskie i rosyjskie służby specjalne wielokrotnie donosiły o powiązaniach UÇK z Al-Kaidą, natomiast w finansowanie Armii Wyzwolenia Kosowa był zaangażowany Osama bin Landen, który przekazał albańskim terrorystom 500–700 mln dolarów, P.L. Williams, *Al-Kaida. Międzynarodowy terroryzm, zorganizowana przestępczość i nadciągająca apokalipsa*, Poznań 2007, s. 88.

[44] D. Gibas-Krzak, *Serbsko-albański konflikt o Kosowo. Uwarunkowania – przebieg – konsekwencje*, Toruń 2009, s. 178–183.

[45] *Džihadisti iz BiH. Ako BiH uđe u EU, mnoga vrata će nam biti otvorena*, http://www.

Rekrutowanie osób do „białej" Al-Kaidy odniosło sukces, co potwierdziły śledztwa policji oraz służb specjalnych. Według oceny wywiadu amerykańskiego w 2004 r. w Albanii, Bułgarii, Macedonii, Kosowie, Bośni i Hercegowinie ok. 6000 ludzi utrzymywało pośrednią lub bezpośrednią więź z Al-Kaidą. Brytyjskie jednostki antyterrorystyczne, które przebywały w Sarajewie, wykryły związki pomiędzy terrorystami, którzy podłożyli bomby w Londynie 7 lipca 2005 r., a członkami komórek bośniackich. W 2005 r. zatrzymano członków Grupy sarajewskiej wyposażonych w materiały wybuchowe. Rozbito także terrorystyczną grupę Maksimus działającą w kantonie Sarajewo, stanowiącą komórkę Al-Kaidy na północną Europę. Na jej czele stał Mirsad Bektašević, dziewiętnastoletni wówczas obywatel Szwecji, zajmujący się rekrutowaniem w Internecie młodych muzułmanów do siatki Bin Ladena. Terroryści zamierzali m.in. przeprowadzić zamach na Siły Unii Europejskiej (EUFOR) w Sarajewie. W marcu 2008 r. aresztowano kolejnych pięciu podejrzanych, którzy utrzymywali kontakty z imamem Muhammadem Porčą z Wiednia znanym ze skrajnych poglądów[46].

Baza stworzona na Bałkanach ma umożliwiać terrorystom szybsze przedostawanie się do Europy Zachodniej. Kolejnym niepokojącym zjawiskiem jest radykalizowanie się mieszkańców tego regionu, budowanie struktur parawojennych, nawiązywanie ściślejszej współpracy z Al-Kaidą i innymi organizacjami ekstremistycznymi oraz terrorystycznymi. Nie jest bowiem tajemnicą, że Bałkany są jednym z regionów, którego mieszkańcy w dość znacznym stopniu zasilali terrorystyczną siatkę Państwa Islamskiego. Według danych CIA oraz służb specjalnych innych krajów z Bałkanów do Syrii i Iraku, gdzie działało Państwo Islamskie, mogło wyjechać nawet kilkaset osób[47]. Z analiz izraelskich służb wywiadowczych wynika, że islamskie organizacje humanitarne bez przerwy przesyłają fundusze dla muzułmanów pochodzenia bośniackiego i albańskiego, tworząc materialne podstawy przyszłych działań o charakterze terrorystycznym[48]. Bośniackie służby bezpieczeństwa oceniły, że liczba uzbrojonych islamistów w tym kraju może wynosić 3 tys.[49] Akcje ekstremistów islamskich nadal stanowią zagrożenie bezpieczeństwa tego regionu, czego przykładem może być zamach na ambasadę USA w Sarajewie, dokonany 28 października 2011 r. przez Mevlida Jašarevicia pod hasłem zemsty za Kaddafiego[50]. W styczniu 2015 r. podczas

nezavisne.com/novosti/bih/Dzihadisti-iz-BiH-Ako-BiH-udje-u-EU-mnoga-vrata-ce-nam-biti-otvorena/353577 [dostęp: 25 III 2018].

[46] K. Izak, *Radykalny islam na Bałkanach źródłem konfliktów społecznych i terrorystycznego zagrożenia dla Europy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 54.

[47] K. Karnowski, *ISIS pokonane. Upadł ostatni bastion Państwa Islamskiego w Syrii*, https://wiadomosci.wp.pl/isis-pokonane-upadl-ostatni-bastion-panstwa-islamskiego-w-syrii-6184061996299905a [dostęp: 12 IV 2018].

[48] *Lieberman: Balkans the next target of Worldwide Jihad*, http://serbianna.com/news/archives/3788 [dostęp: 12 IV 2018].

[49] *Bosnia: 3,000 militants pose grave security threat'*, http://www.adnkronos.com/AKI/English/Security/?id=3.1.677269022 [dostęp: 12 IV 2018].

[50] S. Mišljenović, *Vehabija iz Novog Pazara pucao na ambasadu SAD*, http://www.novosti.rs/vesti/planeta.70.htm [dostęp: 12 IV 2018].

zamachu na redakcję „Charlie Hebdo" w Paryżu użyto broni i amunicji pochodzącej z Bośni i Hercegowiny. W listopadzie tego samego roku na przedmieściach Sarajewa dwóch żołnierzy bośniackich zostało zabitych przez członka sekty wahhabitów. Niedługo potem w okolicach Mostaru został przeprowadzony atak bombowy na samochód, w którym podróżował gen. Anto Jeleč, naczelnik sztabu Sił Zbrojnych Bośni i Hercegowiny. W 2016 r. na szczycie Organizacji Współpracy Islamskiej w Stambule Bakir Izetbegović, były członek Prezydium Republiki Bośni i Hercegowiny, ocenił, że jego kraj cierpi na syndrom rozwoju ekstremizmu religijnego połączony z przypadkami akcji terrorystycznych[51]. Można więc postawić hipotezę, że prawdopodobnie terroryści zamierzają przygotowywać kolejne ataki wymierzone przeciw misjom dyplomatycznym USA, bazom NATO lub siłom zbrojnym Bośni i Hercegowiny, które są wysyłane do udziału w operacjach poza granicami kraju.

Nikogo nie powinna dziwić popularność nurtów fundamentalistycznych i wzrost liczby jego zwolenników w Bośni i Hercegowinie. Na terytorium tego kraju znajduje się bowiem ok. 100 tys. wyznawców i sympatyków skrajnych nurtów islamu czekających na okazję, aby udowodnić, że są prawdziwymi muzułmanami. I mogą to uczynić w bardzo drastyczny sposób[52]. Źródła bośniackie dowodzą, że obecnie muzułmańscy ekstremiści odbywają szkolenia wojskowe w miejscowości Mahnjača, na granicy gminy Teslić w Republice Serbskiej i Zenicy w Federacji Bośni i Hercegowiny[53]. Najnowsze doniesienia wskazują także na powstawania kolejnych baz treningowych fundamentalistów. Do najważniejszych z nich należy zaliczyć bazy zlokalizowane w Bośni i Hercegowinie w miejscowościach: Ošve, 250 km od Belgradu, Dubnica (stanowiąca centrum dżihadystów) i Jezera, wykupiona przez sektę wahabitów, oraz w Serbii: ośrodek „Furkan" w Nowym Pazarze (mają tam być werbowani ochotnicy do walki w Syrii oraz na innych frontach dżihadu[54]).

Wpływy islamskich terrorystów w Bułgarii, Albanii, Macedonii i Grecji

Nie tylko państwa Bałkanów Zachodnich zostały naznaczone groźnym piętnem terroryzmu islamskiego, mającego związki z nurtami radykalnego islamu. W Bułgarii niemal jedną szóstą spośród 7,1 mln mieszkańców stanowią muzułmanie, wyznawcy sunnizmu. W ciągu ostatnich 20 lat udało się w tym państwie zachować równowagę na tle etnicznym, chociaż i tu można zaobserwować ekspansję wahhabizmu. Od połowy lat 90. XX w. przeznaczono w tym rejonie znaczne środki finansowe na budowę ponad 150 nowych meczetów i tzw. ośrodków edukacyjnych, których celem jest szerzenie

[51] F. Alispahić, *Posrbljavanje bošnjačkog liderstva*, „Preporodov Journal" 2016, z. 186, s. 40.

[52] *Egipćanin okuplja vehabije u BiH*, http://www.rtv.rs/sr_lat/region/egipcanin-okuplja-vehabije-u-bih_254995.html [dostęp: 12 IV 2018].

[53] Tamże.

[54] *Ako nas Srbija ne spasi terorizma, onda smo načisto propali*, https://www.fokus.ba/vijesti/globus/ako-nas-srbija-ne-spasi-terorizma-onda-smo-nacisto-propali/100222/ [dostęp: 12 IV 2018].

wahhabizmu[55]. Ogółem w Bułgarii działa 1050 meczetów, a nowe wznosi się przede wszystkim za pieniądze pochodzące z saudyjskich fundacji charytatywnych. Saudyjczycy finansują także stypendia dla studentów bułgarskich na uczelniach religijnych w Arabii Saudyjskiej i Jordanii[56]. Władze Bułgarii próbują podejmować działania mające na celu ograniczanie tendencji fundamentalistycznych. W wielu przypadkach przynoszą one spodziewane rezultaty, np. w 2003 r. zamknięto kilka islamskich ośrodków, które były finansowane głównie przez Saudyjczyków związanych z Bractwem Muzułmańskim. Naukowcy twierdzą, że wzrasta liczba zarówno centrów fundamentalistycznych, jak i medres, w których naucza się reguł wahabbizmu. To zjawisko jest zauważalne przede wszystkim w południowej i północno-wschodniej Bułgarii (Płowdiw, Kazanłyk, Welingrad, Bilka, Razgrad). Szczególnie niebezpieczne jest opanowanie części szkół przez islamskich radykałów oraz to, że to zjawisko nie podlega żadnej państwowej kontroli[57].

Wśród państw bałkańskich niewiele jest takich, które potrafią podejmować efektywne działania antyterrorystyczne. Wyjątek może stanowić Albania. Władze tego kraju od kilkunastu lat aktywnie współpracują z ośrodkami w Europie Zachodniej i USA zajmującymi się zwalczaniem zjawiska islamskiego terroryzmu. I wydaje się, że skuteczność tych działań jest dobrym przykładem dla pozostałych państw tego regionu. Jednym ze spektakularnych przykładów była akcja przeprowadzona w latach 2004–2006 przez służby specjalne i policję polegająca na zablokowaniu działalności wywrotowej saudyjskiego biznesmena Jasina Abdullaha al Kadiego, który współpracował z Al-Kaidą i innymi organizacjami terrorystycznymi. Al Kadi prowadził działalność gospodarczą w Tiranie oraz kierował organizacją charytatywną, dzięki czemu mógł wspierać terrorystów oraz pomagać w tworzeniu miejscowych agend i centrów islamistycznych. W tym samym czasie usunięto z Albanii grupę fundamentalistów podejrzewanych o sponsorowanie terroryzmu i uczestnictwo w Egipskim Islamskim Dżihadzie[58]. Niepokojąca sytuacja panuje natomiast w Macedonii, gdzie rosnące w siłę radykalne nurty islamu przyczyniają się do rozłamu w społeczności muzułmanów. W oficjalnie działającej Islamskiej Wspólnocie Religijnej można dostrzec walkę o władzę pomiędzy umiarkowanymi przedstawicielami głównego nurtu a odłamem wahhabitów, którzy konkurują ze sobą o wpływy i pieniądze. W tym przypadku podziały religijne łączą się z podziałami etnicznymi, co nie sprzyja stabilizacji państwa, rodzi za to dalsze napięcia i zagraża bezpieczeństwu[59]. Także i na tym terytorium radykalizacja społeczności muzułmańskiej dokonała się wraz z rozpadem komunistycznej Jugosławii. W styczniu 1992 r. Albańczycy z Macedonii opowiedzieli się za powołaniem

[55] *Bałkany coraz bardziej islamskie*, https://euroislam.pl/balkany-coraz-bardziej-islamskie/?print=print [dostęp: 12 IV 2018].

[56] K. Izak, *Leksykon organizacji i ruchów*…, s. 525.

[57] *Bałkany coraz bardziej*...; *Terrorism in the Balkans in the 20th*..., s. 8–9.

[58] K. Izak, *Leksykon organizacji i ruchów*..., s. 521.

[59] I. Stawowy-Kawka, *Miejsce ludności muzułmańskiej w Macedonii – przemiany i perspektywy*, „Prace Komisji Środkowoeuropejskiej PAU" 2014, t. 22, s. 135.

do życia autonomicznej republiki o nazwie Illiryda. Na wzór separatystów z Kosowa zaczęli tworzyć nielegalne struktury organizacyjne, w tym szkoły i uniwersytety. Po wojnie o Kosowo w 1999 r. aspiracje polityczne Albańczyków wzrosły. Zaczęli oni się domagać statusu narodu równorzędnego w państwie macedońskim oraz przyłączenia rejonów przygranicznych do Albanii. W 2000 r. macedoński odłam Armii Wyzwolenia Kosowa wywołał incydenty na granicach Macedonii i Kosowa. Do rebelii Wyzwoleńczej Armii Narodowej doszło wiosną 2001 r. – 15 marca Albańczycy zaatakowali Tetovo. W tym buncie brali udział islamscy fundamentaliści wspierani przez Albańczyków z Kosowa, którzy nie zostali rozbrojeni przez siły międzynarodowe. Ofensywa wojsk macedońskich doprowadziła do wycofania się separatystów w rejony pogranicza, jednak walki zostały przerwane dopiero w wyniku interwencji dyplomatycznej Zachodu[60].

Władze Macedonii niechętnie przyznają się do zagrożenia, jakie niesie radykalny islam, chociaż fakty wydają się potwierdzać to niebezpieczeństwo. W 2007 r. trzech albańskich braci pochodzących z Macedonii, wraz z mieszkającymi w USA Jordańczykiem, Turkiem i kosowskim Albańczykiem, miało uczestniczyć w przygotowywaniu ataku na amerykańską bazę wojskową Fort Dix w New Jersey. W maju 2010 r. podczas akcji policyjnej niedaleko Skopja śmierć poniosło czterech ekstremistów, którzy przewozili broń[61]. Macedonia zalicza się do członków międzynarodowej koalicji w walce z terroryzmem, dlatego też nie może być zwolniona z obowiązku śledzenia i reagowania na wszelką potencjalną działalność terrorystyczną. Umiarkowani muzułmanie przyznają, że pod kontrolą wahhabitów znajduje się obecnie pięć meczetów w Skopje, mimo że Islamska Społeczność Religijna zabroniła Ramadanowi Ramadaniemu, którego uważa się za przywódcę ruchu, organizowania nabożeństw i pełnienia funkcji imama meczetu Isa Beg w Skopje. Ramadani poszukując zwolenników obalenia obecnych władz Islamskiej Społeczności Religijnej, odrzucił oskarżenia o radykalizm oraz zaprzeczył doniesieniom o rosnącym zagrożeniu ze strony islamskich ruchów politycznych i religijnych[62].

Zdaniem Ioannisa Michaletosa Grecja, położona na Bałkanach pomiędzy Turcją i Północną Afryką, basenem Morza Śródziemnego, niedaleko Morza Czarnego i Bliskiego Wschodu, jest ważną strefą tranzytową dla międzynarodowego terroryzmu. Pełni funkcję korytarza wykorzystywanego przez dżihadystów. Ten kraj stanowi także dogodne miejsce ataków dla „samotnych wilków" (ang. *lone wolves*), terrorystów, którzy potrafią działać spontanicznie, bez konieczności kontaktowania się z siecią terrorystyczną. „Samotne wilki" to kolejny, wydaje się – wiodący, nurt we współczesnym terroryzmie, szczególnie niebezpieczny dla Grecji mającej istotne znacznie

[60] A. Koseski, *Główne problemy transformacji w Republice Macedonii (1991–2000)*, w: *Transformacja systemowa w krajach Europy Środkowej, Wschodniej i Południowej 1989–2002*, T. Godlewski, A. Koseski, K.A. Wojtaszczyk (red.), Bydgoszcz–Pułtusk 2003, s. 160.

[61] K. Izak, *Leksykon organizacji i ruchów*…, s. 525.

[62] *Bałkany coraz bardziej islamskie*…

jako centrum turystyczne[63]. W latach 2015–2016 ogromna fala imigrantów przeszła przez Grecję, kierując się w głąb Europy, a wraz z nią pojawił się nowy rodzaj organizacji pozarządowych mających na celu pomoc uchodźcom. Wśród nich znalazło się jednak wiele organizacji związanych z frakcjami politycznego islamu, m.in. Islamic Relief Worldwide, która ściśle współdziała z siecią terrorystyczną utworzoną przez Bractwo Muzułmańskie. Islamic Relief Worldwide zakorzeniła się w Grecji jako organizacja niosąca pomoc migrantom, chociaż oficjalnie w listopadzie 2014 r. została uznana przez Zjednoczone Emiraty Arabskie za ugrupowanie terrorystyczne. Zajmowała się m.in. finansowaniem Hamasu. W lipcu 2016 r. władze stanu Missouri stwierdziły, że lokalny, amerykański odłam tej organizacji przekazał 1,4 mln dolarów na potrzeby ekstremistów w Iraku i Afganistanie. Rosyjskie służby specjalne wskazały natomiast, że Islamic Relief Worldwide finansuje kaukaskich dżihadystów. Michaletos zidentyfikował także inne organizacje powiązane z terroryzmem islamskim aktywnie działające na greckiej wyspie Lesbos, którymi są organizacje pozarządowe (NGO): Al Muntada Trust oraz One Nation. Pierwsza z nich finansuje nigeryjskich ekstremistów, druga dostarcza broń do Syrii i jest powiązana z tureckimi organizacjami przekazującymi uzbrojenie dla ISIS. Te organizacje utrzymują też kontakty z siecią Al-Kaidy[64].

Wnioski

Według różnych ocen wywiadowczych na obszarze Bałkanów Zachodnich przebywa około kilku tysięcy osób związanych z Al-Kaidą oraz innymi organizacjami terrorystycznymi. Identyfikowani są przywódcy organizacji terrorystycznych, znane są również nazwiska wielu członków tych organizacji, np. weterana wojny w Afganistanie Sahiba Emira Musy Ajzi, którzy są odpowiedzialni za rekrutację przedstawicieli narodów słowiańskich wyznania islamskiego (tzw. białych konwertytów). Takich młodych ludzi znajduje się przede wszystkim w Bośni i Hercegowinie, Bułgarii, Macedonii, Kosowie oraz Sandżaku. Za głównego przywódcę podziemia terrorystycznego na Bałkanach jest uważany Ajman az-Zavahiri. Liczba mudżahedinów, którzy przybyli tutaj w czasie wojny, zmniejszyła się, lecz pozostawili oni po sobie uczniów, naśladowców, co przyczyniło się do tego, że Bałkany stały się obszarem penetracji wielu organizacji terrorystycznych oraz areną walki o wpływy różnych państw muzułmańskich. Sprzyja temu sytuacja międzynarodowa, gdyż po zimnej wojnie wiele państw bałkańskich nie może się uporać z licznymi problemami wewnętrznymi o charakterze społecznym i ekonomicznym. Wysokie bezrobocie, zastój gospodarczy, skupienie się lokalnych polityków bardziej na walce o władzę i podsycaniu konfliktów etnicznych i religijnych niż na reformach wywołują u młodego pokolenia frustrację. Młodzi ludzie nie widzą

[63] Terroryści nazywani „samotnymi wilkami" mogą być niebezpieczni też dla innych państw bałkańskich.

[64] I. Michaletos, *Contemporary risk assessment of extremism and terrorism in Greece. The case of Islamist-driven security risks in Greece*, w: *Terrorism in the Balkans in the 20th*..., s. 187–195.

dla siebie perspektyw, dlatego stają się łatwą zdobyczą dla werbowników z organizacji terrorystycznych[65].

Nie można też nie dostrzec sprzyjających warunków środowiska naturalnego, które działa na korzyść terrorystów. Bazy treningowo-szkoleniowe ze względu na ukształtowanie terenu mogą być niedostępne dla służb specjalnych i policji. W odległych zakątkach Bałkanów, zwłaszcza w ich górzystej części, istnieją dogodne warunki do rozwoju współczesnych organizacji terrorystycznych o ogólnoświatowym zasięgu. Jest to bardzo niebezpieczne, gdyż Bałkany wydają się być jednym z najważniejszych regionów łączących organizacje wywodzące się z Bliskiego Wschodu z celem ich ekspansji, czyli północną i zachodnią Europą. Jednym z najbardziej niebezpiecznych aspektów tego zbliżenia jest rozbudowa sieci terrorystycznej i szkolenie przyszłych terrorystów, zwłaszcza w formie „białego" dżihadu. Po wojnie domowej w Jugosławii państwa muzułmańskie nie zaprzestały finansowania działalności mającej na celu promowanie islamu w tym regionie. Środki płyną nie tylko z rządowych instytucji, lecz także z prywatnych organizacji charytatywnych[66]. Przykładem tego jest częste stosowanie indoktrynacji religijnej w placówkach oświatowych w krajach postjugosłowiańskich, gdzie dyskryminuje się dzieci wyznające inną niż islam religię[67]. Popularność na Bałkanach zyskują także portale internetowe służące rozpowszechnianiu zasad radykalnego islamu, krytykujące ostro zachodnią kulturę i styl życia. Należą do nich oficjalne strony skrajnych organizacji, np. Młodych Muzułmanów (Mladi Muslimani), oraz witryny wspólnot islamskich. To wszystko sprawia, że radykalizujący się islam i powstałe na jego bazie komórki terrorystyczne mogą stać się zarzewiem nowego konfliktu w „bałkańskiej beczce prochu".

Bibliografia:

Ako nas Srbija ne spasi terorizma, onda smo načisto propali, https://www.fokus.ba/vijesti/globus/ako-nas-srbija-ne-spasi-terorizma-onda-smo-nacisto-propali/100222/ [dostęp: 12 IV 2018].

Alispahić F., *Posrbljavanje bošnjačkog liderstva*, „Preporodov Journal" 2016, z. 186, s. 38–40.

Aralica I., *Što sam rekao o Bosni,* Zagreb 1995.

Arbuckle T., *Unhealthy climate in Kosovo as guerillas gear up for a summer confrontation*, „Jane's International Defense Review" 1999, nr 2.

[65] Zob. *Paradoxes of stabilization. Bosnia and Herzegovina from the perspective of Central Europe*, M. Szpala (ed.), seria: OSW Report, Warsaw 2016.

[66] V. Janková, *Wahhabism in the Balkans. The case study of Bosnia and Herzegovina,* Praha 2014, s. 72.

[67] Tamże.

Bałkany coraz bardziej islamskie, https://euroislam.pl/balkany-coraz-bardziej-islamskie/?print=print [dostęp: 12 IV 2018].

Beloff N., *Tito's flawed legacy. Yugoslavia and the West: 1939–84*, London 1985.

Bodansky Y., *Osama bin Laden człowiek, który wypowiedział wojnę Ameryce*, Warszawa 2001.

Borkowski R., *Terroryzm ponowoczesny. Studium z antropologii polityki*, Toruń 2007.

Bosnia: 3,000 militants pose grave security threat', http://www.adnkronos.com/AKI/English/Security/?id=3.1.677269022 [dostęp: 12 IV 2018].

Bujwid-Kurek E., *Serbia w nowej przestrzeni ustrojowej: dzieje, ustrój, konstytucja,* Kraków 2012.

Długie brody i krótkie spodnie, http://mojesarajevo.blogspot.com/ [dostęp: 12 IV 2018].

Doder M., *Jugoslavenska neprijateljska emigracja*, Zagreb 1989.

Drecun M., *Alahovi ratnici*, Beograd 2008.

Dubicki A., *Terror as a method of fighting of the Iron Guard*, w: *Terrorism in the Balkans in the 20th and 21st century*, D. Gibas-Krzak (ed.), Torun 2018.

Džamić D., *Psi rata na Balkanu. Strani plaćenici u ratnim sukobima na prostorima bivše Jugoslavije*, Beograd 2001.

Egipćanin okuplja vehabije u BiH, http://www.rtv.rs/sr_lat/region/egipcanin-okuplja-vehabije-u-bih_254995.html [dostęp: 12 IV 2018].

Elsässer J., *Jak dżihad przybył do Europy. Wojownicy Boga i tajne służby na Bałkanach*, Warszawa 2007.

Emigrant Croats who were victims of federal terror after 1945, „Slobodna Dalmacija" z 15 sierpnia 2000 r.

Encyklopedia Politologii, t. 5, M. Żmigrodzki (red.), Zakamycze 2002.

Gibas-Krzak D., *Bośnia i Hercegowina: determinanty dziejów. Pomiędzy Serbami, Chorwatami a supremacją Muzułmanów*, Częstochowa 2016.

Gibas-Krzak D., *Serbsko-albański konflikt o Kosowo. Uwarunkowania – przebieg – konsekwencje*, Toruń 2009.

Halimović D., *Vehabije u BiH: Od Bočinje do Maoče*, http://www.slobodnaevropa.org/ [dostęp: 12 IV 2018].

Hauziński J., *Asasyni. Legendarni zabójcy w czasach krucjat*, Poznań 2016.

Hoffman B., *Oblicza terroryzmu*, Warszawa 1999.

Izak K., *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014.

Izak K., *Radykalny islam na Bałkanach źródłem konfliktów społecznych i terrorystycznego zagrożenia dla Europy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 9, s. 52–74.

Karnowski K., *ISIS pokonane. Upadł ostatni bastion Państwa Islamskiego w Syrii*, https://wiadomosci.wp.pl/isis-pokonane-upadl-ostatni-bastion-panstwa-islamskiego-w-syrii-6184061996299905a [dostęp: 12 IV 2018].

Klejn Z., *Bułgaria. Szkice z dziejów najnowszych*, Pułtusk 2005.

Koseski A., *Główne problemy transformacji w Republice Macedonii (1991–2000*), w: *Transformacja systemowa w krajach Europy Środkowej, Wschodniej i Południowej 1989–2002*, T. Godlewski, A. Koseski, K.A. Wojtaszczyk (red.), Bydgoszcz–Pułtusk 2003.

Krzak A., *Active intelligence service (terrorism) of the Comintern and Soviet secret service in Bulgaria in the 1920s – case study*, w: *Terrorism in the Balkans in the 20th and 21st century*, D. Gibas-Krzak (ed.), Torun 2018.

Krzak A., *Niebezpieczeństwo terroryzmu dla państw narodowych na Bałkanach*, w: *Problemy bezpieczeństwa wewnętrznego i bezpieczeństwa międzynarodowego*, K.M. Księżopolski (red.), Warszawa 2009.

Lieberman: Balkans the next target of Worldwide Jihad, http://serbianna.com/news/archives/3788 [dostęp: 12 IV 2018].

Lučić I., *Bosnia and Herzegovina and terrorism*, „National security and the future" 2001, nr 3–4.

Michaletos I., *Contemporary risk assessment of extremism and terrorism in Greece. The case of Islamist-driven security risks in Greece*, w: *Terrorism in the Balkans in the 20th and 21st century*, D. Gibas-Krzak (ed.), Torun 2018.

Mišljenović S., *Vehabija iz Novog Pazara pucao na ambasadu SAD*, http://www.novosti.rs/vesti/planeta.70.html [dostęp: 12 IV 2018].

Nagy Talavera N.M., *The Green Shirts and the Others. A history of fascism in Hungary and Romania*, Iaşi 2001.

Paradoxes of stabilization. Bosnia and Herzegovina from the perspective of Central Europe, M. Szpala (ed.), Warsaw 2016.

Schwartz S., *Kosovo: Background to a War*, London 2000.

Stawowy-Kawka I., *Miejsce ludności muzułmańskiej w Macedonii – przemiany i perspektywy*, „Prace Komisji Środkowoeuropejskiej PAU" 2014, t. 22, s. 121–136.

Šindler D.P., *Nesveti teror. Bosna, Al Kaida i uspon globalnog džihada,* Beograd 2009.

Terrorism in the Balkans in the 20th and 21st century, D. Gibas-Krzak (ed.), Torun 2018.

Trifunović D., *Threat to international security – terrorism in South East Europe*, w: *Służby specjalne w systemie bezpieczeństwa państwa. Przeszłość – teraźniejszość – przyszłość. Materiały i studia*, t. 2, A. Krzak, D. Gibas-Krzak (red.), Szczecin 2012.

Wasilewski T., *Historia Bułgarii*, Wrocław–Warszawa–Kraków–Gdańsk–Łódź 1988.

Wejkszner A., *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010.

Wilamowski J., Szczepanik K., *Ustasze i separatyzm chorwacki*, „Przegląd Historyczny" 1983, z. 1, s. 75–95.

Williams P.L., *Al-Kaida. Międzynarodowy terroryzm, zorganizowana przestępczość i nadciągająca apokalipsa*, Poznań 2007.

Abstrakt

Autorka artykułu prezentuje zjawisko terroryzmu na Bałkanach na przestrzeni wieków XIX i XXI, zwracając uwagę, że ekspansja terroryzmu w tym regionie wymaga podjęcia odrębnych badań, przede wszystkim o charakterze heurystycznym. Wśród nurtów terroryzmu bałkańskiego został wymieniony terroryzm związany z ruchami narodowowyzwoleńczymi i terroryzm polityczny. Ponadto autorka wskazała na akcje terrorystyczne prowadzone w Rumunii i Bułgarii, terroryzm ustaszy i emigracji antyjugosłowiańskiej oraz inne jego formy. Szczególną uwagę poświęciła terroryzmowi związanemu z ekstremalnymi nurtami islamu, który pojawił się na Bałkanach jako dziedzictwo wojny domowej (1992–1995). W epoce postzimnowojennej terroryzm islamski na Bałkanach wiąże się ze wzrostem wpływów fundamentalistów muzułmańskich. Autorka udowadnia hipotezę, że Bałkany ze względu na warunki naturalne stwarzają znakomitą możliwość rozwoju baz i obozów treningowych dla terrorystów powiązanych z globalnym dżihadem. Rozwój terroryzmu na Bałkanach wywołuje zagrożenie dla bezpieczeństwa Europy i jej demokratycznych społeczeństw z powodu prawdopodobieństwa wzniecenia nie tylko konfliktu lokalnego, lecz także o szerszym zakresie, na skalę pozaeuropejską.

Słowa kluczowe: terroryzm międzynarodowy, Bałkany, terror polityczny, fundamentalizm islamski, sekty wahhabitów, sieć globalnego dżihadu.

Tomasz Safjański

Rozpracowywanie działalności terrorystycznej w ramach Europolu – uwarunkowania prawne i praktyczne

Wprowadzenie

Europol jest platformą wielostronnej współpracy wywiadowczej służb policyjnych, ochrony granic, celnych, finansowych, imigracyjnych, żandarmerii, a niekiedy nawet służb specjalnych państw członkowskich UE. Ustanowienie tego rodzaju instytucji zostało przewidziane w traktacie z Maastricht. Europol rozpoczął działalność 3 stycznia 1994 r. jako Eurodrug (ang. Europol Drugs Unit). W lipcu 1998 r. ratyfikowano konwencję o Europolu[1], która weszła w życie w październiku tego samego roku. W myśl jej przepisów Europol uzyskał zdolność operacyjną i oficjalnie rozpoczął działalność 1 lipca 1999 r.[2]

Artur Gruszczak wskazuje Europol jako najważniejszy element europejskiej wspólnoty wywiadowczej, a jego pozycja w tej wspólnocie jest rezultatem powiązań z instytucjami, agencjami i organami UE (m.in. europejską agencją graniczną Frontex, Centrum Analizy Wywiadowczej UE IntCen) oraz służbami ochrony prawa państw członkowskich[3].

Kompetencje Europolu w dziedzinie wywiadu kryminalnego

Kompetencje Europolu dotyczące rozpracowywania działalności terrorystycznej wynikają wprost z Traktatu o funkcjonowaniu Unii Europejskiej[4] (TFUE). Zgodnie z art. 88 ust. 1 TFUE: *Zadaniem Europolu jest wspieranie i wzmacnianie działań organów policyjnych i innych organów ścigania Państw Członkowskich, jak również ich wzajemnej współpracy w zapobieganiu i zwalczaniu poważnej przestępczości dotykającej dwóch lub więcej Państw Członkowskich, terroryzmu oraz form przestępczości naruszających wspólny interes objęty polityką Unii* oraz z ust. 3 tego artykułu: *Wszelkie działania operacyjne Europolu są prowadzone w powiązaniu i w porozumieniu z organami Państwa Członkowskiego lub Państw Członkowskich, których terytorium dotyczą. Stosowanie środków przymusu należy do wyłącznej kompetencji właściwych organów krajowych*. Z treści przedstawionych przepisów traktatowych

[1] *Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie ustanowienia Europejskiego Urzędu Policji (konwencja o Europolu), sporządzona w Brukseli dnia 26 lipca 1995 r.* (Dz.U. z 2005 r. nr 29 poz. 243, ze zm.).

[2] Zob. szerzej T. Safjański, *Europejskie Biuro Policji Europol. Geneza. Główne aspekty działania. Perspektywy rozwoju*, Warszawa 2009.

[3] Zob. szerzej A. Gruszczak, *Europejska wspólnota wywiadowcza. Prawo – instytucje – mechanizmy*, Kraków 2014.

[4] *Traktat o funkcjonowaniu Unii Europejskiej* – wersja skonsolidowana, (Dz. Urz. UE C 115 z 9 maja 2008 r., s. 49).

wynika, że rozpracowywanie działalności terrorystycznej w ramach Europolu jest działaniem w pełni legalnym i jest realizowane na podstawie umów międzynarodowych. Ta współpraca jest jednak uzależniona od spełnienia określonych warunków, nie jest zatem możliwe wykorzystanie potencjału operacyjnego Europolu w każdej sprawie czy w dowolny sposób.

Przedstawiciele Europolu nie mają choćby podstawowych uprawnień służb krajowych – zarówno operacyjno-rozpoznawczych (np. stosowanie kontroli operacyjnej, obserwacji), procesowych (np. związanych z zatrzymywaniem i przeszukiwaniem osób, przesłuchiwaniem, zabezpieczaniem śladów kryminalistycznych), jak i ogólnopolicyjnych (np. legitymowanie, kontrola osobista, przeglądanie zawartości bagaży, sprawdzanie ładunku w portach lub na lotniskach, stosowanie środków przymusu bezpośredniego czy użycie broni palnej). Wymienione kompetencje są przypisane wyłącznie właściwym organom krajowym.

Rozpracowywanie działalności terrorystycznej w ramach Europolu ma wymiar wielostronny. Ta instytucja zapewnia bezpośrednią współpracę w zwalczaniu m.in. tego rodzaju przestępczości wszystkich państw członkowskich UE, co wynika wprost z założeń traktatowych. Każde z państw członkowskich wskazuje organy krajowe właściwe do kooperowania na platformie Europolu, którymi są wszystkie organy uprawnione – zgodnie z prawem krajowym – do zapobiegania i zwalczania zagrożeń transgranicznych. Tak duża liczba organów ma oczywiście wpływ na model prowadzonych czynności.

Działalność kontrterrorystyczna Europolu ma charakter wspomagający działania państw członkowskich, oraz je uzupełnia, powinna również służyć zwiększeniu efektywności tych działań. Wynika to z założenia, że główny ciężar walki z międzynarodowymi przejawami terroryzmu spoczywa na służbach krajowych państw członkowskich, Europol zaś realizuje zadania związane ze zwalczaniem terroryzmu, wówczas gdy ze względu na rozmiar, zasięg lub charakter tych zagrożeń byłoby utrudnione przeciwdziałanie im na poziomie krajowym.

Działania Europolu zmierzają do tego, aby czynności służb krajowych były dobrze ukierunkowane i wzajemnie spójne. W praktyce pomocnicza funkcja kontrterrorystyczna Europolu znajduje zastosowanie w sytuacjach, w których działania służb krajowych mogą być bardziej skuteczne, gdy będą skoordynowane, niż gdyby były realizowane odrębnie przez poszczególne państwa członkowskie. Rolą Europolu jest zatem wspieranie, a nie zastępowanie służb policyjnych państw członkowskich.

Istotne uwarunkowania modelu rozpracowywania działalności terrorystycznej są określone w rozporządzeniu Parlamentu Europejskiego i Rady (UE) 2016/794 w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol)[5]. W świetle art. 4 tego rozporządzenia kompetencje w dziedzinie rozpracowywania działalności terrorystycznej obejmują m.in.:

[5] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW* (Dz. Urz. UE L 135 z 24 maja 2016 r., s. 53).

- zbieranie, przechowywanie, przetwarzanie i analizowanie informacji oraz prowadzenie wymiany informacji, także danych o charakterze operacyjnym,
- niezwłoczne powiadamianie państw członkowskich za pośrednictwem jednostek krajowych o wszelkich informacjach i powiązaniach między przestępstwami, które ich dotyczą,
- koordynowanie, organizowanie i prowadzenie działań procesowych i operacyjnych mających na celu wspieranie i wzmocnienie działań realizowanych przez właściwe organy państw członkowskich,
- dostarczanie państwom członkowskim informacji i zapewnianie wsparcia analitycznego w związku z ważnymi wydarzeniami międzynarodowymi,
- przygotowywanie ocen zagrożenia, analiz strategicznych i operacyjnych,
- wspieranie prowadzonych przez państwa członkowskie transgranicznych działań w zakresie wymiany informacji, transgranicznych operacji i postępowań przygotowawczych, a także wspólnych zespołów dochodzeniowo-śledczych, między innymi dostarczając wsparcie operacyjne[6].

Rozpracowywanie, rozpracowanie operacyjne

Rozpracowywanie jest działaniem z zakresu taktyki kryminalistycznej umożliwiającym realizację następujących funkcji kryminalistyki: rozpoznawczej (mającej na celu uzyskanie możliwie dużej liczby informacji o miejscu, przedmiocie, przeciwniku i taktyce przyszłych i aktualnych działań kryminalistycznych), wykrywczej (służącej wykryciu sprawcy, jego narzędzi i sposobów dokonania przestępstwa przez zebranie, ocenę i analizę informacji) oraz zapobiegawczej (mającej na celu zapobieganie działaniom przestępczym)[7].

Formą działań taktyczno-kryminalistycznych, w ramach której jest rozpracowywana działalność przestępcza, jest rozpracowanie operacyjne. Należy przez nie rozumieć zespół zaplanowanych i systematycznie realizowanych czynności operacyjno-rozpoznawczych wobec osoby fizycznej, prawnej albo grupy osób w związku z przypuszczeniem lub stwierdzeniem przygotowania, usiłowania lub dokonania określonego przestępstwa albo nieustalonego rodzaju działalności przestępczej[8].

Przez rozpracowywanie działalności terrorystycznej należy rozumieć ogół działań Europolu ukierunkowanych na:

- ujawnienie i lokalizowanie zagrożeń bezpieczeństwa UE mających znamiona działalności terrorystycznej,
- uzyskanie informacji pozwalających postawić hipotezę dotyczącą osoby lub organizacji terrorystycznej pozostających w relacji przyczynowej z tym zagrożeniem,

[6] Tamże, art. 4 ust. 1.

[7] Por. S. Pikulski, *Podstawowe zagadnienia taktyki kryminalistycznej*, Białystok 1997, s. 96 i nast.

[8] Poselski projekt ustawy o czynnościach operacyjno-rozpoznawczych, http://orka.sejm. gov.pl/proc6.nsf/projekty/353_p.htm, art. 2 ust. 4 [dostęp: 24 V 2013].

– ustalenie danych umożliwiających neutralizację zagrożenia (np. zatrzymanie osoby, rozbicie organizacji terrorystycznej, udaremnienie ataku terrorystycznego)[9].

Punktem wyjścia do rozpracowywania działalności przestępczej (terrorystycznej) jest informacja. Brak informacji lub jej niska jakość poddaje w wątpliwość skuteczność prowadzonego rozpracowania.

Rozpracowanie analityczne

Ze względu na swoisty status prawny Europolu rozpracowywanie działalności przestępczej przyjmuje formę rozpracowania analitycznego, przez które należy rozumieć specjalną procedurę uzyskiwania, weryfikacji, gromadzenia i dystrybuowania informacji kryminalnych i danych wywiadowczych. Rozpracowanie analityczne w wymiarze taktyczno-kryminalistycznym obejmuje zastosowanie analizy kryminalnej oraz ukierunkowanej wymiany informacji i danych wywiadowczych w celu wspomożenia spraw operacyjnych lub dochodzeń przeprowadzanych w państwach członkowskich wobec zagrożeń – takich samych pod względem rodzajowym, podmiotowym lub podobnych. Czynności podejmowane w ramach rozpracowania analitycznego – określanego jako „projekt analityczny" (ang. *Analysis Project*, AP) – koncentrują się wokół konkretnego podmiotu (osoby, środowiska) lub przedmiotu (miejsca, zjawiska).

Z techniczno-kryminalistycznego punktu widzenia w rozpracowaniu analitycznym są wykorzystywane specjalne narzędzia informatyczne o parametrach bazy danych, nazywane jako: analityczne bazy danych, analityczne pliki robocze, pliki robocze, pliki robocze do celów analizy, pliki analityczne (ang. *Analysis Work Files*, AWF). W celu uniknięcia nieporozumień należy zaznaczyć, że akronim „AWF" jest używany w praktyce zarówno do oznaczenia wymiaru taktycznego, jak i technicznego rozpracowywania działalności przestępczej lub terrorystycznej.

Rozpracowania analityczne stosuje się przede wszystkim przy rozpoznawaniu zagrożeń o najwyższym stopniu trudności wykrywczej (np. pranie pieniędzy) oraz wykrywaniu i zatrzymywaniu sprawców najniebezpieczniejszych przestępstw (np. aktów terrorystycznych)[10]. Podstawą rozpracowań analitycznych jest założenie, że sprawy operacyjne lub dochodzenia prowadzone pod różnymi jurysdykcjami krajowymi często wykazują wiele powiązań (podmiotowych, przedmiotowych i podmiotowo-przedmiotowych). Te powiązania są naturalną konsekwencją angażowania się organizacji terrorystycznych (międzynarodowych grup przestępczych) w przestępczość transgraniczną oraz wzajemnego przenikania się rynków przestępczych. Podstawą rozpoczęcia rozpracowania analitycznego jest zidentyfikowanie powiązań między sprawami, które są prowadzone przez poszczególne państwa członkowskie. We wstępnej fazie przetwarzania danych analitycy Europolu szukają podobieństw – choćby w podstawowym zakresie –

[9] Por. T. Hanausek, *Zarys kryminalistycznej teorii wykrywania*, cz. 2, Warszawa 1987, s. 3 i nast.
[10] Zob. szerzej T. Safjański, *Działania operacyjne Europolu*, Szczytno 2013.

między danymi (np. te same dane osobowe, ten sam adres, ten sam numer rachunku bankowego). Rozpracowania analityczne są wszczynane, gdy Europol stwierdzi, że sprawy prowadzone przez organy ścigania kilku państw członkowskich łączą się pod względem operacyjnym, a zainteresowane państwa uznają potrzebę ich zintegrowanego pilotowania. Następnie przygotowuje się kierunkową analizę przydatności informacji w konkretnych rozpracowaniach analitycznych oraz w poszczególnych dochodzeniach krajowych.

Na potrzeby rozpracowań analitycznych wykorzystuje się informacje uzyskane przez państwa członkowskie podczas realizacji spraw operacyjnych oraz dochodzeń krajowych. Na wniosek Europolu lub z własnej inicjatywy policje krajowe przekazują Europolowi dane, które mogą być niezbędne w konkretnym rozpracowaniu analitycznym. Państwa członkowskie przekazują je wyłącznie w przypadku, gdy na ich przetwarzanie do celów zapobiegania przestępstwom bądź też analizowania lub zwalczania przestępstw zezwala prawo krajowe. Z analitycznego punktu widzenia wymaga to wskazania obszaru dostarczanych danych dotyczących spraw karnych lub spraw operacyjnych w poszczególnych krajach[11]. Te dane są przekazywane przez krajowe jednostki Europolu do krajowych biur łącznikowych przy Europolu w formie not kontrybucyjnych (ang. *contribution note*). Informacje są weryfikowane przez menedżera (ang. *project manager*) pod kątem spełniania wymogów formalnych. W dalszej kolejności są one wprowadzane do analitycznego pliku roboczego.

W rozpracowywaniu analitycznym wyróżnia się następujące elementy:

- informatyczno-techniczny,
- metodyczny,
- zadaniowy (tj.: zakres rozpracowań, cele, terminy),
- osobowy (tzw. grupa analityczna).

Z metodycznego punktu widzenia podstawą rozpracowań analitycznych są głównie działania dotyczące wywiadu kryminalnego (m.in. analiza kryminalna, wymiana informacji) oraz możliwości działań własnych państw członkowskich (np. wspólne zespoły śledcze), przy jednoczesnym ukierunkowaniu na konkretną działalność przestępczą lub określony obszar zagrożeń. Prowadzone są także analizy ogólne (strategiczne) oraz szczegółowe (operacyjne)[12]. Analizy ogólne mają na celu przetwarzanie istotnych informacji dotyczących określonego, szerszego problemu (w wymiarze przestrzennym i czasowym) oraz opracowywanie i ulepszanie inicjatyw właściwych organów krajowych. Analizy szczegółowe służą natomiast uzyskiwaniu konkretnych informacji o przestępczych działaniach należących do mandatu Europolu. Jeżeli analiza ma charakter ogólny, to wszystkie państwa członkowskie są zaznajamiane z jej ustaleniami przekazywanymi w formie sprawozdań sporządzanych przez Europol za pośrednictwem oficerów łącznikowych lub ekspertów.

[11] Art. 1(b) *Aktu Rady UE 1999/C 26/01 z 3 listopada 1998 r. w sprawie przyjęcia przepisów dotyczących plików do celów analizy Europolu* (Dz. Urz. UE C 26 z 30 stycznia 1999 r., s. 1). Obecnie obowiązującym aktem jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) przywołane w przypisie 5 (dop. red.).

[12] Tamże, art. 10.

Europol prowadząc rozpracowania analityczne, organizuje spotkania operacyjne. Współpraca analityków Europolu z policjantami krajowych organów ścigania w zakresie spraw objętych rozpracowaniem analitycznym przebiega na wielu etapach. Oprócz analizy operacyjnej Europol zapewnia państwom członkowskim wsparcie eksperckie. Może ono być udzielane zdalnie z siedziby Europolu lub bezpośrednio na miejscu działań (np. przez mobilne biura). Państwa członkowskie mogą tworzyć wspólne zespoły śledcze, których praca jest ukierunkowana na określone postępowania karne. W modelowym założeniu takie działania zawsze mają prowadzić do powołania wspólnego zespołu śledczego.

Cel rozpracowań analitycznych jest zbieżny z głównym dążeniem procesu wykrywczego, tzn. zmierza zarówno do zgromadzenia kompleksowych danych wywiadowczych o działalności terrorystycznej, jak i innych informacji istotnych w procesie udowadniania tego przestępstwa. Zadaniem rozpracowań analitycznych jest wskazanie kierunków, w jakich proces wykrywczy powinien być prowadzony, luk w materiałach spraw oraz potrzeb dotyczących zbierania informacji. Rozpracowania analityczne pozwalają na porównywanie i sprawdzanie informacji dotyczących przestępstw, które pochodzą z różnych źródeł i z wielu państw. Analitycy mają również możliwość wyszukiwania informacji we wszystkich systemach i bazach danych, jakimi dysponuje Europol. Dzięki temu powstaje system wymiany informacji między projektem analitycznym prowadzonym przez Europol a sprawami operacyjnymi lub dochodzeniami prowadzonymi przez służby krajowe. Operacyjne projekty analityczne zajmują centralne miejsce w tym systemie, co ułatwia prowadzenie spraw lub dochodzeń i tworzy warunki do wykorzystania informacji uzyskanych w ramach innych jurysdykcji. Rozpracowania Europolu mogą być bezpośrednią podstawą działań operacyjnych w państwach członkowskich. Te projekty dają państwom członkowskim możliwość wypełniania braków w prowadzonym przez nie rozpoznaniu operacyjnym.

Kraje członkowskie niejednokrotnie przekazują do plików analitycznych fragmentaryczne informacje, które po poddaniu analizie operacyjnej – razem z informacjami dostarczanymi przez inne kraje członkowskie – pozwalają na identyfikację międzynarodowych struktur przestępczych, a także ich rozbicie. Udział w projekcie analitycznym umożliwia bieżącą wymianę informacji zarówno o poszczególnych grupach, jak i całych strukturach kryminalnych. Dostarczane przez państwa członkowskie informacje stanowią wkład analityczny, w następstwie czego jest możliwe koordynowanie działań w przypadku zainteresowania się innego państwa danym obiektem, przeprowadzenie analizy, a także wytyczenie dalszych kierunków wspólnych działań. Uczestnicy projektu analitycznego otrzymują raporty i oceny z prowadzonych spraw, co pozwala na stałe monitorowanie zagrożenia przestępczością terrorystyczną na obszarze UE. Potencjalne powiązania są gruntownie sprawdzane, umożliwiając podjęcie odpowiednich działań wyprzedzających lub czynności stricte wykrywczych. Operacyjne projekty analityczne wspomagają procesy rozpoznawania oraz rozpracowywania zorganizowanych grup przestępczych o charakterze międzynarodowym[13].

[13] Por. P. Chlebowicz, W. Filipkowski, *Analiza kryminalna. Aspekty kryminalistyczne*

Każdy operacyjny projekt analityczny wymaga utworzenia grupy analitycznej, w której ramach ściśle ze sobą współpracują:

- analitycy Europolu,
- inni urzędnicy Europolu wyznaczeni przez dyrekcję,
- oficerowie łącznikowi państw członkowskich,
- eksperci państw członkowskich dostarczających informacje lub zainteresowanych analizą.

Do wprowadzania danych do określonego pliku roboczego oraz ich zmieniania są uprawnieni jedynie analitycy. Wszyscy uczestnicy rozpracowania analitycznego mogą pobierać dane z takiego pliku. Zgodnie z zasadami uczestnictwa podmioty – w zależności od powierzonej im roli – mogą mieć status wiodący lub wspierający. Zadaniem podmiotu wiodącego jest gromadzenie, przetwarzanie i przekazywanie informacji do krajowej jednostki Europolu, podmiotu wspierającego zaś – analizowanie danych zgromadzonych w systemach informacyjnych policji w celu wskazania podmiotowi wiodącemu tych informacji, które są w zainteresowaniu danego rozpracowania, a także przekazywanie zgromadzonych informacji do Europolu.

W praktyce grupę analityczną pracującą nad danym plikiem roboczym tworzą pracownicy Europolu, z których jeden jest tzw. menedżerem projektu, pozostali zaś pełnią funkcje analityków (są to osoby mające odpowiednie specjalistyczne przeszkolenie[14]) oraz tzw. specjalistów (osoby z określoną wiedzą merytoryczną niezbędną dla danego rozpracowania). Nad danym zagadnieniem pracują dodatkowo osoby, które nie są pracownikami Europolu, są natomiast funkcjonariuszami lub pracownikami organów ścigania lub organizacji rządowych. Na podobnej zasadzie nad danym plikiem pracują osoby niebędące pracownikami Europolu, ale będące funkcjonariuszami lub pracownikami organów ścigania albo organizacji rządowych tzw. państw trzecich, które na podstawie odpowiednich umów wymieniają informacje z Europolem. Analitycy Europolu, którzy są przydzielani do konkretnego projektu, współpracują bezpośrednio z przedstawicielami krajowych zespołów operacyjnych lub dochodzeniowych. Ich zadaniem jest wskazywanie potrzeb zdobycia informacji źródłowych koniecznych do analizy oraz uczestniczenie w określaniu zawartości baz danych. Europol może zaprosić ekspertów z państw trzecich do współpracy w grupie analitycznej pod następującymi warunkami:

- pomiędzy Europolem i danym podmiotem obowiązuje porozumienie lub uzgodnienie robocze zawierające odpowiednie postanowienia dotyczące

i prawnodowodowe, Warszawa 2011.

[14] Takie szkolenia są prowadzone na podstawie określonych standardów gwarantujących możliwość dalszej współpracy analityków kryminalnych z różnych krajów. W Polsce prowadzi się je w jedynym ośrodku przygotowującym kadry, tj. w Wyższej Szkole Policji w Szczytnie. Przygotowanie analityka kryminalnego oprócz specjalistycznego testu psychologicznego i rozmowy kwalifikacyjnej obejmuje przede wszystkim czterotygodniowe szkolenie według programu ANACAPA. Podczas szkolenia uczestnicy zapoznają się z technikami analitycznymi służącymi do wizualizacji informacji oraz obsługi oprogramowania pakietu analitycznego *Analyst Notebook.*

wymiany informacji, w tym przekazywania danych osobowych, oraz poufności wymienianych informacji[15],
- włączenie do współpracy ekspertów danego podmiotu leży w interesie państw członkowskich,
- dany podmiot jest bezpośrednio zainteresowany przedmiotowymi pracami nad analizą,
- wszyscy uczestnicy wyrażają jednomyślnie zgodę na włączenie do prac grupy analitycznej ekspertów danego podmiotu[16].

Rozpracowania analityczne są unikalną i zarazem najbardziej efektywną formą pracy operacyjnej Europolu stwarzającą wiele możliwości w zakresie wykrywania. Rozpracowania analityczne mają na celu identyfikowanie powiązań między sprawami prowadzonymi w państwach członkowskich. Procedura wszczynania rozpracowania analitycznego jest skomplikowana i obejmuje kilka etapów. Najważniejszymi są: wystąpienie z inicjatywą wszczęcia rozpracowania analitycznego, opracowanie studium wykonalności projektu analitycznego, przygotowanie dokumentacji wymaganej do otwarcia AWF i dokumentów planistycznych, przyjęcie oraz rozpoczęcie projektu analitycznego. Przykłady rozpracowań analitycznych ukierunkowanych na wykrywanie zagrożeń związanych z terroryzmem, które były realizowane przez Europol w ostatnich latach, przedstawiono w tabeli.

Tabela. Rozpracowania analityczne Europolu ukierunkowane na wykrywanie zagrożeń związanych z terroryzmem.

Nazwa AWF	**Przedmiot rozpracowania analitycznego**
Hydra	zwalczanie przestępstw powiązanych z działalnością islamskich ekstremistycznych grup lub organizacji terrorystycznych. W ramach tego rozpracowania są wykrywane również zagrożenia dotyczące: finansowania grup terrorystycznych przez islamskie organizacje charytatywne, kurierów przewożących znaczne ilości gotówki w celu finansowania aktów terrorystycznych, wykorzystywania fałszywych kart kredytowych, stosowania oszustw bankowych, a także produkcji fałszywych dokumentów tożsamości na użytek terrorystów
Dolphin	zwalczanie grup terrorystycznych wskazanych przez Radę UE jako stwarzające poważne zagrożenie dla państw członkowskich UE

Źródło: Opracowanie własne.

[15] Państwa objęte jedynie porozumieniem strategicznym nie mogą być zaproszone (np. Rosja, Turcja). Protokół duński wprowadził jednak możliwość przekazywania danych państwu trzeciemu, które nie ma umowy o współpracy operacyjnej z Europolem, w wyjątkowych przypadkach i tylko w razie pilnej potrzeby na podstawie decyzji dyrektora Europolu.

[16] Art. 2 *Decyzji Zarządu Europolu z dnia 20 marca 2007 r. określającej zasady regulujące porozumienia dotyczące włączania ekspertów stron trzecich do działań grup analitycznych* (Dz. Urz. UE C 72 z 29 marca 2007 r., s. 32).

Obecnie obowiązującym aktem jest rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) przywołane w przypisie 5 (dop. red.).

W ramach rozpracowań analitycznych są stosowane następujące taktyczno-kryminalne metody działania:

- gromadzenie informacji kryminalnych,
- operacyjna analiza kryminalna,
- strategiczna analiza kryminalna,
- wymiana informacji kryminalnych.

Gromadzenie informacji kryminalnych

Do tych celów są wykorzystywane wspomniane pliki robocze, w których są zawarte wszechstronne dane wywiadowcze zebrane na potrzeby analizy kryminalnej (operacyjnej i strategicznej). Informacje dotyczące zarówno spraw operacyjnych, jak i dochodzeń są dostarczane przez policje krajów członkowskich. W plikach roboczych są gromadzone dane osobowe i nieosobowe, między innymi o następujących kategoriach osób:

- które zgodnie z prawem krajowym danego państwa członkowskiego są podejrzewane o popełnienie przestępstwa wchodzącego w zakres kompetencji Europolu lub o udział w takim przestępstwie, lub które są skazane za takie przestępstwo,
- wobec których istnieją rzeczywiste wskazania lub poważne podstawy – na mocy prawa krajowego danego państwa członkowskiego – do podejrzeń, że popełnią one przestępstwo wchodzące w zakres kompetencji Europolu,
- które mogą być wezwane do złożenia zeznań w śledztwach lub dochodzeniach w związku z rozpatrywanymi przestępstwami lub w dalszym postępowaniu karnym,
- będących ofiarami jednego z rozpatrywanych przestępstw lub w odniesieniu do których pewne fakty dają podstawy, aby uważać, że te osoby mogą się stać ofiarami takiego przestępstwa,
- mających kontakty z osobami powiązanymi,
- które mogą dostarczyć informacji na temat rozpatrywanych przestępstw.

Szczególnemu reżimowi podlega: gromadzenie, przechowywanie i przetwarzanie danych osobowych dotyczących zarówno pochodzenia rasowego, poglądów politycznych, przekonań religijnych lub innych, jak i informacji o stanie zdrowia oraz życiu seksualnym.

Dane do plików analitycznych są dostarczane głównie przez państwa członkowskie w językach narodowych lub w języku angielskim.

Operacyjna analiza kryminalna

Ta metoda, rozumiana jako instrument wykrywczy, jest wykorzystywana przede wszystkim w sprawach wieloaspektowych obejmujących znaczną liczbę wątków kryminalnych, w których występują skomplikowane powiązania przestępcze oraz pojawia się duża liczba informacji, a ich przetworzenie z zastosowaniem tradycyjnych metod i technik byłoby utrudnione lub wręcz niemożliwe. Operacyjna analiza kryminalna służy przede wszystkim osiąganiu celów procesu wykrywczego.

W ramach analizy operacyjnej stosuje się metody pozwalające na ustalenie sposobu prowadzenia działalności przestępnej, identyfikowanie związków między różnymi obiektami analitycznym (osoba, rzecz, miejsce) oraz określenie struktury zorganizowanych grup przestępczych. Są nimi m.in.:

- analiza sposobu dokonywania danego rodzaju przestępstw (modus operandi),
- analiza porównawcza przestępstw,
- analiza organizacji przestępczych,
- analiza gromadzenia danych w projekcie,
- analiza finansowania przestępstw,
- analiza metod zastosowanych w projekcie.

Wypracowane w Europolu wyniki analiz mogą służyć do inicjowania i wspierania dochodzeń w poszczególnych państwach członkowskich. Dotyczy to zwłaszcza postępowań, które mogą być prowadzone tylko zgodnie z przepisami prawa krajowego i przez odpowiedni organ krajowy, mające jednak powiązania międzynarodowe i tym samym wymagające ścisłej współpracy z Europolem za pośrednictwem oficerów łącznikowych poszczególnych krajów[17].

Strategiczna analiza kryminalna

Podstawową funkcją tej metody jest wspomaganie procesów decyzyjnych. Zastosowanie analizy strategicznej ma na celu dostarczenie kierownictwu policji wszechstronnego materiału diagnozującego obszary potencjalnych zagrożeń wraz z podaniem szacowanej skali i prawdopodobieństwa wystąpienia. W założeniu ten materiał powinien być podstawą do podjęcia skoordynowanych i wyprzedzających działań prewencyjnych. Dzięki temu znacznie rzadziej będzie dochodzić do sytuacji, w których policja zostaje zaskoczona wystąpieniem niespodziewanego zagrożenia lub sytuacji kryzysowej. Wskazane podejście jest zgodne z najnowszymi standardami działania organów ścigania państw członkowskich UE, tzw. *intelligence-led policing*. Z instytucjonalnego punktu widzenia wiodącą rolę w wykorzystaniu analizy strategicznej w procesie zwalczania przestępczości zorganizowanej odgrywa Europol.

Strategiczna analiza kryminalna skupia się na prognozowaniu kierunku oraz siły rozwoju zagrożeń, ocenie ryzyka ich wystąpienia, a także ustalaniu priorytetów, mechanizmów i strategii przeciwdziałania. Przedmiotem analizy są zasoby potencjału przestępczego i ich źródła, a także założenia działań przestępczych. Obejmuje ona również przegląd danych niezwiązanych z konkretnym dochodzeniem czy rozpracowaniem i w związku z tym nie obejmuje danych osobowych. W ujęciu praktycznym strategiczną analizę kryminalną – obok analizy operacyjnej (taktycznej) – postrzega się jako integralną część analizy kryminalnej.

Ta metoda działania jest również odpowiedzią na potrzeby dotyczące polityki bezpieczeństwa i zwalczania przestępczości. Konsekwencją jej zastosowania jest

[17] Zob. P. Chlebowicz, J. Kamińska, *Operacyjna analiza kryminalna w służbach policyjnych*, Warszawa 2015.

dostarczenie szczeblowi kierowniczemu wszechstronnego materiału, dzięki któremu można zdiagnozować obszary potencjalnych zagrożeń wraz z podaniem szacowanej skali i prawdopodobieństwa wystąpienia.

Podczas realizowania analiz strategicznych Europol opracowuje raporty ogólne obejmujące ocenę zagrożenia oraz ocenę ryzyka, przygotowuje rekomendacje dotyczące zwalczania przestępczości zorganizowanej, fenomenologię oraz analizy strukturalne przestępstw na podstawie danych wywiadowczych przekazanych przez kraje członkowskie lub uzyskane z innych źródeł, co pozwala na rozpoznawanie sposobów, obszarów oraz struktur działalności przestępczej. Dzięki prowadzeniu wywiadu kryminalnego (w tym analizy kryminalnej) Europol rozpoznaje i tworzy obraz przestępczości transgranicznej w UE.

Wymiana informacji kryminalnych

Jest to metoda działania polegająca na przekazywaniu, udostępnianiu, uzyskiwaniu lub otrzymywaniu informacji przez organy ścigania lub inne podmioty uprawnione. Europol jest odpowiedzialny za wymianę informacji zgodnie z obowiązującym prawem. Przepisy rozporządzenia Parlamentu Europejskiego i Rady (UE) 2016/794 w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol) dotyczące wymiany informacji i danych wywiadowczych określają ramy działania umożliwiające tę wymianę. Regulują one obieg informacji w ramach Europolu, co ułatwia tej instytucji realizowanie zadań analitycznych dzięki uzupełnianiu swoich baz danych i systemu informacyjnego. W przepisach przewidziano przekazywanie informacji przez Europol właściwym organom państw członkowskich, gdyż jest on zobowiązany do niezwłocznego powiadamiania tych podmiotów o otrzymywanych informacjach ich dotyczących, a także o wszelkich powiązaniach między przestępstwami kryminalnymi, które ustalono. Europol przekazuje również informacje dotyczące przestępców, przestępstw i związanych z nimi miejsc, przedmiotów, zdarzeń, sposobów działań przestępczych, zjawisk kryminalnych oraz ogólnych zagrożeń.

Model wymiany informacji został opracowany przy współpracy z państwami członkowskimi i uzgodniony przez szefów krajowych jednostek Europolu. Gwarantuje on ścisłe przestrzeganie przepisów dotyczących bezpieczeństwa danych. W tym modelu zakłada się współpracę w układach bilateralnych i multilateralnych. W praktyce obieg informacji przebiega następująco:

- krajowa jednostka Europolu – krajowe biuro łącznikowe – Europol,
- właściwa instytucja krajowa – krajowe biuro łącznikowe – Europol.

Poziomy rozpracowań analitycznych

Krajowe służby policyjne jako niedoskonałości rozpracowań analitycznych wskazywały na ich niewystarczający zakres zainteresowania lub zbyt wąskie ukierunkowanie. Niektóre państwa członkowskie optowały za wszczynaniem rozpracowań analitycznych z zastosowaniem wyłącznie podejścia regionalnego.

Mając na względzie te ograniczenia, w 2013 r. rozpracowania analityczne podzielono na trzy poziomy:

1) rozpracowania strategiczne,
2) rozpracowania operacyjne,
3) rozpracowania celowe.

Rozpracowania strategiczne

Mają one na celu przetwarzanie informacji dotyczących przestępczości zorganizowanej i terroryzmu w jak najszerszym wymiarze przestrzennym i czasowym. Prowadzenie rozpracowań analitycznych na poziomie strategicznym pozwala Europolowi na poinformowanie państw o rozmiarach i kierunkach rozwoju zagrożeń oraz na dostarczenie im danych potrzebnych do podjęcia działań wyprzedzających (np. decyzji politycznych, zmian prawa). W chwili obecnej Europol prowadzi dwa rozpracowania analityczne na poziomie strategicznym: AWF Serious Organized Crime (Poważna Przestępczość Zorganizowana) oraz AWF Counter Terrroism (Zwalczanie Terroryzmu)[18].

Rozpracowania operacyjne

Są one ukierunkowane na uzyskiwanie informacji o danym rodzaju przestępczości zorganizowanej oraz działalności terrorystycznej lub o strukturze zagrożenia przestępczością zorganizowaną w danym regionie UE. Zgodnie z przyjętą przez Europol terminologią rozpracowania analityczne prowadzone na poziomie operacyjnym są określane mianem „Focal Points"[19]. Rozpracowania operacyjne mogą być ukierunkowane terytorialnie (np. Bałkany, region Morza Bałtyckiego), podmiotowo (np. rosyjskojęzyczne zorganizowane grupy przestępcze, albańskie grupy przestępcze), na obszar działalności przestępczej (np. handel ludźmi, wyłudzenie podatku VAT) bądź rodzaj dóbr czy towarów będących przedmiotem działalności przestępczej (np. narkotyki, wyroby akcyzowe, waluta euro).

Rozpracowania celowe

Zmierzają one do wykrycia konkretnych zorganizowanych grup przestępczych lub organizacji terrorystycznych, przestępstw oraz ich sprawców. Zgodnie z przyjętą przez Europol terminologią rozpracowania analityczne prowadzone na poziomie celowym są określane mianem „Target Groups"[20].

Dane wywiadowcze uzyskane w wyniku rozpracowań celowych są przekazywane służbom policyjnym zainteresowanych państw członkowskich. Często te służby mają duży potencjał wykrywczy, co umożliwia policjom krajowym podjęcie konkretnych

[18] *Europol, New AWF Concept Guide for MS and Third Parties*, Haga 2012, http://www.statewatch.org/news/2013/jan/europol-awf-new-concept.pdf, s. 10 [dostęp: 15 III 2018].

[19] Tamże, s. 5.

[20] Tamże, s. 7.

działań operacyjnych (np. obserwację, kontrolę operacyjną) lub procesowych (np. zatrzymania, przeszukania). Przykładem może być działanie Europolu w Wielkiej Brytanii w 2010 r., gdy wspierał on jednostkę antyterrorystyczną policji hrabstwa Greater Manchester w brytyjskiej operacji antyterrorystycznej. Przebadano wówczas około 6 tys. dokumentów elektronicznych przekazanych przez policję hrabstwa Greater Manchester, głównie w języku arabskim, aby zidentyfikować osoby mogące stwarzać zagrożenie bezpieczeństwa Wielkiej Brytanii. Weryfikacja plików elektronicznych z systemami Europolu ujawniła istnienie materiałów związanych z terroryzmem. Praca Europolu doprowadziła do wykrycia ekstremistycznego kaznodziei, który był obiektem zainteresowania w innych dochodzeniach prowadzonych w UE. Europol wykorzystał materiały przekazane przez policję hrabstwa Greater Manchester do przeanalizowania ideologii promowanej przez podejrzanego. Wynikiem tych działań Europolu było sporządzenie sprawozdania oraz oceny zagrożenia stwarzanego przez podejrzanego i jego zwolenników w Europie, które wykazały powiązania z dochodzeniami prowadzonymi przez państwa członkowskie. Główny podejrzany został skazany na dwa lata więzienia po uznaniu go za winnego dwóch zarzutów na mocy sekcji 58 ustawy w sprawie terroryzmu (*Terrorism Act 2000*[21]) w związku z posiadaniem materiałów do celów terrorystycznych[22].

Skuteczność opisanych powyżej działań była uzależniona od dostarczenia przez Europol służbom policyjnym państw członkowskich odpowiednich danych wywiadowczych. Jakość danych wywiadowczych wykorzystywanych w razpracowaniach analitycznych jest determinowana bezpośrednio liczbą i jakością przekazanych uprzednio Europolowi informacji kryminalnych. Dostarczycielem tych informacji są państwa członkowskie UE. Występuje tu zatem swoiste sprzężenie zwrotne między pracą wywiadowczą państw członkowskich a pracą Europolu.

Zakończenie

Po przeanalizowaniu przepisów regulujących działanie Europolu można przyjąć następujące założenia istotne dla rozpracowywania działalności terrorystycznej:

1. Kompetencje kontrterrorystyczne Europolu są ściśle określone przepisami prawa (dokładnie wiadomo, jakie działania ta instytucja ma wykonywać lub jakich czynności nie wolno jej podejmować). Formy i metody realizacji omawianych kompetencji wynikają z już ugruntowanej praktyki policyjnej współpracy międzynarodowej.
2. Rozpracowywanie działalności terrorystycznej przez Europol polega przede wszystkim na wykonywaniu zadań wywiadu kryminalnego, takich jak gromadzenie, przetwarzanie (analiza, ocena, interpretacja) oraz wymiana informacji i danych wywiadowczych. Wykorzystanie informacji i danych wywiadowczych przekazywanych w ramach prowadzonych dochodzeń i działań wspólnych

[21] https://www.legislation.gov.uk/ukpga/2000/11/section/58 [dostęp: 15 III 2018].
[22] *Przegląd Europolu. Sprawozdanie ogólne z działalności Europolu*, Haga 2011, s. 28.

zespołów śledczych za pośrednictwem Europolu podlega takim samym rygorom ochrony danych, jakby zostały uzyskane w państwie członkowskim, które te dane otrzymało.

3. Wsparcie kontrterrorystyczne jest udzielane z reguły na wniosek państwa członkowskiego (wyjątek stanowi tzw. spontaniczne przekazanie informacji).
4. Rozpracowywanie działalności terrorystycznej w ramach Europolu wymaga wysokiego profesjonalizmu funkcjonariuszy. Muszą oni wykazać się gruntowną wiedzą zawodową, zdolnościami analitycznymi oraz biegłą znajomością języka angielskiego, a także posiadać rzetelną wiedzę ogólną, prawniczą, kulturową. Ponadto muszą być doskonale przygotowani pod względem informatycznym. Współdziałanie zawsze wiąże się z reprezentowaniem macierzystego państwa, dlatego zadania realizowane nieprofesjonalnie zwykle powodują straty wizerunkowe państwa delegującego, mogą też doprowadzić do odpowiedzialności sądowej za wyrządzone szkody.

Dotychczas Polska uczestniczyła w kilkunastu rozpracowaniach analitycznych, w tym m.in.: AWF „Islamic Terrorism" oraz AWF Hydra (oba rozpracowania dotyczyły działalności terrorystycznej islamskich ekstremistów).

Funkcjonujący w Policji system przetwarzania informacji na potrzeby rozpracowań analitycznych Europolu jest oparty na: wskazaniu osób odpowiedzialnych za koordynację przekazywania informacji na poszczególnych szczeblach organizacyjnych Policji, wyznaczeniu funkcjonariuszy realizujących zadania w grupie analitycznej powołanej przez Europol na rzecz konkretnego pliku roboczego (tzw. eksperci krajowi), opracowaniu procedur obowiązujących przy przetwarzaniu tego typu informacji oraz organizacji szkoleń dotyczących funkcjonalności i wykorzystania AWF. Omawiane założenia zostały wypracowane ponad 10 lat temu w Komendzie Głównej Policji[23].

Do zadań ekspertów krajowych należy przede wszystkim:

- przekazywanie informacji do poszczególnych plików roboczych dotyczących danych zgromadzonych w prowadzonych postępowaniach przygotowawczych lub czynnościach operacyjno-rozpoznawczych,
- przekazywanie informacji uzyskanych z poszczególnych plików roboczych zainteresowanym jednostkom organizacyjnym Policji oraz innym organom powołanym do ochrony bezpieczeństwa i porządku publicznego,
- koordynowanie współpracy Policji z partnerami krajowymi i zagranicznymi w zakresie plików roboczych,
- udział w spotkaniach wynikających z członkostwa Rzeczpospolitej Polskiej w poszczególnych plikach roboczych,

[23] Są one wynikiem prac przeprowadzonych przez zespoły powołane: decyzją nr 211 KGP z 21 marca 2007 r. w sprawie powołania zespołu do opracowania koncepcji ilościowej i jakościowej polskiej kontrybucji do Analitycznych Plików Roboczych Europolu – AWF, decyzją nr 47 KGP w sprawie powołania zespołu do oceny możliwości zwiększenia zaangażowania Policji w międzynarodowych inicjatywach dotyczących zwalczania wschodnioeuropejskiej przestępczości zorganizowanej (niepublikowane) oraz *Decyzją nr 60 Komendanta Głównego Policji z dnia 3 marca 2010 r. w sprawie ekspertów krajowych realizujących zadania w zakresie plików roboczych Europejskiego Urzędu Policji (Europol)* (Dz. Urz. KGP z 2010 r. nr 3 poz. 11).

– inicjowanie i prowadzenie podjętych działań informacyjnych zmierzających do zwiększenia wiedzy na temat plików roboczych w służbie kryminalnej Policji, a także udostępnianie organom bezpieczeństwa i porządku publicznego informacji dotyczących zakresu działania podejmowanych w ramach poszczególnych plików roboczych,
– przekazywanie informacji ze swojej działalności koordynatorowi krajowemu podczas spotkań[24].

Eksperci krajowi wykonują czynności przewidziane dla danej komórki organizacyjnej Komendy Głównej Policji dotyczące realizacji zadań w ramach grupy analitycznej powołanej na potrzeby określonego rozpracowania analitycznego. Są oni też obowiązani do udzielania wsparcia merytorycznego policjantom pełniącym służbę w jednostkach organizacyjnych Policji[25]. Oprócz wymienionych zadań eksperci mogą kierować wnioski do jednostek organizacyjnych Policji o udostępnienie tych danych. Na podstawie złożonych wniosków jednostki Policji przekazują ekspertom krajowym informacje dotyczące poszczególnych plików roboczych, chyba że ich przekazanie mogłoby utrudniać postępowanie karne lub czynności operacyjno-rozpoznawcze (albo innego rodzaju czynności w sprawach o przestępstwa) lub mogłoby zagrozić bezpieczeństwu osób biorących w nich udział[26]. Eksperci krajowi są powoływani i nadzorowani przez kierowników komórek organizacyjnych służby kryminalnej i śledczej KGP[27]. Za koordynację działań ekspertów krajowych odpowiada kierownik komórki organizacyjnej KGP właściwej w sprawach współpracy międzynarodowej. Organizuje on również spotkania z ekspertami krajowymi w celu zapewnienia im pomocy w prawidłowym i efektywnym wykonywaniu zadań, a także wyznacza koordynatora krajowego z podległej komórki organizacyjnej w celu nadzorowania pracy ekspertów krajowych w zakresie realizowanych zadań[28].

Rozpracowywanie działalności terrorystycznej należy do zadań najtrudniejszych i wymaga działań wspomagających (wymiany informacji, analizy kryminalnej). Europol jest angażowany w wykonywanie operacyjnych analiz kryminalnych w sprawach, w których ze względu na aspekty podmiotowe (sprawca, pokrzywdzony) lub przedmiotowe (miejsce, czas, modus operandi, przedmiot czynności wykonawczej) istnieje potrzeba ustalenia powiązań między poszczególnymi elementami zdarzeń w różnych państwach. Dzięki międzynarodowej wymianie informacji i analizie kryminalnej (np. połączonej analizie danych telekomunikacyjnych z kilku państw członkowskich) możliwe jest zdobycie danych wywiadowczych, które zwiększają prawdopodobieństwo wykrycia zagrożeń terrorystycznych. W tych przypadkach rola Europolu polega na tworzeniu przewagi informacyjnej policji krajowych podejmujących czynności

[24] *Decyzja nr 60 Komendanta Głównego Policji z dnia 3 marca 2010 r. w sprawie ekspertów*, paragraf 4.
[25] Tamże, paragraf 5 ust. 3.
[26] Tamże, paragraf 5 ust. 1, 2.
[27] Tamże, paragraf 6, 8.
[28] Tamże, paragraf 7.

operacyjne lub procesowe. Europol stwarza możliwości uzyskania pogłębionych informacji o przestępczości zorganizowanej i zagrożeniach terrorystycznych na potrzeby krajowych służb policyjnych. Materiały wywiadowcze przekazywane przez Europol państwom członkowskim często przyczyniają się do wykrycia przestępstw, struktur organizacyjnych grup przestępczych czy siatek terrorystycznych. Zgromadzenie tego rodzaju materiałów przez krajowe służby policyjne w inny sposób niż w warunkach współpracy w ramach Europolu byłoby znacznie utrudnione. Działania Europolu często pozwalają na znalezienie dodatkowych wątków wykrywczych, a nawet na wskazanie potencjalnych źródeł dowodowych.

Podstawowa rola Europolu w wykrywaniu zagrożeń wynika z możliwości wzmocnienia efektywności działań wykrywczych na poziomie krajowym. Z tego powodu większość działań tej instytucji toczy się równolegle do krajowych działań wykrywczych. Rozpracowania analityczne Europolu były często punktem wyjścia i osią procesu wykrywczego w wielu sprawach o charakterze międzynarodowym. Przedstawiona ocena nie umniejsza podstawowego znaczenia działań realizowanych w celach wykrywaczych przez właściwe organy państw członkowskich. Rezultat wykrywczy działań operacyjnych Europolu musi być bowiem przełożony na mechanizmy zgodne z regułami prawnymi państwa członkowskiego.

Główną przeszkodą w osiągnięciu skuteczności Europolu podczas rozpracowywania działalności terrorystycznej jest nadal ograniczone zaufanie praktyków (funkcjonariuszy) do formuły wielostronnej współpracy, którzy niechętnie dostarczają informacji do rozpracowań analitycznych Europolu (dotyczy to przede wszystkim wrażliwych informacji kryminalnych na temat planowanych zamachów terrorystycznych). W rezultacie Europol nie jest w stanie przygotować danych wywiadowczych o potencjale wyprzedzającym (mogących zapobiec atakowi terrorystycznemu). Może on jedynie śledzić przepływ finansowania działalności terrorystycznej i wskazywać powiązania pomiędzy podejrzanymi o terroryzm, a także źródła pochodzenia nielegalnej broni palnej oraz fałszywych dokumentów – dopiero po przeprowadzonym ataku terrorystycznym[29].

Wrażliwe informacje kryminalne są wymieniane między biurami łącznikowymi państw członkowskich przy Europolu. Kopie tych informacji bardzo rzadko trafiają do rozpracowań analitycznych. Wykorzystanie bezpośredniej współpracy biur łącznikowych to w rzeczywistości ominięcie centralnych systemów wywiadowczych Europolu[30].

Dzielenie się informacjami kryminalnymi podczas współpracy międzynarodowej jest z reguły ograniczone, a przez to ta współpraca jest nieoptymalna[31]. Ze względu na koszty pozyskiwania informacji kryminalnych związanych z zagrożeniami terrorystycznymi i ich wrażliwością rozpracowywanie tych zagrożeń nadal będzie oparte na bezpośrednich relacjach między służbami antyterrorystycznymi państw członkowskich UE. Jest to sprzeczne z ogólną ideą wielostronnej współpracy w ramach Europolu.

[29] T. Safjański, *Barriers to the Operational Effectiveness of Europol*, „Internal Security" 2013, nr 1.

[30] A. James, *Understanding police intelligence work*, t. 2. Bristol 2016, s. 45.

[31] A. James, *Examining intelligence-led policing: developments in research, policy and practice*, [b.m.w.] 2013, s. 100.

Należy zauważyć, że interakcja występująca na styku działań antyterrorystycznych służb wywiadowczych jest sytuacją strategiczną wymagającą podjęcia decyzji: podjąć współpracę czy nie wymieniać informacji? Z politycznego punktu widzenia podjęcie współpracy jest często sprzeczne z interesem operacyjnym konkretnej służby wywiadowczej. Może wówczas zaistnieć konflikt interesów między poszczególnymi służbami wywiadowczymi. Tworząca się relacja współzależności między nimi może spowodować sytuację, w której konkretne zachowanie jednej ze służb ogranicza lub wymusza zachowanie drugiej służby. Racjonalne podejście do wymiany informacji kryminalnych zakłada, że służba współzależna będzie kierowała się interesem własnym i nie wybierze strategii współpracy obciążonej ryzykiem braku efektu (lub poniesienia strat operacyjnych), lecz wybierze bezpieczną strategię odstąpienia od współpracy – w najgorszym przypadku uzyska gorszy rezultat niż przy obustronnej współpracy. Jeżeli taką logikę zastosują obydwie współzależne służby wywiadowcze, to nie dojdzie do wymiany informacji kryminalnych. Opisana sytuacja jest modelowaną na tzw. dylemacie więźnia[32], a współzależność pozostaje w tzw. równowadze Nasha[33]. Oznacza to, że o ile podmioty sytuacji strategicznej są racjonalne, nie mają powodu, aby zachować się inaczej niż tak, jak to wyznacza równowaga Nasha.

Relacje między wszystkimi służbami wywiadowczymi nie muszą przebiegać w przedstawiony sposób. Zaufanie jest koniecznym elementem współpracy antyterrorystycznej. Badacze przedmiotu podnoszą od dawna, że zaufanie (lub ściślej mówiąc – brak zaufania) leży u podstaw problemu dzielenia się informacjami kryminalnymi. Istnieją dowody na występowanie zaburzeń w relacjach Europolu z państwami członkowskimi, które polegają na niechęci dzielenia się informacjami, zwłaszcza gdy dzielenie się nimi wykracza poza ich własne środowisko operacyjne. Sytuacja staje się trudniejsza, gdy wzrasta stawka operacyjna, co prowadzi do naturalnego wzrostu nieufności. Prawdopodobnie to brak zaufania do Europolu jest istotnym czynnikiem powodującym, że ta instytucja gromadzi małą liczbę informacji dotyczących rozpoznawania aktów terrorystycznych, a co za tym idzie – ogranicza ich wykrywanie i im zapobieganie[34].

[32] Problem w teorii gier oparty na dwuosobowej grze o niezerowej sumie, w której każdy z graczy może zyskać, zdradzając przeciwnika, ale obaj stracą, jeśli obaj będą zdradzać. Dylemat ten jest więc niekooperacyjną (o częściowym konflikcie) grą o sumie niezerowej, ponieważ strategia konfliktu przeważa nad strategią pokojową: najwięcej można zyskać zdradzając, a najwięcej stracić – idąc na współpracę.

[33] Profil strategii teorii gier, w którym strategia każdego z graczy jest optymalna, przyjmując wybór jego oponentów za ustalony. W równowadze żaden z graczy nie ma powodów jednostronnie odstępować od strategii równowagi. W tym sensie równowaga jest stabilna. Równowaga Nasha nie musi być efektywna w sensie Pareto. Klasycznym przykładem tej nieefektywności jest paradoks znany jako „dylemat więźnia".

[34] Zob. A. James, T. Safjański, *Europol's Crime Analysis System – Practical Determinants of Its Success*, „Policing: A Journal of Policy and Practice" 2018, nr 2, https"//www.reserchgate.net/publication/324532427_Draft_for_submission_to_Policing_–Europol_paper [dostęp:15 III 2018].

Bibliografia:

Chlebowicz P., Filipkowski W., *Analiza kryminalna. Aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011, Wolters Kluwer.

Chlebowicz P., Kamińska J., *Operacyjna analiza kryminalna w służbach policyjnych*, Warszawa 2015, Difin.

Europol, New AWF Concept Guide for MS and Third Parties, Haga 2012, http://www.statewatch.org/news/2013/jan/europol-awf-new-concept.pdf, s. 10 [dostęp:15 III 2018].

Gruszczak A., *Europejska wspólnota wywiadowcza. Prawo – instytucje – mechanizmy*, Kraków 2014, Wydawnictwo Uniwersytetu Jagiellońskiego.

Hanausek T., *Zarys kryminalistycznej teorii wykrywania*, cz. 2, Warszawa 1987, Departament Szkolenia i Doskonalenia Zawodowego MSW.

James A., *Examining intelligence-led policing: developments in research, policy and practice*, [b.m.w.] 2013, Palgrave Macmillan.

James A., *Understanding Police Intelligence Work*, Bristol 2016, Policy Press.

James A., Safjański T., *Europol's Crime Analysis System – Practical Determinants of Its Success*, „Policing: Journal of Policy and Practice" 2018, nr 2, https://www.reserchgate.net/publication/324532427_Draft_fot_submission_to_Policing_–Europol_paper [dostęp: 15 III 2018].

Pikulski S., *Podstawowe zagadnienia taktyki kryminalistycznej*, Białystok 1997, Temida 2.

Przegląd Europolu. Sprawozdanie ogólne z działalności Europolu, Haga 2011, Europol; także https://www.europol.europa.eu/sites/default/files/documents/pl_europolreview.pdf [15 III 2018].

SOCTA 2013. EU Serious and Organised Crime Threat Assessment, Europol 2013, https://www.europol.europa.eu/sites/default/files/.../socta2013.pdf [dostęp 15 III 2018].

Safjański T., *Barriers to the Operational Effectiveness of Europol*, „Internal Security" 2013, nr 1, s. 53–69.

Safjański T., *Działania operacyjne Europolu*, Szczytno 2013, Wydawnictwo WSPol.

Safjański T., *Europejskie Biuro Policji Europol. Geneza. Główne aspekty działania. Perspektywy rozwoju*, Warszawa 2009, Wolters Kluwer.

Akty prawne:

Traktat o funkcjonowaniu Unii Europejskiej – wersja skonsolidowana (Dz. Urz. UE C 115 z 9 maja 2008 r., s. 49).

Konwencja sporządzona na podstawie artykułu K.3 Traktatu o Unii Europejskiej w sprawie ustanowienia Europejskiego Urzędu Policji (konwencja o Europolu), sporządzona w Brukseli dnia 26 lipca 1995 r. (Dz.U. z 2005 r. nr 29 poz. 243, ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/794 z dnia 11 maja 2016 r. w sprawie Agencji Unii Europejskiej ds. Współpracy Organów Ścigania (Europol), zastępujące i uchylające decyzje Rady 2009/371/WSiSW, 2009/934/WSiSW, 2009/935/WSiSW, 2009/936/WSiSW i 2009/968/WSiSW (Dz. Urz. UE L 135 z 24 maja 2016 r., s. 53).

Abstrakt

W artykule omówiono rolę Europolu w rozpracowywaniu działalności terrorystycznej. Rozpracowanie jest najważniejszą formą działań, w której materializują się funkcje kryminalistyki: rozpoznawanie, wykrywanie i zapobieganie. Uprawnienia operacyjne Europolu dotyczące rozpoznawania, wykrywania i zapobiegania terroryzmu wynikają bezpośrednio z *Traktatu o funkcjonowaniu Unii Europejskiej*. Z punktu widzenia taktyki kryminalistycznej, potencjał antyterrorystyczny Europolu jest oparty na specjalnych analitycznych bazach danych (AWF). W omawianym modelu informacje i dane wywiadowcze są gromadzone, przetwarzane i wymieniane w odniesieniu do ściśle określonych zagrożeń terrorystycznych (osób, grup przestępczych, organizacji terrorystycznych) w celu wsparcia spraw operacyjnych lub postępowań karnych prowadzonych przez krajowe organy policyjne państw członkowskich UE.

Słowa kluczowe: wykrywanie, współpraca międzynarodowa, Europol, rozpracowania analityczne, AWF, bezpieczeństwo UE, taktyka kryminalistyczna.

Dariusz Gradzi

Third Party Providers (TPP)[1] – nowi dostawcy usług płatniczych w środowisku internetowym i mobilnym. Przegląd regulacji prawnych i analiza możliwych zagrożeń cyberbezpieczeństwa płatniczej infrastruktury krytycznej

Uwagi wstępne

Dyrektywa w sprawie usług płatniczych (dalej: dyrektywa PSD I)[2] wprowadziła do europejskiego porządku prawnego pojęcia usługi płatnicze, zamknięty katalog usług płatniczych, a także podmioty mogące świadczyć usługi płatnicze (tzw. dostawcy). Od czasu jej wejścia w życie na rynku rozwinęły się nowe płatnicze usługi elektroniczne realizowane z wykorystaniem infrastruktury internetowej, w tym szczególnie usługi oparte na dostępie do rachunków płatniczych (m.in. bankowych) podmiotów trzecich, którym takie uprawnienie przyznał posiadacz (użytkownik) rachunku (np. klient banku).

Wśród płatności elektronicznych wyróżnia się płatności internetowe[3] oraz płatności mobilne[4]. Mogą one być przeprowadzane między innymi jako płatności przy użyciu karty płatniczej oraz poleceń przelewu (tradycyjny przelew bankowy lub tzw. *pay-by-link*[5] – PBL). Rozwój handlu w środowisku interne-

[1] Ang. *Third Party Payment Service Provider* – dostawca usług płatniczych będący podmiotem trzecim. Zob. M. Mostowik, *Prawna ochrona informacji o rachunku płatniczym w świetle usługi dostępu do informacji o rachunku (AIS)*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 32.

[2] *Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48 WE i uchylająca dyrektywę 97/5/WE* (Dz. Urz. UE L 319 z 5 grudnia 2007 r., s. 1).

[3] B. Chinowski, *Elektroniczne metody płatności. Istota, rozwój, prognozy*, https://www.knf.gov.pl/knf/pl/komponenty/img/Elektroniczne%20metody%20platnosci.pdf, s. 5 [dostęp: 20 X 2017].

[4] Są to płatności dokonywane przy użyciu mobilnego urządzenia wyposażonego w system operacyjny, z multimedialnym interfejsem z wykorzystaniem technologii radiowej, sieci telekomunikacyjnych bezprzewodowych (GSM, GPRS, UMTS, Wi-Fi, NFC, RFiD, Bluetooth), *Final recommendations for the security of payment account access services following the public consultation*, Europejski Bank Centralny, https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf [dostęp: 25 X 2017].

[5] Jest to metoda płatności internetowej polegająca na tym, że podczas zakupów online, przy dokonywaniu płatności przez „bramkę płatniczą", klient otrzymuje specjalny link, który przekierowuje go do banku prowadzącego jego rachunek. Po zalogowaniu się do systemu bankowości elektronicznej pojawia się uzupełniony format przelewu z danymi odbiorcy (przeważnie agenta rozliczeniowego) oraz kwotą. Po autoryzacji przelewu odbiorca dostaje komunikat o wykonaniu płatności i może przystąpić do wykonania umowy, co znacznie przyspiesza transakcje online. Warunkiem skorzystania przez płatnika z tej usługi jest jej udostępnianie przez bank, w którym płatnik ma rachunek. Por. M. Grabowski, *Instrumenty płatnicze w prawie polskim*, https://depotuw.ceon.pl/bitstream/handle/item/327/Instrumenty%20Płatnicze%20w%20prawie%20polskim.pdf?sequence=1, s. 211 [dostęp: 4 X 2017].

towym oraz konieczność przyspieszenia realizacji procesu płatności spowodował ewolucję usług inicjujących płatność przez wprowadzenie interfejsu (tzw. bramki płatniczej, ang. *payment gate*) łączącego stronę internetową akceptanta (np. sklepu) ze stroną dostawcy usług płatniczych (np. banku)[6]. Dodatkowo poza usługami płatniczymi mającymi na celu dokonanie płatności pomiędzy płatnikiem a odbiorcą środków (lub podmiotem działającym na podstawie umowy z nim zawartej, np. agentem rozliczeniowym) pojawiły się nowe usługi uzupełniające, o których będzie mowa w niniejszym artykule. Do nowych usług uzupełniających wprowadzonych drugą dyrektywą w sprawie usług płatniczych (dalej: dyrektywa PSD II)[7] należą:

– usługa inicjacji płatności przez podmiot trzeci,
– usługa dostępu do informacji o rachunku przez podmiot trzeci,
– potwierdzenie dostępności środków pieniężnych na rachunku płatniczym[8].

Powyższe usługi zapewniają użytkownikowi możliwość przyspieszenia transakcji płatniczej oraz dostęp do zagregowanych[9] informacji o rachunku płatniczym online, udostępnianych przez interfejs dostawcy prowadzącego rachunek płatniczy. Dzięki tej ostatniej usłudze użytkownik ma możliwość szybkiego zorientowania się w swojej sytuacji finansowej[10].

Przedmiotem niniejszego artykułu będzie prezentacja nowych usług płatniczych wprowadzonych do europejskiego, i tym samym – polskiego, porządku prawnego przez dyrektywę PSD II oraz zagrożeń w skali mikro i makro, jakie mogą się wiązać z ich funkcjonowaniem. Fundamentem regulacji zawartych w dyrektywie PSD II jest przyznanie płatnikom prawa do korzystania z usług podmiotów trzecich oraz konieczność respektowania tego prawa przez dostawcę prowadzącego rachunek płatniczy (w tym bankowy) – tzw. *Account Servicing Payment Service Provider* (ASPSP). W dyrektywie PSD II przewidziano odpowiednie mechanizmy[11] prawne przełamujące ewentualny brak woli współpracy ze strony ASPSP z TPP[12]. Dostawcy prowadzący rachunek płatniczy zostali zatem zmuszeni prawnie do współpracy z TPP.

---

[6] Por. motyw 27 do preambuły dyrektywy PSD II.

[7] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) 1093/2010 oraz uchylająca dyrektywę 2007/64/WE* (Dz. Urz. UE L 337 z 23 grudnia 2015 r., s. 35).

[8] W przeciwieństwie do usługi inicjacji płatności oraz usługi dostępu do informacji o rachunku potwierdzanie dostępności środków pieniężnych na rachunku nie jest odrębną usługą płatniczą. Por. K. Korus, *Usługi oparte na dostępie do rachunku w dyrektywie PSD II*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 85.

[9] Informacja zagregowana to wszelka informacja odnosząca się do wieloelementowych zbiorów obiektów jednostkowych lub wieloelementowych zbiorów cech tych obiektów, za: J. Oleński, *Ekonomika informacji. Podstawy*, Warszawa 2001, s. 209 (przyp. red.).

[10] Motyw 28 do preambuły dyrektywy PSD II.

[11] Są nimi: sankcje ze strony organu nadzoru – KNF, a także obowiązek notyfikacji wynikający z art. 68 ust. 6 dyrektywy PSD II.

[12] Należy zauważyć, że w ujęciu biznesowym TPP są bezpośrednią konkurencją dla ASPSP.

W obecnych realiach rynkowych ASPSP często uniemożliwiają rozwój TPP przez: blokowanie określonych adresów IP[13] tych dostawców, blokowanie rachunku bankowego płatnika[14] lub uniemożliwianie tzw. *screen scrapingu*[15].

Dane statystyczne i zagrożenia

Cechą wspólną usług TPP jest to, że w celu ich wykonania jest niezbędne uzyskanie przez podmiot trzeci dostępu do rachunku płatniczego (bankowego). Tego typu usługi do tej pory nie doczekały się regulacji prawnej, choć są realizowane na rynku finansowym od wielu lat. Powodem takiego stanu rzeczy było to, że w przypadku tych usług nie dochodzi do wejścia przez TPP w posiadanie środków pieniężnych[16]. A zatem ci dostawcy mogli korzystać z wyłączenia stosowania przepisów dyrektywy PSD I oraz ustawy o usługach płatniczych[17] (dalej: UUP) w brzmieniu przed implementacją do polskiego porządku prawnego dyrektywy PSD II[18]. Dyrektywa PSD II przyniosła zmiany w postaci konieczności – co do zasady – uzyskania zezwolenia organu nadzoru (w Polsce – Komisji Nadzoru Finansowego) na świadczenie tych usług.

Usługi TPP mają prowadzić do ułatwienia i przyspieszenia płatności w środowisku internetowym. Należy jednak zwrócić uwagę na możliwe zagrożenia, jakie będą się wiązały z pojawieniem się nowych usług oraz nowych dostawców. Według danych statystycznych liczba wykrytych cyberataków na firmy w Polsce w 2015 r. w stosunku do 2014 r. wzrosła o 46 proc. Największym czynnikiem ryzyka dla sektora finansowego jest zagrożenie atakami na systemy IT[19]. W 2014 r. w w naszym kraju około 230 tys. komputerów miało zainstalowane złośliwe oprogramowanie, z czego aż 50 tys. przypadków dotyczyło złośliwego oprogramowania w postaci trojana bankowego[20]. Liczba użytkowników bankowości mobilnej przez ostatnie cztery lata

[13] Ang. *Internet Protocol* (IP), zob. http://munitus.pl/co-to-jest-ip.html [dostęp: 4 X 2017].

[14] Zob. M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 33.

[15] Ang. s*creen scraping* – metoda dostępu do bankowości elektronicznej użytkownika polegająca na tym, że klient upoważnia bank (np. ten, w którym ubiega się o kredyt) do zalogowania się do jego rachunku płatniczego w innym banku (gdzie użytkownik posiada historię płatniczą) na skutek przekazania pierwszemu bankowi danych do logowania. Logowanie następuje przez analizę treści interfejsu bankowego za pośrednictwem systemu informatycznego pierwszego banku, który automatycznie dokonuje wprowadzenia loginu i hasła klienta w określone pola. Dalej następuje zalogowanie się do systemu bankowości elektronicznej. Zob. ostrzeżenie wydane przez KNF 14 VII 2014 r. pt. *Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego*, https://www.knf.gov.pl/?articleId=53072&p_id=18 [dostęp: 23 X 2017].

[16] Art. 6 pkt 10 UUP w zw. z art. 3 lit. 1 dyrektywy PSD I.

[17] *Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych* (t.j.: Dz.U. z 2017 r. poz. 2003, ze zm.).

[18] Co nastąpiło *Ustawą z dnia 10 maja 2018 r. o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw* (Dz.U. z 2018 r. poz. 1075).

[19] Ang. *Information Technology*, https://pl.wikipedia.org/wiki/Technologia_informacyjna [dostęp: 15 VIII 2018].

[20] Por. A. Marciniak, *Bankowy CERT – nowa broń w walce z cyberprzestępczością*, w: *Wyzwania informatyki bankowej 2016*, A. Kawiński, A. Sieradz (red.), Gdańsk 2016, s. 181–182.

wzrosła do około 8,2 mln (wzrost o 680 proc.)[21]. Sam zaś udział w tej liczbie właścicieli smartfonów korzystających z bankowości mobilnej wynosił w 2013 r. 12 proc., a w 2015 r. – 43 proc. [22]

Liczba transakcji bezgotówkowych zwiększa się każdego roku średnio o 15 proc. Kwotowo liczba poleceń przelewów wzrosła z 31 bln zł w 2010 r. do 47,5 bln zł w 2015 r. Udział poleceń przelewu w 2015 r. w odniesieniu do wszystkich transakcji bezgotówkowych wynosił 45 proc., natomiast liczba transakcji dokonywanych przy użyciu karty płatniczej w 2015 r. wyniosła 54 proc. (dla porównania 2010 r. – 36 proc.). Transakcje kartowe w latach 2009–2015 osiągnęły średnioroczny wzrost o 24 proc. [23] Liczba wydanych kart płatniczych w Polsce w 2014 r. to ponad 36 mln[24]. W 2013 r. udział kartowych transakcji oszukańczych w wartości wszystkich transakcji kartowych wyniósł 0,005 proc. [25]

Jednocześnie w latach 2005–2015 zwiększyła się liczba sieci akceptacji kart płatniczych (stanowiących tzw. POS[26], w których przypadku jest przyjmowana zapłata kartami płatniczymi) z 55 tys. punktów POS w 2005 r. do 184 tys. w 2015 r. Liczba pojedynczych terminali POS do akceptacji kart płatniczych wzrosła w tym okresie ze 129 tys. do 463 tys. Zwiększył się także odsetek Polaków aktywnie korzystających z konta bankowego przez Internet. W 2009 r. wynosił on 46 proc., podczas gdy w 2016 r. – 69 proc.[27] Liczba rachunków bankowych prowadzonych dla osób prywatnych przez banki, oddziały instytucji kredytowych oraz Spółdzielcze Kasy Oszczędnościowo-Kredytowe wzrosła z 44 mln w 2010 r. do 58 mln w 2015 r.[28]

W pierwszym kwartale 2017 r. w Internecie odnotowano ponad 15 tys. akceptantów[29] oraz 11,5 mln transakcji płatniczych. Wartość tych transakcji wyniosła 1,78 mld zł. Dziennie odnotowywano średnio ponad 128 tys. transakcji[30]. Powyższe dane statystyczne pokazują nieodwracalną tendencję wzrostową rynku płatności bezgotówkowych i elektronicznych transakcji płatniczych[31].

---

[21] Zob. raporty z badań przeprowadzonych przez portal PRNews.pl za IV kwartał 2012 r. i I kwartał 2017 r., https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-i-kw-2017-360755 [dostęp: 23 X 2017]; https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-iv-kw-2013-16158 [dostęp: 23 X 2017].

[22] Zob. A. Marciniak, *Bankowy CERT – nowa broń*…

[23] *Stan obrotu bezgotówkowego w Polsce*, https://www.mr.gov.pl/media/30118/Rozwoj_obrotu_bezgotowkowego_112016.pdf [dostęp: 10 X 2017].

[24] *Porównanie wybranych elementów polskiego systemu płatniczego z systemami innych krajów Unii Europejskiej za 2015 r.*, https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_2014.pdf, s. 18 [dostęp: 10 X 2017].

[25] Tamże, s. 31.

[26] Ang. *points of sale*.

[27] D. Maison, *Postawy Polaków wobec obrotu bezgotówkowego. Raport z badania 2016 i analiza porównawcza z danymi z 2009 i 2013 r.*, https://www.nbp.pl/badania/seminaria/8v2017.pdf [dostęp: 10 X 2017].

[28] *Porównanie wybranych elementów polskiego systemu płatniczego*…, s. 6.

[29] Akceptantem jest np. sklep internetowy.

[30] *Informacja o kartach płatniczych I kwartał 2017 r.*, https://www.nbp.pl/systemplatniczy/karty/q_01_2017.pdf, s. 36 [dostęp: 10 X 2017].

[31] *Stan obrotu bezgotówkowego w Polsce*…

Powyższe dane prowadzą do wniosku, że działalność TPP, zwłaszcza w początkowym okresie, powinna być szczególnie nadzorowana i weryfikowana, z uwagi na potencjalne zagrożenia tzw. ekosystemu finansowego, który jest oparty na wzajemnym zaufaniu jego uczestników i dbaniu o bezpieczeństwo użytkowników końcowych.

Usługi płatnicze oraz ich dostawcy – charakterystyka prawna

Przed dalszą analizą nowych usług płatniczych konieczne jest objaśnienie terminów, które pozwolą na zrozumienie procesu dokonywania płatności elektronicznej i zaprezentowanie jej uczestników. Zgodnie z polską ustawą o usługach płatniczych:

- dostawca – to podmiot świadczący usługi płatnicze. UUP zawiera zamknięty katalog dostawców, którymi mogą być m.in.: banki krajowe, instytucje kredytowe, instytucje pieniądza elektronicznego, instytucje płatnicze, spółdzielcze kasy oszczędnościowo-kredytowe oraz biura usług płatniczych, co oznacza, że inne podmioty nie mogą świadczyć tych usług pod rygorem odpowiedzialności karnej[32];
- akceptant – to odbiorca inny niż konsument, dla którego agent rozliczeniowy świadczy usługę płatniczą (np. sklep stacjonarny lub internetowy). Jest to podmiot przyjmujący zapłatę w formie bezgotówkowej[33];
- usługa płatnicza – to usługa, której istotą jest transfer środków, np. przelew bankowy, czyli środki z rachunku w jednym banku zostają zapisane na rachunku użytkownika w innym banku. Ta usługa zmierza do umożliwienia płatnikowi przekazania środków pieniężnych do odbiorcy. UUP wprowadza zamknięty katalog usług płatniczych;
- użytkownik – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, korzystająca z usług płatniczych jako płatnik lub odbiorca;
- płatnik – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, składająca zlecenie płatnicze prowadzące do obciążenia jej rachunku płatniczego lub dokonania wpłaty środków (podmiot dokonujący płatności);
- odbiorca – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, będąca odbiorcą środków pieniężnych stanowiących przedmiot transakcji płatniczej (podmiot otrzymujący płatność);
- zlecenie płatnicze – to oświadczenie płatnika lub odbiorcy skierowane do dostawcy, zawierające polecenie wykonania transakcji płatniczej[34]. Inicjuje ono transakcję płatniczą. Do jego złożenia może być użyty instrument płatniczy. Zlecenie, o którym mowa, powinno zawierać dane umożliwiające

[32] Art. 150 i nast. UUP.
[33] M. Pacak, *Usługi płatnicze. Komentarz*, Warszawa 2014, s. 181.
[34] Tamże, s. 182.

przeprowadzenie transakcji, takie jak: dane płatnika i odbiorcy, kwota transakcji, unikatowy identyfikator odbiorcy, np. numer rachunku bankowego IBAN (*International Bank Account Number*)[35];

– transakcja płatnicza – to wpłata, transfer lub wypłata środków pieniężnych zainicjowane przez płatnika lub odbiorcę. Transakcja płatnicza może być:
  • zainicjowana przez płatnika, np. polecenie przelewu (tradycyjny przelew bankowy), w którym płatnik przesyła do swojego dostawcy usług płatniczych polecenie dokonania transakcji[36],
  • zainicjowana przez odbiorcę, jeśli płatnik uprzednio udzielił odbiorcy zgody na zainicjowanie transakcji. W tym wypadku to odbiorca inicjuje transakcję płatniczą bez udziału płatnika (np. polecenie zapłaty[37]);
– instrument płatniczy – to urządzenie lub zbiór procedur uzgodniony przez użytkownika i dostawcę, wykorzystywane przez użytkownika do składania zleceń płatniczych. Są to m.in.:
  • zestawy procedur technicznych, np. bankowość elektroniczna[38],
  • przedmioty materialne, np. karty płatnicze – tzw. instrumenty transakcyjne[39];
– karta płatnicza[40] – to karta uprawniająca do wypłaty gotówki (bankomatowa) lub umożliwiająca złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego;
– karta debetowa – to karta płatnicza umożliwiająca wykonywanie transakcji płatniczych, z wyjątkiem transakcji w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu;
– karta kredytowa – to karta płatnicza umożliwiająca wykonywanie transakcji płatniczych w ciężar środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu.

W świetle postanowień UUP w polskim porządku prawnym występują m.in. następujące usługi płatnicze:

– prowadzenie rachunku płatniczego (podmiotem uprawnionym do prowadzenia takiego rachunku są nie tylko banki), dokonywanie wypłat gotówki;
– przyjmowanie wpłat gotówki;
– wykonywanie transakcji płatniczych przy użyciu karty płatniczej lub podobnego instrumentu płatniczego;

---

[35] M. Grabowski, *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2012, s. 28.

[36] Tamże, s. 27.

[37] Art. 63d *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (t.j.: Dz.U. z 2017 r. poz. 1876, ze zm.).

[38] M. Grabowski, *Ustawa o usługach płatniczych*…, s. 19.

[39] K. Korus, *Pojęcie usługi płatniczej w ustawie o usługach płatniczych*, „Monitor Prawa Bankowego" 2012, nr 7–8, s. 37.

[40] Należy odnotować, że zagadnienia dotyczące kart płatniczych są szczegółowo regulowane przez *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę* (Dz. Urz. UE L 123 z 19 maja 2015, s. 1).

- realizacja poleceń zapłaty;
- realizacja polecenia przelewu (tradycyjny przelew bankowy);
- wydawanie instrumentów płatniczych (np. kart płatniczych), tzw. *issuing*;
- *acquiring* – wykonywanie transakcji płatniczych zainicjowanych przez akceptanta lub za jego pośrednictwem instrumentem płatniczym płatnika, szczególnie autoryzacja wykonywanych transakcji, przesyłanie do wydawcy karty płatniczej lub systemów płatności zleceń płatniczych mających na celu przekazanie akceptantowi należnych mu środków[41]; wyjątkiem jest rozrachunek transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami[42]. Są to transakcje, w których np. jest dokonywana płatność kartą płatniczą w sklepie (u tzw. akceptanta karty); akceptant autoryzuje i rozlicza transakcję w ramach usług *acquiringu* świadczonych przez agentów rozliczeniowych, ci zaś przekazują zlecenie płatnicze do banku (czyli do wydawcy karty należącej do osoby dokonującej płatności) i po otrzymaniu z tego banku środków pieniężnych rozliczają się z akceptantem;
- świadczenie przekazu pieniężnego (transfer środków pieniężnych przyjętych od płatnika bez prowadzenia dla niego rachunku płatniczego do odbiorcy, np. przyjmowanie opłat za drobne rachunki w celu ich przekazania usługodawcom lub przyjmowanie wpłat w celu ich udostępnienia odbiorcy);
- świadczenie usługi inicjowania transakcji płatniczej;
- świadczenie usługi dostępu do informacji o rachunku[43].

Obszary infrastruktury płatniczej narażone na ryzyko

Należy wyróżnić następujące elementy[44] w obszarze infrastruktury płatności elektronicznych wrażliwe na zagrożenia:

- systemy płatności[45] podmiotów rozliczających transakcje płatnicze (np. Krajowa Izba Rozliczeniowa SA) oraz infrastruktury systemów kart płatniczych –

[41] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Warszawa 2012, s. 107.

[42] *Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami* (t.j.: Dz.U. z 2018 r. poz. 145, ze zm.).

[43] Świadczenia: usługi inicjowania płatności oraz usługi dostępu do informacji o rachunku zostały dodane do UUP na podstawie dyrektywy PSD II ustawą o zmianie ustawy o usługach płatniczych.

[44] D. Gradzi, *Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa – przegląd regulacji prawnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 38.

[45] SORBNET2, TARGET2-NBP dla płatności wysokokwotowych, ELIXIR, EXPRESS ELIXIR, Krajowy System Rozliczeń, System płatności BlueCash, System Płatności Mobilnych BLIK, System Płatności Kartowych dla płatności detalicznych, http://www.nbp.pl/home.aspx?f=/systemplatniczy/nadzor_syst_platn/systemy_platnosci.html [dostęp: 15 X 2017].

schematów płatniczych (organizacji kartowych)[46],
- informatyczne systemy bankowe[47] oraz infrastruktura podmiotów zaangażowanych w procesowanie transakcji płatniczych (dostawców, w tym agentów rozliczeniowych),
- infrastruktura akceptantów, tj. podmiotów będących odbiorcami płatności elektronicznej[48],
- aplikacje i infrastruktura użytkowników końcowych, zarówno internetowych, jak i mobilnych (w tym urządzenia przenośne i komputery).

Część spośród powyższych elementów stanowi infrastrukturę krytyczną[49] objętą Narodowym Programem Ochrony Infrastruktury Krytycznej[50]. Te elementy należy sklasyfikować jako systemy finansowe, których funkcjonowanie jest możliwe dzięki systemom łączności i systemom teleinformatycznym.

Krytyczna infrastruktura państwa[51] obejmuje m.in. systemy bankowe i finansowe oraz telekomunikacyjne[52]. Składają się na nią rzeczywiste (obiekty, serwery) oraz cybernetyczne systemy, które tylko w przypadku współistnienia umożliwiają świadczenie usług płatniczych. Ze względu na specyfikę usług płatniczych (zdalny dostęp) oraz otwarty charakter systemów bankowych, do których wejście jest możliwe przy wykorzystaniu publicznych sieci, te systemy są narażone na cyberprzestępczość. Cyberprzestępczość jest rozumiana jako (…) *posługiwanie się sieciami telekomunikacyjnymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne*[53]. W *Rządowym Programie Ochrony Cyberprzestrzeni RP na lata 2011–2016*[54] zdefiniowano cyberprzestępstwo jako (…) *czyn zabroniony popełniony w „cyberprzestrzeni"*. Cyberprzestrzeń jest definiowana w powyższym dokumencie jako

[46] Art. 2 ust. 19b) ustawy o usługach płatniczych definiuje organizację kartową jako podmiot określający zasady wydawania i akceptowania kart płatniczych, zawierający umowy z wydawcami (bankami) lub agentami rozliczeniowymi (będzie to np. VISA lub MasterCard).

[47] K. Radziejewski, *Cyberbezpieczeństwo w administracji rządowej w Rzeczpospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 313.

[48] Art. 2 ust. 1b) UUP definiuje akceptanta jako odbiorcę innego niż konsument, na którego rzecz agent rozliczeniowy świadczy usługę płatniczą – w tym ujęciu będzie to np. sklep internetowy akceptujący zarówno płatności kartowe, jak i płatności dokonywane za pośrednictwem tzw. *pay-by-linków*, czyli przelewów natychmiastowych, w ich przypadku kwota transakcji płatniczej jest rozliczna przy udziale pośredniczącego agenta rozliczeniowego.

[49] W rozumieniu art. 3 pkt. 2 ppkt. b), c) i d) *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (t.j.: Dz.U. z 2018 r. poz. 1401).

[50] W rozumieniu art. 5b) ustawy o zarządzaniu kryzysowym.

[51] Por. art. 3 pkt 2 ustawy o zarządzaniu kryzysowym.

[52] Por. tamże oraz R. Kośla, *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac*, http://www.cert.pl/PDF/Kosla_p.pdf [dostęp: 2 X 2017].

[53] M. Staszczyk, *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, http://www.finanseiprawofinansowe.uni.lodz.pl/Publikacje/5/4_Staszczyk.pdf, s. 46 [dostęp: 2 X 2017].

[54] *Rządowy Program Ochrony Cyberprzestrzeni RP*, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf, s. 6 [dostęp: 17 VIII 2018].

(…) *cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązaniami pomiędzy nimi oraz relacjami z użytkownikami*. Statystyki incydentów w cyberprzestrzeni koordynowanych przez CERT[55] pokazują wzrost liczby tych incydentów w stosunku do lat poprzednich. W 2014 r. zarejestrowano ponad 12 tys. zgłoszeń, z czego 7,4 tys. zakwalifikowano jako rzeczywiste incydenty, w 2015 r. zaś zarejestrowano ponad 16 tys. zgłoszeń, a 8,9 tys. z nich zakwalifikowano jako tego typu incydenty[56].

Wystąpienie zagrożenia w powyższych obszarach infrastruktury krytycznej może być sklasyfikowane jako zdarzenie o charakterze terrorystycznym[57] implikujące wprowadzenie stopni alarmowych CRP[58] – w przypadku wystąpienia sytuacji, co do której istnieje podejrzenie, że powstała wskutek przestępstwa o charakterze terrorystycznym lub zagrożenia zaistnienia takiego przestępstwa[59]. Przestępstwem o charakterze terrorystycznym jest między innymi czyn zabroniony, zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej pięć lat, popełniony w celu wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczpospolitej Polskiej lub sama groźba popełnienia takiego czynu dotyczącego szczególnie infrastruktury krytycznej. Możliwe bowiem jest wykorzystanie bankowej infrastruktury krytycznej przez TPP i spowodowanie szkody majątkowej, której wysokości nie da się przewidzieć, zarówno bankom jak i ich klientom.

Third Party Providers – regulacje prawne

Aktami prawnymi regulującymi dostęp podmiotów trzecich do rachunków płatniczych są[60]:

- dyrektywa PSD II;
- *Rozporządzenie delegowane Komisji (UE) 2018/389 z dnia 27 listopada 2017 r. uzupełniające dyrektywę Parlamentu Europejskiego i Rady (UE) 2015/2366 w odniesieniu do regulacyjnych standardów technicznych dotyczących silnego uwierzytelniania klienta i wspólnych i bezpiecznych otwartych standardów*

[55] Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, http://www.cert.gov.pl/cer/o-nas/15,O-nas.html [dostęp: 10 X 2017]. W dniu 28 VIII 2018 r. CERT.GOV.PL przekształcił się w CSIIRT,GOV – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego (podstawa: *Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*, Dz.U. z 2018 r. poz. 1560) – dop. red.

[56] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [dostęp: 3 X 2017].

[57] W rozumieniu art. 2 pkt. 7 *Ustawy z dnia 10 czerwca 2016 o działaniach antyterrorystycznych* (t.j.: Dz.U. z 2018 r. poz. 452, ze zm.).

[58] Zgodnie z art. 15 ust. 2 ustawy o działaniach antyterrorystycznych.

[59] W rozumieniu art. 115 par. 20 *Ustawy z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: Dz.U. z 2017 r. poz. 2204, ze zm.).

[60] W opracowaniu uwzględniono zarówno akty prawne uchwalone, jak i pozostające na etapie prac legislacyjnych.

komunikacji (dalej: RTS)[61], regulujące sposób komunikacji pomiędzy TPP a ASPSP[62]. Zostało ono wydane na podstawie art. 98 ust. 4 zd. 2 dyrektywy PSD II w związku z art. 10–14 rozporządzenia (UE) nr 1093/2010 w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego)[63]. RTS nie wymaga implementacji do krajowego porządku prawnego[64], a państwa członkowskie UE mają zapewnić przymusowo jego stosowanie przez TPP i ASPSP, począwszy od pierwszego dnia po upływie 18 miesięcy od daty wejścia w życie RTS;
– UUP oraz ustawa o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw[65].

Wspólny zakres zastosowania dyrektywy PSD II do TPP

Podmioty trzecie działają obecnie na rynku usług płatniczych i są jego aktywnymi uczestnikami. Realizują wiele transakcji płatniczych o bardzo wysokiej wartości[66] (w 2014 r. z usług tylko jednego dostawcy TPP korzystało 8 mln osób w 11 krajach; od 2005 r. dostawca, o którym mowa, przeprowadził ponad 100 mln transakcji). Z tego powodu dyrektywa PSD II wprowadzała wymóg niedyskryminacji tych podmiotów

[61] Dz. Urz UE L 69 z 13 marca 2018 r., s. 23. Regulacyjne standardy techniczne są wydawane na podstawie art. 290 *Traktatu o funkcjonowaniu UE* – wersja skonsolidowana, Dz. Urz. C326/49 z 26 października 2012, s. 47) i stanowią tzw. drugi poziom w systemie aktów prawa UE. Opracowywane są m.in. przez European Banking Authority (EBA) – Europejski Urząd Nadzoru Bankowego – i jako projekt są przedkładane do Komisji Europejskiej. Komisja Europejska jest uprawniona do przyjmowania tzw. aktu nieustawodawczego o zasięgu ogólnym, który uzupełnia akt ustawodawczy (w niniejszym przykładzie – dyrektywę PSD II). RTS jest zatem wiążący dla krajów członkowskich lub instytucji nadzorowanych (np. banków). Komisja Europejska przedkłada RTS Radzie Unii Europejskiej oraz Parlamentowi Europejskiemu, które mogą dany akt odrzucić. Por. G. Włodarczyk, *Struktura i status aktów prawa Unii Europejskiej ze szczególnym uwzględnieniem RTS, ITS i tzw. Guidelines*, http://mifid.pl/wp-content/uploads/2015/11/Struktura-aktów-Unii-Europejskiej-ze-szczególnym-uwzględnieniem-RTS-ITS-i-tzw.-Guidelines.pdf, s. 4 [dostęp: 4 X 2017]; https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32018R0389&from=EN [dostęp: 15 VIII 2018].

[62] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 [dostęp: 14 X 2017].

[63] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE* (Dz. Urz. UE L 331 z 15 grudnia 2010 r., s. 12).

[64] K. Korus, *Usługi oparte na dostępie*…, s. 82.

[65] Zob. ustawę o zmianie ustawy o usługach płatniczych.

[66] https://www.sofort.com/pol-PL/newsroom/prasowe/SOFORT-Banking-utrzmuje-szybkie-tempo-wzrostu [dostęp: 23 X 2017]; https://retailnet.pl/2015/06/22/13453-dagmara-kruszewska-sofort-3-mln-transakcji-miesiecznie/; http://prnews.pl/wiadomosci/sofort-wyniki-za-1-polowe-2016-50-sklepow-dziennie-chce-rozpoczac-wspolprace-6553123.html [dostęp: 14 X 2017].

do czasu implementacji jej przepisów[67]. Warto odnotować, że Komisja Nadzoru Finansowego w przeszłości wydawała ostrzeżenia przed działalnością TPP[68].

Dyrektywa PSD II wprowadza trzy rodzaje usług TPP określanych też jako usługi XS2A[69]. Są nimi:

- usługa inicjowania płatności (dalej: *Payment Initiation Service* albo – w przypadku podmiotu świadczącego taką usługę – podmiot ten jest zwany dalej: dostawcą usługi PIS) oznacza usługę inicjowania, na wniosek użytkownika, zlecenia płatniczego odnośnie do rachunku płatniczego posiadanego u innego dostawcy usług płatniczych[70]. Dostawca usługi PIS nie może wchodzić w żadnym momencie w posiadanie środków pieniężnych, co odróżnia tę formę płatności od tzw. przelewów natychmiastowych (ang. *pay-by-link*), w których „pośrednik" (agent rozliczeniowy) wchodzi w posiadanie tych środków;
- usługa dostępu do informacji o rachunku (dalej: *Account Information Service* albo – w przypadku podmiotu świadczącego taką usługę – podmiot ten jest zwany dalej: dostawcą usługi – AIS) oznacza usługę online, która polega na dostarczaniu kompletnych informacji na temat rachunku płatniczego posiadanego przez użytkownika usług płatniczych[71];
- potwierdzenie dostępności środków pieniężnych na rachunku płatniczym (*Confirmation of the Availability of Funds* albo – w przypadku podmiotu świadczącego taką usługę – podmiot ten jest zwany dalej: dostawcą usługi CAF), które nie stanowi osobnej usługi płatniczej i nie jest wymienione w załączniku nr 1 do dyrektywy PSD II.

Dostawca prowadzący rachunek płatniczy jest zobowiązany do zezwalania dostawcom usług PIS i AIS na poleganie na procedurach uwierzytelniania użytkowników zapewnianych przez ASPSP[72]. Powyższa regulacja prowadzi do wniosku, że TPP ma prawo do zastosowania własnego uwierzytelnienia użytkownika, niezależnie od uwierzytelnienia ASPSP, ale może także wykorzystać wyłącznie uwierzytelnienie użytkownika stosowane przez ASPSP.

Wszelkie prawne obowiązki nałożone przez dyrektywę PSD II na ASPSP mają zastosowanie wyłącznie wtedy, gdy ASPSP prowadzą dla użytkownika rachunek

---

[67] Motyw 29 i 33 do dyrektywy PSD II.

[68] Zob. *Ostrzeżenie KNF przed dopuszczeniem pośredników do rachunku bankowego w płatnościach internetowych z dnia 18.11.2013 r.* oraz *Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego z dnia 14.07.2014 r.*, w: *Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe*, wydana przez KNF w listopadzie 2015 r., s. 2, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/Rekomendacja_dot_bezpieczenstwa_transakcji_platniczych [dostęp: 25 X 2017].

[69] Tzw. *access to account* (dostęp do rachunku), zob. M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 32.

[70] Art. 4 pkt 15 dyrektywy PSD II.

[71] Art. 4 pkt 16 dyrektywy PSD II.

[72] Art. 97 ust. 5 dyrektywt PSD II.

płatniczy. Rachunek bankowy jest rachunkiem płatniczym wówczas, gdy służy do wykonywania transakcji płatniczych[73]. Dostęp do informacji innych niż informacje o rachunku płatniczym (np. kredytach, lokatach, depozytach, inwestycjach) nie podlega regulacji dyrektywy PSD II[74].

Zakres stosowania dyrektywy PSD II dotyczy wyłącznie usług płatniczych świadczonych w Unii Europejskiej. Mankamentem takiego ujęcia jest to, że w przypadku, gdy działalność usługodawcy nie dotyczy krajów UE, to usługa TPP może być świadczona bez żadnych ograniczeń wynikających z dyrektywy PSD II, ale też bez możliwości domagania się przez TPP od ASPSP określonego zachowania, do którego ten podmiot jest zobowiązany na mocy przepisów wymienionej dyrektywy[75].

Obowiązki nałożone na ASPSP związane z dostępem do rachunków płatniczych przez TPP dotyczą wyłącznie sytuacji, gdy te rachunki są prowadzone przez ASPSP online. Dyrektywa PSD II nie definiuje, co należy rozumieć przez dostępność rachunku płatniczego online. Trafnie przyjmuje się, że ten termin należy rozumieć szeroko i obejmować nim przypadki każdej formy komunikacji za pośrednictwem systemów teleinformatycznych stron w czasie rzeczywistym[76].

Gwarancją możliwości świadczenia przez TPP usług, które są konkurencyjne i stoją w opozycji do interesów tzw. bankowych dostawców usług płatniczych, jest art. 36 dyrektywy PSD II. Przewiduje się w nim, że każda instytucja płatnicza powinna mieć dostęp do usług świadczonych w ramach rachunków płatniczych. Te usługi powinny być świadczone przez ASPSP na podstawie zasad obiektywnych, niedyskryminujących i proporcjonalnych. Każda odmowa świadczenia takich usług dla TPP powinna być należycie umotywowana i przedstawiona organowi nadzoru – Komisji Nadzoru Finansowego.

Dostawcy usług płatniczych będący TPP nie są zobligowani do nawiązywania jakiejkolwiek relacji umownej z ASPSP. Wymóg współpracy ASPSP z TPP wynika bezpośrednio z dyrektywy PSD II[77]. TPP w przypadku świadczenia usług inicjowania płatności nie wchodzi na żadnym etapie transakcji płatniczej w posiadanie środków pieniężnych. W przypadku, gdy TPP zamierza to robić, jest zobligowany do wystąpienia do Komisji Nadzoru Finansowego i uzyskania pełnego zezwolenia na świadczenie usług płatniczych.

---

[73] Por. K. Korus, *Pojęcie usługi płatniczej*…, s. 33.

[74] K. Korus trafnie wskazuje, że rachunki powiązane z kredytami mogą być rachunkami płatniczymi. Zob. K Korus, *Usługi oparte na dostępie*…, s. 86; także: *Rekomendacja Rady Prawa Bankowego i Zespołu ds. Regulacji Płatniczych Związku Banków Polskich w sprawie wybranych problemów interpretacyjnych ustawy o usługach płatniczych*, http://zbp.pl/public/repozytorium/dla_bankow/prawo/rada_prawa_bankowego/dzialalnosc/rekomendacja_grupa_robocza.doc [dostęp: 25 X 2017]; M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 33.

[75] K. Korus, *Usługi oparte na dostępie*…, s. 87.

[76] Tamże, s. 87–88.

[77] Por. motyw 30 do preambuły oraz art. 66 ust. 5 dyrektywy PSD II.

Usługa inicjowania płatności – uwagi ogólne

Usługa PIS ma w założeniu przyspieszać wykonanie umowy przez akceptanta (np. wysyłkę towaru przez sklep internetowy), daje mu bowiem gwarancję uzyskania zapłaty za towar lub usługi. Za pośrednictwem PIS zostaje zainicjowana określona płatność elektroniczna na rachunek płatniczy akceptanta, tak jakby użytkownik robił to osobiście. Zgoda na wykonanie transakcji płatniczej udzielona przez płatnika za pośrednictwem PIS jest równoznaczna ze zgodą na realizację takiej transakcji wyrażoną przez płatnika bezpośrednio dostawcy[78].

Modelowy schemat transakcji płatniczej przy udziale PIS polega na tym, że zlecenie płatnicze płatnika (np. osoby dokonującej zakupu towaru w środowisku internetowym) jest przekazywane przy udziale dostawcy usługi PIS do ASPSP za pośrednictwem bankowości elektronicznej, udostępnianej użytkownikowi przez ASPSP. Odbiorcą środków pieniężnych jest przeważnie sprzedawca towaru, którego łączy z dostawcą usługi PIS umowa o obsługę takich płatności[79]. Usługa PIS umożliwia dokonanie płatności w środowisku internetowym bez potrzeby posiadania innego instrumentu płatniczego, np. karty płatniczej[80].

Indywidualne dane uwierzytelniające służące do bezpiecznego uwierzytelniania użytkownika (potwierdzania jego tożsamości przez dostawcę), którymi posługuje się użytkownik lub dostawca usługi PIS, są wydawane przez dostawcę prowadzącego rachunek płatniczy[81].

Usługa PIS została unormowana w art. 4 pkt 15 i art. 66 dyrektywy PSD II. Polega ona na złożeniu przez dostawcę usługi PIS – na polecenie i w imieniu użytkownika – zlecenia płatniczego do ASPSP w celu przekazania środków pieniężnych na rachunek odbiorcy wskazany przez użytkownika[82]. Podstawową usługą płatniczą, która jest przedmiotem PIS, jest polecenie przelewu[83]. Głównymi dostawcami tego typu usług są takie marki, jak Sofort[84] oraz Trustly[85].

Usługa inicjowania płatności – zagadnienia regulacyjne

Dostawcą usługi PIS może być wyłącznie dostawca usług płatniczych mający taki status na podstawie przepisów ustawy o usługach płatniczych. W przypadku dostawcy mającego status instytucji płatniczej jest wymagane rozszerzenie posiadanego zezwolenia o świadczenie usług płatniczych w zakresie PIS i AIS[86]. Dostawca usługi PIS

[78] Art. 64 ust. 2 dyrektywy PSD II.

[79] K. Korus, *Usługi oparte na dostępie*…, s. 84.

[80] Motywy 28 i 29 do preambuły dyrektywy PSD II.

[81] Motywy 30 do preambuły dyrektywy PSD II.

[82] K. Korus, *Usługi oparte na dostępie*…, s. 84.

[83] W rozumieniu art. 3 ust. 4 UUP.

[84] https://www.sofort.com/pol-PL/kupujacy/sb/zakupy-online-z-sofort-banking/.

[85] https://trustly.com/pl/.

[86] Instytucje kredytowe w rozumieniu art. 4 ust. 1 pkt 1 *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów*

musi posiadać kapitał założycielski w wysokości 50 tys. euro[87], który powinien się składać co najmniej z jednego z następujących elementów:

- instrumentu kapitałowego,
- agio emisyjnego[88] związanego z instrumentami kapitałowymi,
- zysków zatrzymanych,
- skumulowanych innych całkowitych dochodów,
- kapitału rezerwowego[89].

Powyższe ma stanowić element gwarancyjny w przypadku wystąpienia niepożądanych zdarzeń związanych z działalnością TPP.

Dostawca usług płatniczych świadczący usługi PIS powinien mieć ubezpieczenie od odpowiedzialności cywilnej lub inną porównywalną gwarancję w celu możliwości pokrycia przez niego zobowiązań[90]. Ta regulacja i odpowiedni poziom zabezpieczenia mają szczególne znaczenie dla stabilności i bezpieczeństwa banku (lub innego podmiotu prowadzącego rachunek płatniczy), gdyż w przypadku wystąpienia nieautoryzowanej transakcji płatniczej inicjowanej przez dostawcę usługi PIS, to ASPSP (np. bank) zwraca bezzwłocznie, a w każdym wypadku nie później niż do końca następnego dnia roboczego, płatnikowi (klientowi) kwotę nieautoryzowanej transakcji[91]. W dalszej kolejności dostawca usługi PIS, w przypadku gdy jest odpowiedzialny za nieautoryzowaną transakcję, rekompensuje ASPSP straty poniesione lub sumy zapłacone w wyniku zwrotu na rzecz płatnika, łącznie z kwotą nieautoryzowanej transakcji płatniczej[92].

Artykuł 66 dyrektywy PSD II wprowadza do europejskiego porządku prawnego założenia i ramy regulujące usługę PIS. Fundamentalnymi sprawami są poniższe zagadnienia dotyczące wymogów regulacyjnych nałożonych na dostawcę usługi PIS oraz na ASPSP.

Obowiązki dostawcy usługi PIS[93]:

- dyrektywa PSD II przewiduje, że korzystanie z PIS jest prawem płatnika (użytkownika), a ASPSP musi respektować to uprawnienie;
- dostawca usługi PIS musi uzyskać zgodę płatnika na zainicjowanie zlecenia płatniczego;

---

ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz. Urz. UE L 176 z 27 czerwca 2013 r., s. 1) nie potrzebują takiego zezwolenia, zgodnie z art. 11 ust. 1 dyrektywy PSD II.

[87] Art. 7 pkt b) dyrektywy PSD II.

[88] Jest to różnica pomiędzy wartością nominalną określonego instrumentu kapitałowego, np. akcji, a jego ceną emisyjną.

[89] Art. 7 PSD II w zw. z art. 26 ust. 1 lit. a)-e) rozporządzenia PE i Rady (UE) nr 575/2013 w sprawie wymogów ostrożnościowych.

[90] Art. 5 ust. 2 dyrektywy PSD II.

[91] Art. 73 ust. 2 dyrektywy PSD II.

[92] Art. 73 ust. 2 zd. 2 dyrektywy PSD II.

[93] Art. 66 ust. 1 i 3 dyrektywy PSD II.

- prawo do korzystania z PIS przysługuje wyłącznie w przypadku, gdy ASPSP prowadzi dla użytkownika rachunek płatniczy dostępny online;
- dostawca usługi PIS przy świadczeniu usługi inicjowania płatności nie wchodzi w żadnym momencie w posiadanie środków pieniężnych płatnika;
- dostawca usługi PIS nie może zmieniać kwoty zlecenia płatniczego;
- dostawca usługi PIS nie może zmieniać odbiorcy zlecenia płatniczego;
- dostawca usługi PIS nie może zmieniać żadnych innych cech transakcji płatniczej;
- dostawca usługi PIS musi zagwarantować, aby indywidualne dane uwierzytelniające użytkownika nie były dostępne dla innych (niż użytkownik i wydawca tych danych) stron;
- dostawca usługi PIS musi zagwarantować, aby indywidualne dane uwierzytelniające użytkownika były przekazywane za pośrednictwem bezpiecznych i wydajnych kanałów;
- dostawca usługi PIS musi zagwarantować, aby wszelkie informacje o użytkowniku usług płatniczych były dostarczane wyłącznie odbiorcy i tylko za wyraźną zgodną użytkownika usług płatniczych;
- dostawca usługi PIS jest zobligowany – każdorazowo, gdy jest inicjowana płatność – do identyfikowania siebie wobec dostawcy usług płatniczych prowadzącego rachunek płatniczy płatnika (ASPSP);
- dostawca usługi PIS jest zobligowany – przy inicjowaniu płatności – do bezpiecznego porozumiewania się z ASPSP, płatnikiem i odbiorcą, zgodnie z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II[94];
- dostawca usługi PIS nie może przechowywać szczególnie chronionych danych dotyczących płatności;
- dostawca usługi PIS nie może żądać od użytkownika usług płatniczych innych danych niż dane niezbędne do wykonania usługi inicjacji płatności;
- dostawca usługi PIS nie może używać, uzyskiwać ani przechowywać żadnych danych do celów innych niż do wykonania usługi inicjowania płatności wyraźnie zleconej przez płatnika.

[94] Europejski Urząd Nadzoru Bankowego (EUNB) we współpracy z Europejskim Bankiem Centralnym (EBC) i po przeprowadzeniu konsultacji z wszystkimi stosownymi podmiotami zainteresowanymi, w tym podmiotami na rynku usług płatniczych, opracowuje projekt regulacyjnych standardów technicznych skierowanych do dostawców usług płatniczych, określających:

1) wymogi dotyczące silnego uwierzytelniania klienta,
2) wyłączenia ze stosowania silnego uwierzytelniania klienta,
3) wymogi, jakie muszą spełniać środki bezpieczeństwa, w celu ochrony poufności i integralności indywidualnych danych uwierzytelniających użytkowników usług płatniczych,
4) wymogi w zakresie wspólnych i bezpiecznych otwartych standardów komunikacji do celów identyfikowania, uwierzytelniania, powiadamiania i informowania, a także na potrzeby wdrożenia środków bezpieczeństwa, między dostawcami usług ASPSP, PIS, AIS, płatnikami, odbiorcami i innymi dostawcami usług płatniczych.

Obowiązki ASPSP[95]:

- ASPSP jest zobowiązany do porozumiewania się z dostawcą usługi PIS w sposób bezpieczny, zgodnie z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II;
- ASPSP bezzwłocznie po otrzymaniu zlecenia płatniczego od dostawcy usługi PIS jest zobowiązany do przekazania lub udostępniania mu wszystkich informacji o zainicjowaniu transakcji płatniczej oraz wszystkich informacji dostępnych dostawcy ASPSP w odniesieniu do wykonania transakcji płatniczej;
- ASPSP musi traktować zlecenia płatnicze przekazane za pośrednictwem dostawcy usługi PIS w sposób niedyskryminujący w stosunku do zleceń płatniczych przekazanych bezpośrednio ASPSP przez samego płatnika, szczególnie pod względem czasu wykonania, priorytetowego charakteru, opłat, co jednak nie dotyczy przypadku, gdy postępowanie dyskryminujące jest uzasadnione przyczynami obiektywnymi;
- świadczenie usług PIS nie może być uzależnione od istnienia stosunku umownego między dostawcą usługi PIS a ASPSP.

Usługa dostępu do informacji o rachunku – uwagi ogólne

Usługa AIS jest regulowana przez art. 4 pkt 16 oraz art. 67 dyrektywy PSD II. Polega ona na dostępie dostawcy tego typu usługi do rachunku płatniczego (bankowego) prowadzonego dla użytkownika. Dostawca usługi AIS dokonuje logowania do systemu bankowości elektronicznej użytkownika za jego zgodą, a następnie pobiera i przekazuje mu zagregowane informacje w komunikacji online. Uzyskuje w ten sposób dostęp do danych „na temat rachunku" oraz danych dotyczących wszystkich transakcji płatniczych na tym rachunku[96].

Usługa dostępu do informacji o rachunku – zagadnienia regulacyjne

Artykuł 67 dyrektywy PSD II wprowadza do europejskiego porządku prawnego ramy regulacyjne AIS. Świadczenie usług AIS nie wymaga uzyskania zezwolenia krajowego organu nadzoru (KNF), a wyłącznie rejestracji w tym organie[97]. Dostawca usługi AIS powinien posiadać ubezpieczenie od odpowiedzialności lub inną porównywalną gwarancję w celu możliwości pokrycia przez niego zobowiązań[98].

Obowiązki dostawcy usługi AIS:

- dyrektywa PSD II przewiduje, że korzystanie z AIS jest prawem płatnika (użytkownika), ASPSP zaś musi respektować to uprawnienie;

[95] Art. 66 ust. 4 dyrektywy PSD II.
[96] K. Korus, *Usługi oparte na dostępie*…, s. 85; także: art. 67 ust. 2 lit. d) dyrektywy PSD II.
[97] Art. 33 i 5 ust. 3 dyrektywy PSD II.
[98] Art. 5 ust. 3 dyrektywy PSD II.

- dostawca usługi AIS musi uzyskać zgodę użytkownika na świadczenie swoich usług dla niego;
- prawo do korzystania z usług AIS przysługuje użytkownikowi wyłącznie w przypadku, gdy ASPSP prowadzi dla użytkownika rachunek płatniczy dostępny online;
- dostawca usługi AIS musi zapewnić, aby indywidualne dane uwierzytelniające użytkownika nie były dostępne dla innych stron, z wyjątkiem użytkownika i wydawcy indywidualnych danych uwierzytelniających użytkownika;
- dostawca usługi AIS musi zapewnić, aby indywidualne dane uwierzytelniające użytkownika były przekazywane przez dostawcę świadczącego usługi AIS za pośrednictwem bezpiecznych i wydajnych kanałów;
- dostawca usługi AIS musi w przypadku każdej sesji komunikacyjnej identyfikować siebie wobec ASPSP;
- dostawca usługi AIS musi porozumiewać się z ASPSP i użytkownikiem w sposób bezpieczny – zgodnie z art. 98 ust. 1 lit. d) dyrektywy PSD II;
- dostawca usługi AIS może uzyskiwać dostęp wyłącznie do informacji dotyczących wyznaczonych rachunków płatniczych i związanych z nimi transakcji płatniczych;
- dostawca usługi AIS nie może żądać szczególnie chronionych danych dotyczących płatności związanych z rachunkami płatniczymi;
- dostawca usługi AIS nie może używać, uzyskiwać ani przechowywać żadnych danych do celów innych niż do wykonania usługi dostępu do informacji o rachunku, wyraźnie zleconej przez użytkownika usług płatniczych zgodnie z przepisami o ochronie danych.

Obowiązki ASPSP:

- ASPSP musi porozumiewać się z dostawcą usługi AIS w sposób bezpieczny i zgodny z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II;
- ASPSP musi traktować wnioski o udostępnienie danych przekazane za pośrednictwem dostawcy usługi AIS w sposób niedyskryminujący, chyba że postępowanie dyskryminujące jest uzasadnione przyczynami obiektywnymi;
- świadczenie usług AIS nie może być uzależnione od istnienia stosunku umownego między dostawcą usługi AIS a ASPSP;
- zgodnie z motywem 28 do preambuły dyrektywy PSD II ASPSP udostępnia wszystkie informacje dotyczące rachunku płatniczego, przede wszystkim: numer IBAN lub NRB, wysokość salda, historię transakcji (kwotę, tytuł, datę wykonania, dane drugiej strony[99]).

[99] M. Mostowik, *Prawna ochrona informacji o rachunku*…, s. 34.

Głównymi dostawcami tych usług są takie podmioty, jak: Kontomierz[100], AFAS[101], tink[102], Money Dashboard[103] i Quontis[104].

Potwierdzenie dostępności środków pieniężnych na rachunku płatniczym – uwagi ogólne

Dyrektywa PSD II wprowadza oprócz powyższych usług TPP także proces potwierdzania dostępności środków pieniężnych na rachunku płatniczym płatnika. Ten proces nie jest jednak ujęty w regulacjach jako odrębna usługa płatnicza. Umożliwia wydawcy instrumentu płatniczego opartego na karcie płatniczej[105] – uprzednio wskazanemu ASPSP przez użytkownika, którego rachunek płatniczy ASPSP dostarcza – domaganie się od ASPSP w czasie rzeczywistym, przy użyciu komunikacji online, informacji, czy na rachunku użytkownika znajduje się określona kwota. Proces potwierdzania dostępności środków pieniężnych reguluje zatem obowiązki ASPSP wobec wydawcy instrumentu płatniczego opartego na karcie płatniczej. Obowiązkiem użytkownika jest wcześniejsze poinformowanie ASPSP o zamiarze korzystania z CAF[106].

Potwierdzenie dostępności środków pieniężnych na rachunku płatniczym – zagadnienia regulacyjne

Obowiązkiem ASPSP jest potwierdzenie – na wniosek dostawcy wydającego instrumenty płatnicze oparte na karcie – dostępności na rachunku płatniczym płatnika kwoty niezbędnej do wykonania transakcji płatniczej realizowanej na podstawie karty[107] (usługa CAF).

Wymogi prawne do stosowalności usługi CAF[108]:

- rachunek płatniczy płatnika musi być dostępny za pośrednictwem Internetu w momencie występowania z wnioskiem o potwierdzenie dostępności środków pieniężnych;
- płatnik musi udzielić ASPSP zgody na odpowiadanie na wnioski określonego dostawcy usług płatniczych w celu potwierdzenia, że kwota odpowiadająca

[100] http://kontomierz.pl.
[101] https://www.afas.nl.
[102] https://www.tinkapp.com/en/.
[103] https://www.moneydashboard.com.
[104] http://www.qontis.ch.
[105] Instrument oparty na karcie płatniczej to dowolny instrument płatniczy (m.in. karta, telefon komórkowy, komputer) umożliwiający zainicjowanie transakcji płatniczej z wykorzystaniem infrastruktury systemu kart płatniczych, por. art. 2 pkt 20 rozporządzenia PE i Rady (UE) 2015/751 w sprawie opłat interchange w odniesieniu do transakcji płatniczych.
[106] K. Korus, *Usługi oparte na dostępie*…, s. 85.
[107] Art. 65 ust. 1 dyrektywy PSD II.
[108] Tamże.

określonej transakcji płatniczej realizowanej na podstawie karty jest dostępna na rachunku płatniczym płatnika;
– zgoda dla ASPSP od użytkownika dotyczącą odpowiadania na wnioski musi być udzielona przed wystąpieniem z pierwszym wnioskiem o potwierdzenie.

Wymogi prawne nałożone na dostawcę występującego z wnioskiem:

– płatnik musi udzielić dostawcy wyraźnej zgody na występowanie z wnioskiem o potwierdzenie dostępności środków pieniężnych;
– płatnik musi zainicjować transakcję płatniczą realizowaną przy użyciu instrumentu płatniczego opartego na karcie;
– dostawca usługi CAF musi uwierzytelnić samego siebie wobec dostawcy ASPSP;
– dostawca usługi CAF musi porozumiewać się z ASPSP w sposób bezpieczny, zgodnie z postanowieniami art. 98 ust. 1 lit. d) dyrektywy PSD II.

Potwierdzenie dostępności środków pieniężnych na rachunku płatniczym przez ASPSP ma polegać na udzieleniu odpowiedzi „tak" lub „nie". Stan salda nie jest podawany. Dostawca usługi CAF nie może przechowywać ani wykorzystywać odpowiedzi uzyskanej od ASPSP do celów innych niż wykonanie transakcji płatniczej realizowanej na podstawie karty[109]. Potwierdzenie dostępności środków nie daje możliwości blokowania przez ASPSP określonej kwoty na rachunku płatnika do czasu rozliczenia płatności[110].

W celu wykonywania usługi CAF niezbędne jest zezwolenie na wydawanie instrumentów płatniczych opartych na karcie.

Działalność TPP a cyberbezpieczeństwo

Zapobieganiem i przeciwdziałaniem cyberprzestępczości w zakresie infrastruktury płatniczej powinny zająć się oprócz uprawnionych podmiotów publicznych także branżowe organizacje finansowe[111] (we współpracy z właściwymi służbami publicznymi) jako podmioty bezpośrednio narażone na zagrożenie cyberprzestępczością i zainteresowane poprawą cyberbezpieczeństwa. Przykładem takiej organizacji jest FinansCERT z Norwegii[112]. Ta organizacja jest CERT-em[113] w norweskim sektorze finansowym: bankowym i ubezpieczeniowym. Do jej głównych zadań należą:

– śledzenie zagrożeń zewnętrznych,
– wsparcie w zwalczaniu ataków i ograniczaniu strat,
– koordynacja współpracy z instytucjami publicznymi i służbami porządkowymi (Interpol, Policja).

[109] Art. 65 ust. 3 dyrektywy PSD II.
[110] Art. 65 ust. 4 dyrektywy PSD II.
[111] Zob. A. Marciniak, *Bankowy CERT – nowa broń*…
[112] FinansCERT jako organizacja została powołana 23 IV 2013 r. przy norweskiej branżowej organizacji zrzeszającej instytucje finansowe, http://www.finanscert.no [dostęp: 15 X 2017].
[113] Computer Emergency Response Team (z ang. zespół reagowania na incydenty komputerowe).

Innymi organizacjami branżowymi, których przedmiotem działalności jest zwalczanie zagrożeń w zakresie bezpieczeństwa informacji, są m.in.: National Cyber-Forensics & Training Alliance (NCFTA), Financial Services Information Sharing and Analysis Center (FS-ISAC), Soltra czy działająca w Unii Europejskiej European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC)[114] tj. organizacje pozarządowe o globalnym zasięgu mające siedziby w Stanach Zjednoczonych.

Bankowe Centrum Cyberbezpieczeństwa

We wrześniu 2015 r. z inicjatywy Rady Bankowości Elektronicznej działającej przy Związku Banków Polskich (ZBP) została wydana rekomendacja dotycząca bezpieczeństwa oraz zapobiegania brakowi dostępu do bankowości elektronicznej. Rekomendacja zawiera zalecenie, aby banki zrzeszone w ZBP nawiązały współpracę w zakresie:

- przeciwdziałania atakom na platformy bankowości elektronicznej banków oraz ich klientów,
- reagowania na ataki.

Rezultatem tej rekomendacji było powołanie Bankowego Centrum Cyberbezpieczeństwa (BCC)[115]. BCC stanowi obecnie jedną z najważniejszych platform Narodowego Centrum Cyberbezpieczeństwa (NC Cyber)[116]. Współpracuje z Policją oraz Krajową Izbą Rozliczeniową SA, operatorami telekomunikacyjnymi, operatorami szybkich płatności i giełdami bitcoin[117]. W przypadku zagrożenia cyberbezpieczeństwa BCC staje się sztabem kryzysowym zarządzającym sytuacją kryzysową w sektorze bankowym. Aktualnie obszarami zainteresowania BCC są przede wszystkim:

- monitoring sektora bankowego w zakresie cyberbezpieczeństwa i reagowania na zagrożenia;
- zarządzanie komunikacją zwłaszcza przez:
  - opracowanie spójnej polityki informacyjnej w stosunku do klientów i mediów w sektorze bankowym, której głównym założeniem jest niezwłoczne informowanie o wszelkich zagrożeniach cyberbezpieczeństwa lub awariach systemów bankowości elektronicznej,

[114] A. Marciniak, *Bankowy CERT – nowa broń*…

[115] Por. informację o otwarciu BCC udostępnioną na stronie internetowej ZBP, https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa [dostęp: 25 X 2017]; zob. odpowiedź A. Stróżyńskiej na interpelację, BM-WOP.072.69.2017, Warszawa 22 VI 2017 r., http://www.sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=75AD31FB, [dostęp: 25 X 2017]; A. Marciniak, *Bankowy CERT – nowa broń*…

[116] NCC zostało powołane 4 VII 2016 r. i działa w strukturze NASK (Naukowej i Akademickiej Sieci Komputerowej), która jest państwowym instytutem badawczym w rozumieniu *Ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych* (t.j.: Dz.U. z 2018 r. poz. 736) oraz par. 3 ust. 2 pkt 1 ppkt d) *Rozporządzenia Rady Ministrów z dnia 7 czerwca 2017 w sprawie nadania Naukowej i Akademickiej Sieci Komputerowej statusu państwowego instytut badawczego* (Dz.U. z 2017 r. poz. 1193). Do zadań NASK należy zapewnianie cyberbezpieczeństwa podmiotom publicznym przez rozwój Narodowego Centrum Cyberbezpieczeństwa.

[117] A. Marciniak, *Bankowy CERT – nowa broń*...

- opracowanie procedur komunikacji pomiędzy uczestnikami,
- opracowanie procedur współpracy i kanałów komunikacji z organami ścigania, innymi CERT-ami, producentami oprogramowania oraz opracowanie systemów zabezpieczeń;

– definiowanie i monitorowanie wdrażania działań prewencyjnych w sektorze[118].

Z łatwością można sobie wyobrazić sytuację, w której TPP w początkowej fazie działalności – budując swoją reputację na rynku oraz zaufanie użytkowników i po jakimś czasie dysponując już danymi, które umożliwiają zalogowania się do rachunków bankowych klientów – doprowadza na masową skalę do wielu nieautoryzowanych transakcji. Za te transakcje wobec klientów rzekomo korzystających z usługi PIS w pierwszej kolejności prawnie i finansowo odpowiada bank. Bank występuje do TPP z roszczeniem o zwrot należności będących przedmiotem nieautoryzowanych transakcji. To roszczenie może być zaspokojone tylko pod warunkiem, że TPP jest wypłacalny. Można podać także inny przykład, gdy dostawca usługi AIS posiadający bazę danych wrażliwych uprawniających do zalogowania się do kont bankowych, doprowadza umyślnie do utraty takiej bazy. Koszty, nie tylko finansowe (powodowane dużą liczbę transakcji płatniczych o ogromnej wartości), lecz także społeczne (powodowane utratą zaufania klientów do systemu płatniczego) mogą być trudne do oszacowania. Nawet w przypadku gdy wyrządzona szkoda zostanie pokryta w pełni, istotnym kosztem będzie utrata zaufania do sektora finansowego przez klientów.

Biorąc powyższe pod uwagę, należy stwierdzić, że działalność TPP może powodować także problemy prawne na płaszczyźnie:

– tajemnicy bankowej[119],
– tajemnicy płatniczej[120],
– prawa do ochrony danych osobowych,
– prawa do prywatności, zarówno dla posiadacza rachunku, jak i osób trzecich, których dane osobowe widnieją w aplikacji bankowości elektronicznej jako płatnicy lub odbiorcy[121].

Podsumowanie

Usługi TPP są i nadal będą wykonywane w segmencie płatności elektronicznych, a ich jeszcze większy wzrost nastąpi wtedy, gdy zostaną na stałe połączone z dostawcami portali społecznościowych i usług masowych, takich tak: Facebook, Apple, Amazon, Netflix, Google[122], Uber, Spotify.

[118] Tamże, s. 193.

[119] Zob. art. 104 ust. 1 *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (t.j.: Dz.U. z 2017 r. poz. 1876, ze zm.).

[120] Zob. art. 11 ust. 1 UUP.

[121] W zakresie wskazanych rodzajów ryzyka por. M. Mostowik, *Prawna ochrona informacji o rachunku…*, s. 35–42.

[122] Określanych w skrócie FAANG (Facebook, Apple, Amazon, Netflix, Google).

Zarówno dostawcy świadczący usługi inicjowania płatności (PIS) oraz usługę dostępu do rachunku płatniczego (AIS) po jednej stronie, jak i dostawcy tradycyjnych usług płatniczych po drugiej powinni przestrzegać wymogów dotyczących ochrony danych i bezpieczeństwa wynikających z dyrektywy PSD II oraz RTS. Regulacyjne standardy techniczne powinny zapewnić interoperacyjność[123] różnych rozwiązań komunikacyjnych z technologicznego punktu widzenia. Ponadto dzięki regulacyjnym standardom technicznym dostawca prowadzący rachunek płatniczy (ASPSP) ma możliwość zorientowania się, czy przy przeprowadzaniu danej transakcji płatniczej kontaktuje się z nim dostawca PIS, a nie bezpośrednio jego klient[124].

Należy zwrócić uwagę, że regulacje w dyrektywie PSD II w zakresie działalności TPP są bardzo ogólne. Wszystkie istotne sprawy techniczne, które mają zapewnić bezpieczeństwo tych usług oraz podmiotów z nich korzystających i je dostarczających, zostały rozstrzygnięte przez RTS. Z uwagi na to, że usługi TPP są świadczone między innymi w środowisku internetowym, nieprawidłowości w ich funkcjonowaniu mogą zagrażać cyberbezpieczeństwu płatniczej infrastruktury krytycznej. Związek Banków Polskich stale monitoruje sytuację rzeczywistą i prawną. Zwraca przy tym uwagę na zagrożenia związane z działalnością TPP[125].

Zapisy prawne zawarte w dyrektywnie PSD II dotyczące TPP są przykładem skutecznego lobbingu regulacyjnego podmiotów świadczących od lat usługi omawiane w artykule. Podmioty będące TPP z uwagi na potencjalne zagrożenia w skali mikro (utrata środków finansowych przez użytkownika) i makro (zagrożenie funkcjonowania płatniczej infrastruktury krytycznej) powinny spotkać się z ostrożnym podejściem do tych podmiotów ze strony regulatora – Komisji Nadzoru Finansowego oraz użytkowników w początkowej fazie ich funkcjonowania.

Bibliografia:

Chinowski B., *Elektroniczne metody płatności. Istota, rozwój, prognozy*, https://www.knf.gov.pl/knf/pl/komponenty/img/Elektroniczne%20metody%20platnosci.pdf [dostęp: 20 X 2017].

Grabowski M., *Instrumenty płatnicze w prawie polskim*, Warszawa 2013, CeDeWu.

Grabowski M., *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2012, C.H. Beck.

Gradzi D., *Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa – przegląd regulacji prawnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 38–54.

[123] Cecha produktu lub systemu, którego interfejsy umożliwiają współpracę z innymi produktami lub systemami.

[124] Motyw 93 do preambuły dyrektywy PSD II.

[125] Por. *Notatkę dotyczącą usług opartych o dostęp stron trzecich (PISP, AISP) do rachunków płatniczych w świetle PSD2 Rady Bankowości Elektronicznej Związku Banków Polskich*, https://zbp.pl/public/repozytorium/wydarzenia/images/luty_2017/Polish_Bank_Association_Notatka_PL_Third_Party_Services_PSD2_January_2017_fin.pdf [dostęp: 10 X 2017].

Kaszubski R., Obzejta Ł., *Karty płatnicze w Polsce*, Warszawa 2012, Wolters Kluwer.

Korus K., *Pojęcie usługi płatniczej w ustawie o usługach płatniczych*, „Monitor Prawa Bankowego" 2012, nr 7–8, s. 43–58.

Korus K., *Usługi oparte na dostępie do rachunku w dyrektywie PSD II*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 81–93.

Maison D., *Postawy Polaków wobec obrotu bezgotówkowego. Raport z badania 2016 i analiza porównawcza z danymi z 2009 i 2013 r.*, https://www.nbp.pl/badania/seminaria/8v2017.pdf [dostęp: 10 X 2017].

Marciniak A., *Bankowy CERT – nowa broń w walce z cyberprzestępczością*, w: *Wyzwania informatyki bankowej 2016,* A. Kawiński, A. Sieradz (red.), Gdańsk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf [dostęp: 2 X 2017].

Mostowik M., *Prawna ochrona informacji o rachunku płatniczym w świetle usługi dostępu do informacji o rachunku (AIS)*, „Monitor Prawa Bankowego" 2017, nr 7–8, s. 35–42.

Pacak M., *Usługi płatnicze. Komentarz*, Warszawa 2014, LexisNexis.

Radziejewski K., *Cyberbezpieczeństwo w administracji rządowej w Rzeczpospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 16, s. 308–330.

Staszczyk M., *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości*, http://www.finanseiprawofinansowe.uni.lodz.pl/Publikacje/5/4_Staszczyk.pdf [dostęp: 2 X 2017].

Akty prawne:

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) 1093/2010 oraz uchylająca dyrektywę 2007/64/WE (Dz. Urz. UE L 337 z 23 grudnia 2015 r., s. 35).

Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48 WE i uchylająca dyrektywę 97/5/WE (Dz. Urz. UE L 319 z 5 grudnia 2007, s. 1).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j.: Dz.U. z 2017 r. poz. 2003, ze zm.).

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j.: Dz.U. z 2018 r. poz. 1401).

Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami (t.j.: Dz.U. z 2018 r. poz. 145, ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j.: Dz.U. z 2017 r. poz. 1876, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: Dz.U. z 2017 r. poz. 2204, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j.: Dz.U. z 2018 r. poz. 452, ze zm.).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 575/2013 z dnia 26 czerwca 2013 r. w sprawie wymogów ostrożnościowych dla instytucji kredytowych i firm inwestycyjnych, zmieniające rozporządzenie (UE) nr 648/2012 (Dz. Urz. UE L 176 z 27 kwietnia 2013 r., s. 1).

Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2015/751 z dnia 29 kwietnia 2015 r. w sprawie opłat interchange w odniesieniu do transakcji płatniczych realizowanych w oparciu o kartę (Dz. Urz. UE L 123 z 19 maja 2015, s. 1).

Projekt ustawy o zmianie ustawy o usługach płatniczych oraz niektórych innych ustaw, numer z wykazu: UC81.

Abstrakt

Płatności internetowe i mobilne z uwagi na ich bezgotówkowy charakter i szybkość dokonywania transakcji cechują się dużym potencjałem rozwojowym. Wraz ze wzrostem ich wolumenu ilościowego i kwotowego rosną także zagrożenia związane z ich procesowaniem, ponieważ odbywają się one bez fizycznego udziału stron transakcji i w środowisku internetowym. Nowe metody płatności doprowadziły do pojawienia się nowych dostawców usług płatniczych – tzw. *Third Party Payment Service Providers*, tj. dostawców będących podmiotami trzecimi, których działalność może się wiązać z określonymi zagrożeniami. W skali mikro można stypizować zagrożenia związane z bezpieczeństwem środków finansowych użytkowników. W skali makro należy wskazać na potencjalne zagrożenia tzw. płatniczej infrastruktury krytycznej i szerzej – cyberbezpieczeństwa.

Słowa kluczowe: dyrektywa PSD, cyberprzestępczość, *Third Party Providers*, infrastruktura krytyczna, Komisja Nadzoru Finansowego, elektroniczne transakcje płatnicze, płatności mobilne, płatności internetowe, *Account Servicing Payment Service Provider*, *Account Information Service*, *Payment Initiation Service*.

Konrad Hennig

Krajowa własność technologii wytwarzania energii jako czynnik składowy bezpieczeństwa energetycznego Polski

Bezpieczeństwo energetyczne każdego kraju jest uzależnione od takiego ukształtowania bilansu energetycznego, aby gwarantował on najwyższą odporność na: ataki z zewnątrz (rozproszenie instalacji wytwórczych), awarie (opanowanie technologii) oraz zaburzenia dostaw źródeł energii (niezależność lub dywersyfikacja źródeł i kanałów transportu). W praktyce politycznej bezpieczeństwo energetyczne bywa często rozumiane jedynie jako niezależność energetyczna, czyli maksymalizacja wykorzystania źródeł energii pozyskiwanych na własnym terytorium. Oparcie krajowego bilansu energetycznego na dostępnych w danym kraju źródłach energii pierwotnej jest z pewnością pierwszym krokiem odpowiedzialnej polityki energetycznej. Nie mniej istotne, a często pomijane, jest wykorzystywanie własnych technologii pozyskania źródeł oraz wytwarzania energii. Wobec rosnącego znaczenia wyzwań ekonomicznych i technologicznych w rywalizacji mocarstw zagadnienia bezpieczeństwa energetycznego stają się istotnym elementem debaty publicznej. Można wyróżnić cztery elementy składowe bezpieczeństwa energetycznego: 1) niezależność pozyskiwania źródeł energii; 2) stabilność sieci elektroenergetycznej i przesyłu paliw; 3) dywersyfikacja zagranicznych kierunków dostaw surowców energetycznych i źródeł wytwarzania energii na terenie kraju; 4) niezależność technologiczna, czyli krajowa własność technologii wytwarzania energii, na której autor skoncentrował się w niniejszym artykule.

Stopień niezależności energetycznej – obliczony jako udział energii wytworzonej z krajowych źródeł w całości zużytej energii – prezentuje się następująco dla pięciu wybranych państw UE (tab. 1).

Tab. 1. Stopień niezależności energetycznej dla wybranych państw (dane z 2014 r.).

Kraj	**Zużycie energii ogółem** (w tys. toe)	**Pozyskanie energii ogółem** (w tys. toe)	**Stopień niezależności energetycznej** (współczynnik proporcji)
Niemcy	306 753	120 713	**0,393519**
Hiszpania	114 559	35 101	**0,306401**
Francja	242 642	137 128	**0,565145**
Wlk. Brytania	179 421	108 236	**0,603252**
Polska	94 018	67 326	**0,716097**

Źródło: Opracowanie własne za: „Energy Balances of OECD Countries", IEA.

Polska wykazuje się wysokim stopniem niezależności energetycznej, co wynika z proporcjonalnej do potrzeb polskiej gospodarki eksploatacji węgla kamiennego i brunatnego oraz wydobycia gazu ziemnego, pokrywającego ok. 30 proc. krajowego zapotrzebowania. *Najważniejszym pozyskiwanym nośnikiem energii jest węgiel kamienny (60,6% w 2015 r.). Drugim pod względem wielkości wydobycia nośnikiem był węgiel brunatny z udziałem wynoszącym 17,9%. Udział gazu ziemnego w pozyskaniu wyniósł 5,4%, ropy naftowej 1,4%, a pozostałych, w znacznej mierze odnawialnych nośników energii, 14,7%*. Z kolei (…) *najważniejszym zużywanym nośnikiem był węgiel kamienny z udziałem wynoszącym 39,5%. Udział ropy naftowej wyniósł 25,1%, a gazu ziemnego 14,0%. Węgiel brunatny stanowił 11,6% zużytej energii, a pozostałe nośniki 9,8%*[1]. Czy w związku z tym można uznać z satysfakcją, że jako kraj Polska ma zapewniony podstawowy poziom bezpieczeństwa energetycznego?

Być może na tak postawione pytanie byłoby możliwe udzielenie odpowiedzi twierdzącej przy perspektywie ujęcia statystycznego. Należy jednak mieć świadomość, że bezpieczeństwo to nie stan, ale zbiór diachronicznych procesów. Zmienność zjawisk w czasie, szczególnie wobec ich złożoności i wzajemnej współzależności, wymusza uwzględnienie dynamiki stojących przed rządami wyzwań oraz zagrożeń. Procesy widziane dzisiaj w małej skali mogą w perspektywie niedługiego czasu rosnąć geometrycznie, zagrażając stabilności systemu elektroenergetycznego czy paliwowego. Z wielką ostrożnością należy pochodzić do złudnego optymizmu płynącego z dotychczasowych doświadczeń funkcjonowania systemu elektroenergetycznego opartego na spalaniu węgla.

W polityce rządowej duży nacisk kładzie się w ostatnich latach na dywersyfikację dostaw paliw płynnych (zwłaszcza gazu), podczas gdy polski system elektroenergetyczny cierpi na wyjątkowo niską elastyczność pięciu podstawowych obszarów regulujących pracę tego systemu: 1) sterowania dostawami; 2) sterowania zapotrzebowaniem; 3) magazynowania; 4) starzejących się sieci oraz 5) konstrukcji rynków hurtowego, bilansującego i detalicznego[2]. To powoduje, że ten system jest narażony na utratę stabilności dynamicznej (ryzyko obniżenia napięcia: *brown-out*, ryzyko odcięcia napięcia: *black-out*) na skutek niezbilansowania ilości energii wyprodukowanej w danym czasie z ilością energii przetworzonej w odbiornikach i utraconej podczas przesyłu. Elastyczność systemu elektroenergetycznego w Polsce jest ograniczona przez brak zarówno połączeń międzynarodowych, magazynów energii, jak i krajowej rezerwy mocy, którą można dysponować. Instalacje węglowe stanowiące bazę w produkcji prądu są częściowo elastyczne, ale ich wygaszanie wiąże się z wysokim ryzykiem uszkodzeń i awarii, a praca w pełnej ich mocy jest uzależniona od dostęp-

[1] *Gospodarka paliwowo-energetyczna w latach 2014 i 2015*, Warszawa 2016, http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5485/4/11/1/gospodarka_paliwowo_energetyczna_2014_2015.pdf [dostęp: 12 VI 2017].

[2] I. Kielichowska, E. Haesen, T. Sach, *Flexibility Tracker Country Report Poland*, http://www.leonardo-energy.org/resources/503/flexibility-tracker-country-report-poland-5814f41cb7050 [dostęp: 12 VII 2017].

ności wody chłodzącej. Najwyższą elastyczność wykazują instalacje gazowe, które są wykorzystywane tylko w segmentach ciepłownictwa, skojarzonej kogeneracji komunalnej i przemysłowej. Instalacje wiatrowe i fotowoltaiczne są zależne wyłącznie od pogody i nie jest możliwe dysponowanie nimi zgodnie z potrzebami Krajowego Systemu Elektroenergetycznego. Wzrost udziału tych dwóch instalacji w miksie energetycznym prowadzi do dalszego nabrzmiewania problemu niskiej elastyczności systemu. Wyłącznie elektrownie szczytowo-pompowe, nieliczne w Polsce, mają wysoką elastyczność (reakcja w ciągu 2–3 minut) oraz możliwość magazynowania energii. Tym bardziej dziwi zawieszenie pod koniec lat 80. XX w. budowy Elektrowni Wodnej Młoty (750 MW), a następnie sprzedanie jej Électricité de France. Nieukończona elektrownia wróciła wraz z końcem 2017 r. w ręce Polskiej Grupy Energetycznej S.A., więc można się spodziewać przeprowadzenia w najbliższym czasie analizy opłacalności jej dokończenia. Jedyną alternatywną lokalizacją umożliwiającą budowę elektrowni o porównywalnej skali jest zwałowisko zewnętrzne Pola Szczerców przy Kopalni Węgla Brunatnego Bełchatów. Obecnie w Polsce działa sześć elektrowni szczytowo-pompowych: 1) Żarnowiec; 2) Porąbka-Żar; 3) Żydowo; 4) Solina; 5) Dychów oraz 6) Niedzica. Łącznie są w stanie magazynować 10 GWh, a ich moc zainstalowana wynosi 1700 MW.

Podobnie jak kilka dekad temu elastyczność polskiego systemu elektroenergetycznego jest uzależniona od stopni zasilania, a więc elastyczności odbiorców energii elektrycznej, a nie jej wytwórców. Wprowadzenie odpłatnego ograniczania poboru prądu przez wybranych odbiorców DSR (*Demand Side Response*)[3] pozwoli wyłącznie na ominięcie kosztu politycznego wprowadzenia stopni zasilania (w połowie 2018 r. umowy DSR zostały podpisane na ok. 500 MW[4]), ale nie zmieni dotychczasowej logiki. Co więcej, (…) *sieci przesyłowe są wiekowe i obciążone: ponad 80% sieci 220 kV, 56% sieci 400 kV oraz 34% podstacji ma ponad 30 lat; również w przypadku sieci dystrybucyjnych ich przeciętny wiek to ponad 30 lat*[5]. Podstawą konstrukcji rynku zakupów energii przez odbiorców hurtowych są kontrakty terminowe i zakupy Rynku Dnia Następnego. Polska jest dopiero w przededniu zróżnicowania cen dla okresów szczytu i nizin poboru mocy, a za ich pośrednictwem sterowania zapotrzebowaniem na prąd odbiorców przemysłowych.

Zapewnienie bezpieczeństwa energetycznego przez zwiększanie elastyczności sieci elektroenergetycznej wymaga wdrożenia całego szeregu rozwiązań technologicznych, realizacji inwestycji o wartości kilkudziesięciu miliardów złotych i aktualizacji uregulowań prawnych. Dzięki przedsiębiorstwom technologicznym, które starają się zainteresować decydentów swoimi produktami i rozwiązaniami informatycznymi, zwiększa się świadomość powyższych potrzeb. Ścisłe powiązania branży energetycznej z przemysłem i konieczność odpowiadania na zapotrzebowania

[3] Odpłatne ograniczanie poboru prądu przez dużych odbiorców.

[4] https://www.pse.pl/uslugi-dsr-informacje-ogolne [dostęp: 8 VI 2018].

[5] *Elastyczność w energetyce – wyzwania stojące przed Polską*, http://nowa-energia.com.pl/2017/03/30/elastycznosc-w-energetyce-wyzwania-stojace-przed-polska/ [dostęp: 20 VII 2017].

gospodarki stwarza nadzieję, że zaniedbania trzech ostatnich dekad uda się odrobić szybciej, niż w przypadku modernizacji technicznej Sił Zbrojnych RP.

Niezależność energetyczna i stabilność sieci elektroenergetycznej to jednak nie wszystko. Nie mniej ważna dla bezpieczeństwa energetycznego jest dywersyfikacja krajowych źródeł wytwarzania energii elektrycznej. Struktura polskiego bilansu energetycznego jest pokłosiem decyzji podjętych w czasach komunizmu przez decydentów radzieckich. W 1990 r. produkcja prądu była oparta w 98 proc. na spalaniu węgla w elektrowniach zawodowych i elektrociepłowniach, a w 2 proc. na elektrowniach wodnych. Węgiel kamienny stanowił wówczas źródło prawie 70 proc. energii konwencjonalnej, a brunatny niemal 30 proc. Pomimo korzystania z własnego surowca, nie była to sytuacja optymalna z punktu widzenia bezpieczeństwa systemu. Jak w przypadku każdej monokultury, cały krajowy system elektroenergetyczny był narażony na ryzyko zmian w jednym sektorze (czyli w sektorze węglowym), związanych ze wzrostem cen surowca bądź wdrożeniem unijnej polityki antywęglowej. Udział węgla w produkcji prądu ograniczono obecnie do 86 proc., część pozostałych 14 proc. stanowi współspalanie biomasy w instalacjach węglowych. Gospodarka energetyczna wciąż nie może pochwalić się proporcjonalnie zdywersyfikowanym bilansem energetycznym, w którym udział poszczególnych 4–5 źródeł wynosiłby 15–30 proc., co wydaje się być sytuacją optymalną.

Kształtowanie się krajowych bilansów energetycznych było na całym świecie wynikiem wieloletnich procesów, na które wpływało wiele endo- i egzogenicznych czynników. Odmienne uwarunkowania poszczególnych państw skutkowały wytworzeniem się diametralnie różnych proporcji udziału energii odnawialnej, jądrowej, węglowej czy gazowej. Najistotniejszą rolę w powstawaniu miksu energetycznego danego kraju odgrywało ukształtowanie powierzchni tego kraju, jego zasoby wodne, zasoby paliw kopalnych, sytuacja geopolityczna i stopień rozwoju technologicznego. W konsekwencji zarówno bilans energii pierwotnej, struktura wytwarzania energii elektrycznej oraz wykorzystanie paliw w sektorze komunalno-bytowym mogą różnić się znacznie nawet pomiędzy bardzo podobnymi i sąsiadującymi ze sobą państwami, gdyż wystarczy różnica jednego czynnika, aby diametralnie zaburzyć proporcje udziału poszczególnych źródeł energii.

Struktura wytwarzania energii elektrycznej dla danego kraju jest względnie trwała, co jest związane z tym, że procesy intencjonalnego przechodzenia na inne źródła energii trwają latami, np. cykl planowania i budowy jednej elektrowni konwencjonalnej to 5–12 lat, jej budowa pochłania ogromne koszty kapitałowe, a w przypadku zmiany bilansu kraju średniej wielkości należy zbudować co najmniej kilka takich elektrowni. Przechodzenie na inne źródła energii jest zazwyczaj motywowane odkryciem na terenie danego państwa bardziej efektywnych źródeł energii, np. rozpoczęciem eksploatacji nieznanych wcześniej zasobów kopalin lub wypracowaniem nowej technologii (bądź rezygnacji ze stosowanej technologii) w związku z katastrofami naturalnymi czy antropogenicznymi). W przypadku większości zmian nowe źródła zamiast zastępować dotychczasowe, uzupełniały wzrastające zapotrzebowanie gospodarki na energię

elektryczną. Przykładem wprowadzania intencjonalnych zmian są Japonia[6] i Niemcy, które podjęły decyzję stopniowego wygaszenia elektrowni atomowych do 2022 r. Wydaje się, że polska transformacja energetyczna nie będzie tak rewolucyjna, a wykorzystywanie nowego źródła wytwarzania będzie wynikało z zaspokajania rosnącego popytu. Otwartym pytaniem pozostaje, jakie źródło będzie wybrane przez polski rząd (do tego pytania autor powróci w podsumowaniu niniejszego tekstu).

Z ekonomicznego punktu widzenia bilans energetyczny jest funkcją dostępności i kosztu wytworzenia energii. W przypadku Polski dostępność poszczególnych źródeł energii można podzielić na trzy segmenty (tab. 2).

Tab. 2. Dostępność źródeł energii w Polsce.

Poziom dostępności	**Źródło wytwarzania energii**
Dostępność wysoka	węgiel kamienny i brunatny, biopaliwa stałe i ciekłe (odpady stałe roślinne i zwierzęce, odpady przemysłowe stałe i ciekłe, odpady komunalne, biogaz z wysypisk śmieci i oczyszczalni ścieków), energia geotermalna
Dostępność średnia	gaz ziemny (w tym łupkowy), energia wiatru
Dostępność niska	ropa, energia wody, energia jądrowa, energia promieniowania słonecznego

Źródło: Opracowanie własne autora.

Pod względem technicznych kosztów wytworzenia energii poszczególne źródła prezentują się następująco (tab. 3).

Tab. 3. Jednostkowe koszty techniczne wytworzenia energii w Polsce (zł/MWh) w latach 2012–2015.

Źródło energii	**2012**	**2013**	**2014**	**2015**
Węgiel brunatny	139,7	134,6	134,9	130,4
Woda	186,2	153,0	170,5	164,2
Węgiel kamienny	212,5	199,3	183,9	172,3
Wiatr	208,0	222,1	227,8	210,9
Gaz ziemny	303,1	372,2	261,0	241,2
Biomasa	446,1	405,6	361,6	367,9

Źródło: Opracowanie własne za: Z. Kasztelewicz, A. Tajduś, T. Słomka, *Węgiel brunatny to paliwo przyszłości czy przeszłości?*, w: *Węgiel brunatny gwarantem bezpieczeństwa energetycznego* (materiały pokonferencyjne), Kraków 2016, s. 237.

[6] W Japonii po kilku latach od katastrofy w Fukushimie można zauważyć stopniowe odchodzenie od tak radykalnych decyzji, zob. J. Malko, *Energetyka japońska. Jak radykalna transformacja?*, „Energetyka" 2013, nr 6; także http://www.cire.pl/pliki/2/energ_japonska.pdf [dostęp: 18 VIII 2017].

Z powyższych danych wynika, że w Polsce czynniki ekonomiczne premiują wykorzystanie węgla brunatnego, kamiennego i energii wody, a wpływają na ograniczenie stosowania gazu ziemnego i biomasy. W polskim miksie energetycznym nie występuje energia jądrowa, a energia słoneczna i geotermalna jest obecna w śladowych ilościach, gdyż użytkowanie tych dwóch źródeł powoduje podwyższenie kosztów wytworzenia. Kryteria ekonomiczne nie są jednak decydujące przy podejmowaniu decyzji politycznych. Powinny być oczywiście brane pod uwagę ze względu na spadek międzynarodowej konkurencyjności energochłonnych sektorów gospodarki przy wysokich cenach energii, ale polityka energetyczna państwa musi uwzględniać również inne czynniki, a nie tylko efektywność ekonomiczną. Z punktu widzenia bezpieczeństwa energetycznego istotne są czynniki geograficzne i technologiczne: dostępność źródeł energii oraz opanowanie przez krajowy przemysł technologii wytwarzania z nich prądu. O niezależności energetycznej nie można mówić na podstawie samego tylko posiadania źródeł energii (kopalnych lub odnawialnych), ale dopiero po uwzględnieniu posiadania przez przedsiębiorstwa i instytucje naukowo-badawcze danego kraju know-how całego cyklu projektowania obiektów wydobywczych i wytwórczych oraz produkcji maszyn i urządzeń służących do wydobycia i wytwarzania energii elektrycznej.

K r a j o w e p r z e d s i ę b i o r s t w a – zarejestrowane, płacące podatki, prowadzące działalność produkcyjną i badawczo-rozwojową w danym kraju, znajdujące się w rękach państwa bądź obywateli danego kraju – w przypadku Polski mają zdolność całkowicie samodzielnej realizacji projektów wydobywczych kopalin znajdujących się w konwencjonalnych złożach na terytorium kraju: węgla kamiennego, brunatnego, ropy i gazu ziemnego oraz energii geotermalnej. Polska jest ważnym producentem kolektorów słonecznych (ogrzewanie wody użytkowej w sektorze komunalno-bytowym) i coraz lepiej radzi sobie z rozwojem własnych technologii w energetyce wiatrowej (również zlokalizowanej na morzu), choć najistotniejsze elementy (turbina wiatrowa i generator) wciąż pochodzą od zagranicznych dostawców. W mniejszym stopniu opanowaliśmy technologię wytwarzania energii elektrycznej. Pomimo że Polska ma zdolności produkcyjne instalacji bazujących na węglu kamiennym, brunatnym i energii wody, to duże inwestycje były w ostatnich latach niejednokrotnie realizowane przez firmy zagraniczne bądź konsorcja firm krajowych i zagranicznych – najważniejsze technologie dostarczał Siemens, Hitachi Mitsubishi oraz General Electric. Zastawienie najważniejszych modernizacji i inwestycji w instalacje wytwarzania obrazuje tab. 4.

Tab. 4. Wykonawcy wybranych inwestycji w moce wytwórcze.

Rok realizacji	Inwestor	Lokalizacja	Wykonawca
1	2	3	4
1995–2004	Elektrownia Wodna Żarnowiec S.A.	Żarnowiec	system WDPF 2 firmy Westinghouse, system Compass firmy Brüel&Kjœr, system HydroScan firm MCM i IRIS, Automatyczny System Technicznej Kontroli Zapór od firmy Budokop Sp. z o.o.
2013–2017	PKN Orlen SA	Elektrociepłownia Przemysłowa Włocławek	blok gazowo-parowy od konsorcjum General Electric i SNC Lavalin
2012–2014	Jastrzębska Spółka Węglowa SA	Koksownia Przyjaźń w Dąbrowie Górniczej	generalny wykonawca: Energoinstal; turbozespół na gaz koksowniczy firmy Siemens
2011–2013	KGHM Polska Miedź SA	EC Głogów EC Polkowice	bloki gazowo-parowe firmy Energoinstal
2004–2011	PGE S.A.	Elektrownia Bełchatów	blok nadkrytyczny na węgiel brunatny konsorcjum firm General Electric, Alstom i Rafko
2014–2017	Spółka Energetyczna Jastrzębie SA	EC Zofiówka	kogeneracyjny blok fluidalny CFB od konsorcjum Energoinstal S.A. (80 proc.) i Przedsiębiorstwa Budownictwa Ogólnego Skobud (20 proc.)
2013–2017	PGE S.A.	EC Gorzów Wielkopolski	blok gazowo-parowy od konsorcjum firm Siemens Sp. z o.o. oraz Siemens Industrial Turbomachinery AB
2012–2017	Enea S.A.	Elektrownia Kozienice	blok na węgiel kamienny o parametrach nadkrytycznych od konsorcjum Polimex-Mostostal i Hitachi Power Europe
2015–2018	Fortum	EC Zabrze	blok kogeneracyjny na paliwo alternatywne, węgiel i biomasę; inżynier kontraktu ILF Consulting Engineers; kocioł z cyrkulacyjnym złożem fluidalnym od firmy Amec Foster Wheeler; turbozespół wraz z generatorem oraz systemem wymienników ciepłowniczych od Doosan Škoda Power; zewnętrzny układ podawania węgla i paliwa alternatywnego od BMH Technology; konstrukcje stalowe od firmy Mostostal Zabrze; roboty budowlane świadczone przez Budimex SA

1	2	3	4
2014–2019	PGE S.A.	Elektrownia Turów	blok na węgiel brunatny od konsorcjum Mitsubishi Hitachi Power Systems Europe (55,38 proc.), Budimex (22,31 proc.) oraz Tecnicas Reunidas (22,31 proc.)
2014–2019	PGE S.A.	Elektrownia Opole	konsorcjum firm Rafako, Polimex-Mostostal i Mostostal Warszawa. Blok ultra nadkrytyczny firmy General Electric; dwa kotły BP firmy Rafako; generatory i turbiny parowe na parametry ultrakrytyczne, kotły, systemy pomocnicze elektrowni oraz instalacje ochrony środowiska od firmy Alstom
2014–2019	Tauron S.A.	Elektrownia Jaworzno	konsorcjum Rafako (99,99 proc.) i Mostostal Warszawa (0,01 proc.); turbina firmy Siemens
2014–2016	Zakłady Azotowe Kędzierzyn	EC Kędzierzyn-Koźle	kompletna instalacja kogeneracyjna od firmy Rafako
2012–2019	Tauron S.A. PGNiG Termika	EC Stalowa Wola	w 2016 r. zerwano kontrakt z generalnym wykonawcą, hiszpańską firmą Abener Energia; turbina gazowa General Electric oraz turbozespół parowy Skoda Power; budowę w formule EPCM (Engineering Procurement Construction Management) dokończy konsorcjum Zakładów Pomiarowo-Badawczych Energetyki Energopomiar i Energoprojekt-Katowice
2017–2020	PGNiG Termika	EC Żerań	kogeneracyjny blok gazowo-parowy od konsorcjum firm Mitsubishi Hitachi Power Systems Europe Gmbh, Mitsubishi Hitachi Power Systems Ltd, Mitsubishi Hitachi Power Systems Europe, Polimex-Mostostal

Źródło: Opracowanie własne na podstawie materiałów prasowych przedsiębiorstw oraz informacji pt. *Budowane i planowane elektrownie*, http://www.rynek-energii-elektrycznej.cire.pl/st,33,335,tr,145,0,0,0,0,0,budowane-i-planowane-elektrownie.html [dostęp: 16 VIII 2017].

Istnienie krajowych firm specjalizujących się w poszczególnych branżach podkreślono wyraźnie w *Programie dla sektora górnictwa węgla kamiennego w Polsce* z 2016 r.:

> Polska posiada rozwinięty sektor górniczy, w tym przemysł maszyn i urządzeń górniczych. Rodzime firmy produkujące maszyny i urządzenia górnicze są przedsiębiorstwami prywatnymi, często notowanymi na Giełdzie Papierów Wartościowych w Warszawie. Przeważająca większość firm skupiona jest w południowej części kraju. Należy także zaznaczyć, że polski sektor maszyn górniczych charakteryzuje się dużą różnorodnością. W ciągłej produkcji są maszyny służące do wydobywania surowców mineralnych, sekcje obudowy zmechanizowanej, przenośniki (taśmowe i zgrzebłowe), maszyny służące do transportu ludzi i materiałów, urządzenia zapewniające bezpieczeństwo, sprzęt wiertniczy, przewody elektryczne, transformatory, pompy, odzież robocza i inne. Polskie marki są rozpoznawalne na świecie i cenione za wysoką jakość. Obecnie eksport ukierunkowany jest głównie na: Rosję, Chiny, Mongolię, Kazachstan, Australię, Indonezję, Indie, Kanadę, Stany Zjednoczone, Argentynę, Kolumbię, Ekwador i Kongo. Jak wynika z powyższego krajowi producenci są rozpoznawalni na wszystkich kontynentach, na których prowadzone jest wydobycie surowców mineralnych i energetycznych metodą odkrywkową, otworową i podziemną[7].

Polski przemysł specjalizuje się w wydobyciu konwencjonalnych kopalin. Eksploatacją krajowych zasobów gazu i ropy naftowej zajmuje się PGNiG SA, wydobycie węgla kamiennego prowadzą m.in.: JSW SA, PGG S.A., Bogdanka S.A., a węgla brunatnego PGE GiEK S.A., ZE PAK SA oraz KWB Sieniawa Sp. z o.o. Polskie firmy są również potentatem w produkcji maszyn i urządzeń. Grupa Famur S.A. (m.in. Kopex, Famak, Famago, Fugo, Pioma), Bumech S.A. i Fasing S.A. produkują wszystkie rodzaje maszyn górniczych i przenośników. Realizacji pierwszych całościowych zleceń dla KWB Turów podjęła się niedawno spółka RAMB z grupy PGE S.A. Prężnie działają instytuty badawcze i biura projektowe, m.in. Energoprojekt-Katowice SA, SKW Biuro Projektowo-Techniczne Sp. z o.o., Poltegor-Projekt Sp. z o.o., Główny Instytut Górnictwa, Poltegor-Instytut, Instytut Chemicznej Przeróbki Węgla. Potentaci polskiego rynku wraz z polskimi podwykonawcami mają możliwości pełnego zakresu poszukiwania i badania złóż, budowy szybów projektowania kopalń i prowadzenia wydobycia. Polska ma całościowe know-how i zaplecze produkcyjne maszyn i urządzeń dla prowadzenia nowych projektów wydobywczych.

Nieco gorzej sytuacja wygląda w przypadku instalacji wytwórczych ze względu na technologiczne zacofanie polskich firm w podnoszeniu sprawności tych instalacji i ograniczaniu emisyjności. Firmy budowlane – Elektrobudowa SA, Mostostal Warszawa SA i Polimex-Mostostal S.A. – zapewniają obsługę kontraktów budowlanych i dostarczają konstrukcje stalowe elektrowniom i elektrociepłowniom budowanym w Polsce. Rafako S.A. i Remak S.A. dostarczają kotły i oprzyrządowanie elektrowniom węglowym, a Energoprojekt-Warszawa SA czy HydroErgia Sp. z o.o. sp.k elektrowniom wodnym. Dziesiątki małych i średnich firm produkują podzespoły i urządzenia dla górnictwa i energetyki. Spośród nich warto wymienić Konsorcjum Przemysłowe INTEC-WAKMET,

[7] *Program dla sektora górnictwa węgla kamiennego w Polsce*, Warszawa 2016, s. 80.

grupę Revico, Ania Holding, firmę CHEMAR Armatura Sp. z o.o. czy Fabrykę Kotłów SEFAKO S.A. Brakuje polskiego producenta turbogeneratorów parowych i gazowych. Przemysł polski posiłkuje się rozwiązaniami Siemensa, General Electric, Doosan Škoda Power czy Mitsubishi Hitachi Power Systems Europe. Szanse na repolonizację elbląskiego Zamechu (który po prywatyzacji w 1990 r. przeszedł z rąk ABB i Alstomu do General Electric) nie wydają się dzisiaj realne. Najgorzej jednak polski przemysł wypada w sektorze odnawialnych źródeł energii – brakuje przede wszystkim firmy produkującej nowoczesne i konkurencyjne turbiny bezprzekładniowe. Nieco lepiej sytuacja wygląda w obszarze energii słonecznej. Polska jest potentatem produkcji i wykorzystania kolektorów solarnych (podgrzewanie wody użytkowej), a w produkcji paneli fotowoltaicznych wyspecjalizowała się bydgoska firma FreeVolt, która prowadzi zaawansowane badania nad zastosowaniem grafenu, co zwiększy wydajność ogniw o kilkadziesiąt procent. Rozwój tych technologii mógłby być stymulowany polityką przemysłową państwa realizowaną przez cztery największe grupy energetyczne znajdujące się w rękach Skarbu Państwa. W sektorze mikroinstalacji i prosumenckiej[8] energetyki rozproszonej Polska jest jeszcze na początku drogi, pomimo samych zalet tego rodzaju energetyki i finansowania tysięcy drobnych inwestorów.

Posiadanie własnego zaplecza technologicznego i produkcyjnego maszyn i urządzeń do wydobycia kopalin oraz wytwarzania energii elektrycznej oprócz gwarancji bezpieczeństwa energetycznego przynosi krajowej gospodarce dodatkowe korzyści. Są nimi: rozwój technologiczny polskich przedsiębiorstw osiągających wysoką wartość dodaną z prowadzonej działalności, uczelni i instytutów badawczych oraz istnienie wysokopłatnych miejsc pracy wymagających zaawansowanych kompetencji i oferujących wysokie wynagrodzenia (w przypadku polskiej gospodarki to prawie pół miliona pracowników).

Rozwój krajowych koncernów przemysłowych powinien być objęty dużo większą troską władz publicznych niż start-upy powstające w branży nowych technologii. Tym bardziej, że ryzyko negatywnej weryfikacji modelu biznesowego w przypadku start-upów jest dużo wyższe. Słabością polskiej gospodarki na tle zachodniej konkurencji jest niedostatek dużych przedsiębiorstw przemysłowych, co skutkuje brakiem partnera dla polskich uczelni technicznych i niską innowacyjnością całej gospodarki. Brakuje rozwiniętych, doświadczonych firm dysponujących gotówką i mających zdolność kredytową, które mogłyby podejmować wyzwania komercjalizacji nowych technologii. Ta strukturalna słabość polskiej gospodarki ma przyczyny historyczne. Start polskich firm na otwartym międzynarodowym rynku był trudniejszy niż zachodnich firm ze względu na nierynkowe warunki wzrostu w gospodarce socjalistycznej i konsekwencje uwarunkowań organizacyjno-kulturowych, m.in. wpływy antyrozwojowych grup interesu czy nieelastyczna postawa związków zawodowych.

[8] Polski ustawodawca wdrożył rozbudowane instrumentarium finansowego i regulacyjnego wspierania energetyki zawodowej, pracuje nad systemem wsparcia dla elektrociepłownictwa, natomiast małych wytwórców prądu, będących jednocześnie jego konsumentami (małe firmy i gospodarstwa domowe), traktuje z dużą rezerwą.

W gospodarce socjalistycznej obrót gospodarczy był z przyczyn politycznych ograniczony, co wpłynęło na niedostateczne wykształcenie się przedsiębiorstw o wysokim stopniu specjalizacji produktowej i technologicznej. Specjalistyczne kompetencje były rozdzielone między różne zakłady, zamiast zostać skoncentrowane w jednym podmiocie świadczącym tym zakładom usługi. Po 1989 r. nie scentralizowano odgórnie zakładów mających podobne kompetencje. Rządy III RP zrezygnowały z prowadzenia skoordynowanej polityki przemysłowej, a nawet zbierania danych o losach przedsiębiorstw prywatyzowanych przez urzędy wojewódzkie i centralne[9].

Budowanie przedsiębiorstw na podstawie posiadanych technologii (patentów, know-how), kompetencji pracowników, znajomości rynku oraz relacji handlowych było wyróżnikiem zachodniego modelu kapitalizmu, podczas gdy w bloku komunistycznym tymi samymi zasobami dysponowało państwo będące właścicielem wszystkich przedsiębiorstw. Brakowało rozdzielenia własności przedsiębiorstw górniczo-energetycznych (wydobycie kopalin i wytwarzanie energii) oraz produkcyjnych (produkcja maszyn i urządzeń do wydobycia i wytwarzania). Pomimo funkcjonowania w ramach bloku państw socjalistycznych pewnych mechanizmów odgórnej koordynacji polityki gospodarczej, nie udało się w porównywalnym do Zachodu stopniu zbudować silnych przedsiębiorstw technologicznych, zdolnych do istnienia na rynkach zagranicznych. Funkcjonowanie na tak dużym rynku wiąże się z koniecznością poniesienia wysokich kosztów badań oraz stałych kosztów zatrudniania specjalistów posiadających wyjątkową wiedzę i umiejętności. Podjęcie ekspansji zagranicznej nie jest zatem decyzją zarządzających, ale wynika ze struktury rynku, z konieczności prowadzenia określonego rodzaju działalności. Transformująca się (a w rzeczywistości – wychodząca z bankructwa) polska gospodarka nie zapewniła potencjalnym narodowym czempionom dostatecznie stabilnych warunków, aby przetrwać najtrudniejszy okres. Na skutek patologicznego modelu transformacji ustrojowej Polska pozbawiła się zagranicznych rynków zbytu, a krajowy był zbyt mały, aby zapewnić ciągłość działania firm o wysokim stopniu specjalizacji. Musiały one dodatkowo nadganiać zapóźnienie technologiczne wobec zagranicznej konkurencji, nie mając praktycznie żadnego dostępu do kredytu.

Niewydolności gospodarcze w czasach realnego socjalizmu związane z centralnym planowaniem sprzyjały daleko idącej integracji pionowej kombinatów przemysłowych. Wobec ograniczonych możliwości pozyskiwania towarów i usług z przedsiębiorstw zewnętrznych firmy energetyczne wytwarzały własne zaplecze we wszystkich niezbędnych obszarach (bocznice kolejowe, środki transportu, produkcja komponentów, oddziały remontowe, zaplecze gastronomiczne, hotelowe, wczasowe, sportowe). W dużych przedsiębiorstwach powstawały nawet przyzakładowe gospodarstwa rolne, które miały dostarczać żywność stołówkom pracowniczym. Po przemianach ustrojowych proste usługi, jak ochrona, sprzątanie, logistyka, gastronomia, zostały prze-

[9] Zob. B. Godusławski, *Prywatyzacyjne fakty i mity. Do dzisiaj nie wiemy, ile firm sprzedaliśmy*, http://biznes.gazetaprawna.pl/artykuly/1087293, prywatyzacyjne-fakty-i-mity.html [dostęp: 25 XI 2017].

kazane podmiotom zewnętrznym (niekiedy pozostającym w dalszym ciągu w grupie kapitałowej). W strukturach państwowych przedsiębiorstw energetycznych pozostały komórki zajmujące się procesami wymagającymi zaawansowanych kompetencji i zaplecza technicznego, na przykład robotami budowlanymi, remontowymi, produkcją komponentów i półproduktów.

Polski rząd przy podejmowaniu decyzji o inwestycjach w moce wytwórcze kolejnych elektrowni powinien mieć na celu wzmacnianie kondycji finansowej i kompetencji technologicznych polskich przedsiębiorstw. Analogia do programu modernizacji technicznej Sił Zbrojnych RP, jaka pojawiła się na początku artykułu, nie była przypadkowa. Przy zakupach rodzajów uzbrojenia niedostępnych w kraju jest podpisywana umowa offsetowa gwarantująca transfer technologii i zaangażowanie krajowych przedsiębiorstw w produkcję komponentów, serwis i montaż. Energetyka, sektor paliwowy, telekomunikacja i uzbrojenie to równie strategiczne obszary wobec siebie, w których powinno się dążyć do możliwie najwyższej niezależności technologicznej i biznesowej. Takie założenia były podstawą polityki gospodarczej Korei Południowej i Tajwanu, która okazała się skuteczna.

Truizmem jest stwierdzenie, że rozwój technologii w danym kraju powinien być skorelowany z rozwojem biznesowych struktur organizacyjnych, które będą komercjalizowały nowe produkty czy rozwiązania. W Polsce kuleje przede wszystkim obszar wdrożeń produkcyjnych, a finansowanie przez państwo badań naukowych dotyczących tego obszaru okazuje się marnotrawieniem publicznych pieniędzy. Ogromnym problemem jest też nadzór właścicielski. Kultura polityczna polskich elit jest wyjątkowo niesprzyjająca dla rozpoczynania przez państwo nowych przedsięwzięć gospodarczych, o czym świadczą negatywne doświadczenia z komercjalizacją azotku galu i grafenu oraz rozwijaniem gazomobilności opartej na CNG i LNG.

Stojąc u progu transformacji energetycznej wymuszonej starzeniem się bloków energetycznych i zmianą międzynarodowego otoczenia regulacyjnego, należy mieć na uwadze otwarcie polskiego bilansu energetycznego na te technologie, które już istnieją lub które można opanować nie tylko od strony naukowej, lecz także produkcyjnej. Nie ulega wątpliwości, że polski miks energetyczny w dużej mierze będzie oparty w dalszym ciągu na węglu kamiennym, brunatnym, gazie ziemnym, biomasie i energii wody. Pojawiła się już w nim energia wiatru, a należy również rozważyć wprowadzenie energii jądrowej. W ocenie autora przy wyborze między dwiema technologiami o zbliżonym koszcie (np. elektrownie wiatrowe na morzu i elektrownie jądrowe) należy kierować się większym udziałem krajowych przedsiębiorstw w realizacji tych inwestycji, co niezaprzeczalnie przemawia na korzyść energii wiatrowej. Minimalizacja ryzyka przedłużającej się budowy, przekraczanych kosztorysów, a może nawet wstrzymania budowy, powinna przekonywać polskie władze do uznania, że energia jądrowa to dla Polski zbyt złożony projekt. Zwłaszcza, że już raz wstrzymano budowę takiej elektrowni w Żarnowcu, a harmonogram przyjęty 28 stycznia 2014 r. przez Radę Ministrów w *Programie polskiej energetyki jądrowej* został już, po zaledwie czterech latach, przekroczony. Niestety, w chwili obecnej Polska podąża szlakiem wytyczonym

przez Brazylię, która jest modelowym przykładem niedojrzałej polityki energetycznej, dlatego warto przedstawić jej program atomowy.

Budowa pierwszej brazylijskiej elektrowni atomowej rozpoczęła się w 1971 r. w Angra dos Reis, miejscowości pozbawionej tradycji przemysłowych, oddalonej o 130 km od Rio de Janeiro, 220 km od São Paulo i 350 km od Minas Gerais. Inwestorem był państwowy koncern energetyczny, a dostawcą technologii amerykański Westinghouse. Pierwszy blok, Angra 1 o mocy 657 MW, udało się ukończyć po 14 latach, w 1985 r. po dwóch procesach sądowych i licznych niedociągnięciach stwierdzonych po obu stronach. Umowa z firmą Westinghouse zakładała budowę elektrowni pod klucz, ale bez przekazania stronie brazylijskiej najważniejszych technologii (w tym wzbogacania uranu, a więc produkcji paliwa do własnej elektrowni). W związku z tym już w 1975 r. Brazylijczycy podpisali umowę o współpracy z niemieckim Siemensem, który oprócz budowy kolejnych bloków miał przekazać technologię produkcji paliwa jądrowego. Rozpoczęto budowę dwóch reaktorów bazujących na technologii Siemensa, jednak z powodu braku środków, ich budowa została w latach 1986–1995 wstrzymana. Dopiero w 2000 r. udało się ukończyć budowę reaktora Angra II. Przyspieszenie nastąpiło po *black-oucie* z 1999 r., spowodowanym wstrzymaniem pracy elektrowni wodnych (dostarczających większość prądu brazylijskim odbiorcom) z powodu suszy. Budowa trzeciego reaktora, rozpoczęta w 1984 r., jest kontynuowana od 2009 r. we współpracy z francuską Arevą, mimo zapowiedzi sprzed dwóch lat, że Brazylia osiągnie całkowitą samodzielność technologiczną w wydobyciu i wzbogacaniu uranu, przy budowie elektrowni, w wytwarzaniu prądu i utylizowaniu odpadów nuklearnych. Na marginesie warto wspomnieć, że w Brazylii znajdują się znaczne złoża uranu, ponad 5 proc. światowych zasobów, więc ten kraj jest w sposób naturalny predestynowany do wykorzystania energii jądrowej (w przeciwieństwie do Polski)[10]. Pomimo ambitnych planów z lat 60. XX w. i cyklicznie potwierdzanych perspektyw budowy co najmniej trzech elektrowni atomowych, dopiero w najbliższych latach zostanie zakończona budowa pierwszej z nich, po blisko 50 latach od rozpoczęcia procesu inwestycyjnego.

Niewątpliwie Brazylia jest dzisiaj dużo bardziej zaawansowana technologicznie w rozwoju energetyki jądrowej niż Polska. Jednak droga, jaką przeszła Brazylia – koszty na poziomie kilkunastu miliardów dolarów wydanych na przestrzeni 50 lat – nie napawa optymizmem i nie zachęca do podjęcia przez Polskę tych samych wyzwań. Pozyskiwanie technologii jądrowej od zagranicznego partnera w przypadku państwa postkolonialnego, jakim jest Polska, o słabej strukturze instytucjonalnej, rynkach finansowych, niestabilnym systemie politycznym i nieugruntowanej kulturze politycznej, będzie najprawdopodobniej projektem skazanym z góry na porażkę. Dla Polski takim doświadczeniem (choć w dużo mniejszej skali) była budowa gazoportu w Świnoujściu. Wykonawca tej inwestycji, włoski Saipem, prze-

[10] Zob. *Angra-3 PWR Nuclear, Brazil*, http://www.power-technology.com/projects/angranuclear/ [dostęp: 22 VIII 2017].

kroczył zarówno budżet inwestycji, jak i harmonogram oddania jej do użytku. Taki sam los spotyka w ostatnich latach większość inwestycji jądrowych prowadzonych przez firmy zachodnie (Olkiluoto w Finlandii, Hinkley Point w Wielkiej Brytanii oraz w USA – Vogtle w Georgii i Virgil C. Summer w Południowej Karolinie). Warto również mieć świadomość przeszkód, jakie napotyka Słowacja posiadająca już cztery reaktory jądrowe, a więc mająca doświadczenie w wykorzystaniu technologii atomowej. Słowacja kontynuuje rozpoczętą w 1986 r. – i wznowioną po 16 latach przerwy w 2008 r. – budowę dwóch dodatkowych bloków w elektrowni Mochovce. W 2017 r. przedłużono harmonogram o kolejne sześć lat i po raz czwarty podniesiono szacunkowe koszty tej inwestycji, które przekroczyły już dwukrotnie pierwotną wysokość. Są to środki zamrożone na bardzo długi czas, bez generowania dodatnich przepływów finansowych. Jest to ryzyko, na które należy być szczególnie uwrażliwionym.

Koszt 1 MW zainstalowanego w elektrowni jądrowej ciągle rośnie, natomiast elektrowni wiatrowej na morzu – nieustannie spada. Być może – kierując się zasadą oparcia bezpieczeństwa energetycznego na własnych zasobach źródeł energii (odnawialnych i kopalnych) oraz na własnych technologiach wytwarzania energii elektrycznej – w Polsce szybciej mogłaby powstać firma produkująca turbiny wiatrowe (domykając tym samym łańcuch produkcyjny wiatraków), niż opanowano by technologię wykorzystania energii atomowej. Tym samym można byłoby uniknąć ryzyka wzrostu kosztów oraz przedłużania terminów oraz przyszłych awarii i problemów związanych ze składowaniem radioaktywnych odpadów. Decyzja rządu Republiki Federalnej Niemiec o odejściu od atomu powinna być dla Polski przestrogą przed wkraczaniem na ścieżkę energii atomowej. Dwie firmy prowadzące w chwili obecnej projekty budowy farm wiatrowych na Bałtyku (Polenergia 1200 MW i PGE Energia Odnawialna 1040 MW) przewidują, że moc farm będzie równa mocy wytworzonej przez dwa spośród trzech planowanych na Pomorzu bloków atomowych. W 2017 r. koszt budowy instalacji o mocy 1 GW w elektrowni jądrowej przekroczył już (w przypadku technologii francuskiej i amerykańskiej) koszt takiej samej inwestycji w wiatraki na morzu. Zaletą wiatraków są niższe koszty eksploatacji, krótszy czas budowy, mniejsze ryzyko awarii i zerowy koszt paliwa. Wadą jest brak sterowalności i niższy współczynnik wykorzystania mocy zainstalowanej. To źródło energii wymaga zatem uzupełnienia źródłem rezerwowym (optymalnie – gazowym), które jest najtańsze na poziomie inwestycji (CAPEX) i najdroższe w eksploatacji (OPEX). Należy jednak pamiętać, że reaktory jądrowe również mają bardzo niski współczynnik elastyczności: w godzinach nocnych przy niskim zapotrzebowaniu na prąd mogą zmniejszyć swoją produkcję o zaledwie 10 proc. w stosunku do mocy zainstalowanej. Argumentem, który powinien przeważyć w procesie decyzyjnym o nowym miksie energetycznym dla Polski, powinna być zatem możliwość stosowania krajowych technologii i zaangażowania polskich dostawców instalacji wytwarzania. Już dzisiaj komponentów do budowy morskich farm wiatrowych dostarcza polski przemysł stoczniowy, m.in. Stocznia Remontowa Nauta S.A. i Energomontaż-Północ Gdynia SA. Najważniejszym

komponentem, a jednocześnie jedynym, jaki musi być importowany, jest turbina. Jednak to i tak znacznie mniejsza część kosztów inwestycyjnych, która wypłynęłaby za granicę niż w przypadku elektrowni jądrowej. Utrzymanie przepływu kapitału, jaki pochłonie transformacja polskiej energetyki, będzie decydowało o przejściu z grona krajów rozwijających się do grona krajów rozwiniętych. Kluczem do rozwoju jest bowiem wzmacnianie pozycji krajowych przedsiębiorstw w zakresie wysokomarżowej produkcji przemysłowej. A taką właśnie jest sektor wydobycia surowców i wytwarzania energii elektrycznej. Jest to szansa, której polska polityka przemysłowa nie może przeoczyć i zmarnować.

Bibliografia:

Angra-3 PWR Nuclear, Brazil, http://www.power-technology.com/projects/angranuclear/ [dostęp: 22 VIII 2017].

Budowane i planowane elektrownie, http://www.rynek-energii-elektrycznej.cire.pl/st,33,335,tr,145,0,0,0,0,0,budowane-i-planowane-elektrownie.html [dostęp: 16 VIII 2017].

Elastyczność w energetyce – wyzwania stojące przed Polską, http://nowa-energia.com.pl/2017/03/30/elastycznosc-w-energetyce-wyzwania-stojace-przed-polska/ [dostęp: 20 VII 2017].

Godusławski B., *Prywatyzacyjne fakty i mity. Do dzisiaj nie wiemy, ile firm sprzedaliśmy*, http://biznes.gazetaprawna.pl/artykuly/1087293,prywatyzacyjne-fakty-i-mity.html [dostęp: 25 XI 2017].

Gospodarka paliwowo-energetyczna w latach 2014 i 2015, Główny Urząd Statystyczny, Warszawa 2016, http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5485/4/11/1/gospodarka_paliwowo_energetyczna_2014_2015.pdf [dostęp: 12 VI 2017].

https://www.pse.pl/uslugi-dsr-informacje-ogolne [dostęp: 8 VI 2018].

Kasztelewicz Z., Tajduś A., Słomka T., *Węgiel brunatny to paliwo przyszłości czy przeszłości?*, w: *Węgiel brunatny gwarantem bezpieczeństwa energetycznego* (materiały pokonferencyjne), Kraków 2016, s. 225–254.

Kielichowska I., Haesen E., Sach T., *Flexibility Tracker Country Report Poland*, http://www.leonardo-energy.org/resources/503/flexibility-tracker-country-report-poland-5814f41cb7050 [dostęp: 12 VII 2017].

Malko J., *Energetyka japońska. Jak radykalna transformacja?*, „Energetyka" 2013, nr 6; także http://www.cire.pl/pliki/2/energ_japonska.pdf [dostęp: 18 VIII 2017].

Program dla sektora górnictwa węgla kamiennego w Polsce, Ministerstwo Energii, Warszawa 2016.

Abstrakt

Na bezpieczeństwo energetyczne składają się cztery czynniki, których łączne osiągnięcie pozwala mówić o zaistnieniu stabilnych ram sektora energetycznego. Pierwszym jest niezależność pozyskania źródeł energii na terenie własnego kraju, drugim stabilność sieci elektroenergetycznej i przesyłu paliw, trzecim dywersyfikacja zarówno źródeł zagranicznych dostaw surowców energetycznych, jak i źródeł wytwarzania energii na terenie kraju, czwartym zaś – niezależność technologiczna, czyli krajowa własność technologii wytwarzania energii. Autor koncentruje się na czwartym składniku bezpieczeństwa energetycznego, wskazując, że Polska ma rozwinięty przemysł na potrzeby wydobycia węgla kamiennego i brunatnego, budowy elektrowni węglowych, wiatrowych i wodnych, ale nie ma krajowego producenta generatorów elektrycznych: zarówno turbin parowych, jak i turbin wiatrowych. Najmniejszy potencjał polskie firmy mają w zakresie wybudowania elektrownii jądrowych, dlatego ich budowa skutkowałoby wypłynięciem znacznych środków finansowych poza granice kraju.

Słowa kluczowe: bezpieczeństwo energetyczne, miks energetyczny, niezależność energetyczna, gospodarka, energetyka.

Krzysztof Tylutki

Informacja masowego rażenia – OSINT w działalności wywiadowczej

Gdzie jest mądrość, którą straciliśmy w wiedzy?
Gdzie jest wiedza, którą straciliśmy w informacjach?[1]
Gdzie są informacje, które straciliśmy w bitach…

We współczesnym świecie, określanym jako cywilizacja informacyjna, surowcem strategicznym staje się informacja oceniana jako wartość stanowiąca kapitał, nie tylko intelektualny. Nie bez powodu mówi się, że ten ma władzę, kto ma wiedzę, a w węższym rozumowaniu – informacje. Należy zgodzić się z Jamesem Gleickiem, że informacja jest wszędzie, rządzi światem, jest jego krwią i paliwem[2]. Zgromadzenie Ogólne Organizacji Narodów Zjednoczonych w 2016 r. wydało zalecenia w formie rezolucji, aby dostęp do Internetu, który należy uznać za największe źródło informacji, był traktowany na równi z prawem do życia i jako jedno z podstawowych praw człowieka[3]. Informacja staje się elementem wojny informacyjnej, współczesną bronią mającą globalny zakres rażenia, służącą do osiągnięcia przewagi nad przeciwnikiem, określonych celów strategicznych czy w końcu – dominacji w środowisku bezpieczeństwa. Glynn Harmon przyjmuje, że informacja jest rodzajem metaenergii, która porusza większe ilości energii i decyduje o żywiołowości działań podejmowanych przez człowieka[4]. Tę zależność dostrzegł generał John Shalikashvili, który stwierdził, że dopóki wiadomość o zwycięstwie nie pojawi się w źródłach otwartych, w telewizji CNN, dopóty nie uzna, że wygrał wojnę.

Pojęcie informacja jest złożone i występuje w wielu dyscyplinach naukowych. Po raz pierwszy zostało użyte pod koniec XIX wieku przez austriackiego uczonego Ludwiga Boltzmanna do określenia zmian zachodzących w procesach fizycznych. Za ojca teorii informacji uznaje się jednak amerykańskiego matematyka Claude'a E. Shannona, który uważał, że informacja to wybór możliwych opcji. Zdefiniował on jednostkę miary informacji jako **bit**, czyli taką ilość informacji, jaka jest niezbędna do dokonania wyboru między dwiema jednakowo prawdopodobnymi, wzajemnie wykluczającymi się możliwościami. Międzynarodowa norma ISO podaje, że informacja to dane,

[1] Th.S. Eliot, *Choruses from the Rock*, London 1934, https://ww.bayes.it/pdf/Choruses_FromTheRock.pdf [dostęp: 19 VI 2018] – tłum. aut.

[2] J. Gleick, *Informacja – bit, wszechświat, rewolucja*, Kraków 2012, s. 14.

[3] Zob. *Report of the Human Rights Council on its thirty-second session*, General Assembly United Nations, Human Rights Council, Thirty-second session, A/HRC/32/L.20, 14 XI 2016.

[4] Zob. G. Harmon, *The measurement of information*, „Information Processing and Management" 1984, nr 1–2.

które są przetwarzane, organizowane i skorelowane w celu nadania im znaczenia[5]. Dotyczy faktów, pojęć, przedmiotów, zdarzeń, pomysłów oraz procesów[6]. Piotr Sienkiewicz definiuje informację jako zbiór faktów, zdarzeń lub cech zawarty w wiadomości, podany w formie pozwalającej odbiorcy na ustosunkowanie się do zaistniałej sytuacji i podjęcie odpowiednich działań umysłowych lub fizycznch[7]. Informacja, jak słusznie dostrzega się w słowniku Merriam-Webster, to po prostu wiedza uzyskiwana od innych lub na studiach, przez zastosowanie obserwacji czy badań. Zgodnie z definicją *Słownika Języka Polskiego*[8] informacje to w zasadzie dane wywiadowcze. Pełne zrozumienie tego pojęcia jest możliwe dzięki wyjaśnieniu szczególnych funkcji informacji:

- **ilustrującej** – opisującej rzeczywistość (informacja jest jej obrazem);
- **decyzyjnej** – motywującej do działania;
- **sterującej** – budującej systemy informatyczne, bazy wiedzy stanowiące podstawy planowania i podejmowania optymalnych i racjonalnych decyzji;
- **progresywnej** – rozwijającej posiadaną wiedzę;
- **kapitałotwórczej** – uzależniającej od środków finansowych, urządzeń, ludzi oraz ich wiedzy;
- **kulturotwórczej** – zaspokajającej duchowe potrzeby człowieka;
- **komunikacyjnej** – umożliwiającej uczestnictwo w życiu społecznym;
- **integracyjnej** – sprzyjającej rozwojowi relacji międzyludzkich;
- **ideologicznej** – rozwijającej świadomość udziału społeczeństwa w życiu publicznym państwa;
- **opiniotwórczej** – kształtującej poglądy, opinię publiczną na dany temat[9];
- **informacyjnej** – dostarczającej niezbędnej wiedzy, dzięki czemu poprawia się efektywność pracy analitycznej;
- **koordynacyjnej** – porządkującej i harmonizującej realizację równoległych działań;
- **kontrolnej** – weryfikującej oraz oceniającej jakość i spójność danych, ich funkcjonalność – zgodnie z ustalonymi zasadami bezpieczeństwa.

Na podstawie powyższego zestawienia można uznać, że informacja to po prostu towar, przedmiot wyprodukowany jako rezultat ludzkiej pracy, który ma swoją cenę i odbiorcę. Informacja jest elementem składowym wiedzy człowieka oraz głównym czynnikiem uwzględnianym przy podejmowaniu decyzji i organizowaniu procesów w sferze produkcyjnej. Przyczynia się więc do wytwarzania określonego produktu analitycznego[10]. Aby ten produkt był wartościowy, informacja musi być:

---

[5] ISO 22320:2011, *Social security – Emergency management – Requirements for incident response*, November 2011.

[6] ISO 2382-1:1993, *Information technology – Vocabulary*, Part 1: *Fundamental terms*, November 1993.

[7] P. Sienkiewicz, *10 wykładów*, Warszawa 2005, s. 62.

[8] *Słownik Języka Polskiego*, t. 1–3, M. Szymczak (red.), Warszawa 1978–1981, s. 863.

[9] Zob. B. Stefanowicz, *Informacja. Wiedza. Mądrość*, seria: Biblioteka Wiadomości Statystycznych, t. 66, Warszawa 2013, s. 42–45.

[10] Tamże, s. 36.

- **dokładna** – musi w sposób wiarygodny odzwierciedlać rzeczywistość, tak aby stanowiła dla produktu analitycznego realną wartość;
- **aktualna** – dostępna w czasie umożliwiającym właściwe działanie decydenta;
- **kompletna** – musi dostarczać decydentowi wszelkich potrzebnych mu faktów i szczegółów, przedstawiać pełny obraz sytuacji, bez jego zniekształcania;
- **istotna** – przydatna dla decydenta w realizacji konkretnych potrzeb zaistniałych w szczególnych warunkach.

Każde źródło informacji ma właściwe sobie cechy i jest postrzegane indywidualnie przez poszczególne osoby. Informacje, które można znaleźć w internecie, są charakteryzowane jako godne zaufania i dostępne w dowolnym czasie, informacje telewizyjne jako bezstronne i bieżące, a informacje prasowe jako wyważone i rzetelne[11]. Z badań Krystyny Polańskiej wynika, że najważniejszym elementem przy ocenie wiarygodności danej informacji są: zaufanie do źródła, które je podaje, aktualność, logiczne powiązanie informacji z innymi faktami lub wiadomościami oraz przekazywanie takiej samej informacji przez kilka niezależnych źródeł[12]. Oprócz informacji wiarygodnych, rzetelnych i aktualnych pojawiają się także informacje mylące, czasem nawet świadomie wprowadzające w błąd. Należy pamiętać, że ilość informacji może nie mieć nic wspólnego z ich wiarygodnością, a wręcz przeciwnie – zdarza się, że wiele z nich jest nieprawdziwych, dezinformujących[13], przez co zmniejszają swoją wartość. Widoczna jest tutaj manipulacja informacją, która jest wyrażana w jej ocenach, selekcji i doborze, co jest spowodowane tym, że dzięki specyfice Web 2.0 informacje mogą być zamieszczane przez każdego uczestnika wirtualnej społeczności. Anonimowym edytorom Wikipedii zdarzyło się uśmiercić żyjących: senatora Teda Kennedy'ego i polityka Roberta Byrda. Z kolei artykuł o wojnie domowej w Syrii, który ukazał się w 2012 r., ze względu na dynamicznie zmieniającą się sytuację w regionie był ponad 7,5 tys. razy edytowany przez użytkowników Wikipedii, co utrudniało rzetelną ocenę konfliktu. Nie jest to jednak rekord, życiorys prezydenta USA Georga W. Busha był w 2005 r. aktualizowany ponad 20 tys. razy.

Ze względu na czas uzyskania i możliwości wykorzystania informacji w procesie decyzyjnym można wyróżnić:

- **informację relacjonującą** – opisującą zdarzenie, które zaistniało lub dzieje się w chwili obecnej;
- **informację wyprzedzającą** – ukazującą planowane czynności, działania, które

[11] K. Stankiewicz, *Wpływ Internetu na percepcję wiarygodności informacji*, w: L. Haber, *Społeczeństwo informacyjne. Wizja czy rzeczywistość?*, Kraków 2004, s. 409.

[12] Zob. K. Polańska, *Informacja, jej wiarygodność i co z nich dla nas wynika*, w: *Informacja – dobra lub zła nowina*, A. Szewczyk (red.), Szczecin 2004.

[13] Vladimir Volkoff definiuje dezinformację jako czynność podejmowaną z zaangażowaniem wielu środków, powadzoną w sposób systematyczny i fachowy, zawsze za pośrednictwem mass mediów i adresowaną do opinii publicznej. Dezinformacja ma na celu realizację konsekwentnego programu, zmierzającego do zastąpienia w świadomości, a przede wszystkim w podświadomości, mas będących przedmiotem tych działań poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa za korzystne dla siebie, zob. V. Volkoff, *Dezinformacja: oręż wojny*, Warszawa 1991, s. 6–8.

są w obszarze zainteresowania; jest to najcenniejsza informacja w procesie podejmowania decyzji;

- **informację weryfikującą** – potwierdzającą posiadaną wiedzę na dany temat, zjawisko, zdarzenie.

Zapotrzebowanie na informacje nie jest wartością stałą, w zależności od sytuacji wygląda różnie, jego zróżnicowanie jest szczególnie widoczne na różnych poziomach podejmowania decyzji, począwszy od taktycznego czy operacyjnego, po strategiczny. Im wyższy szczebel zarządzania, tym większa koncentracja informacji i szerszy ich zakres tematyczny. Na niższych poziomach kierowania informacje powinny być bardziej szczegółowe i mieć węższy zakres tematyczny. Taki rozkład informacji jest nazywany „odwróconą piramidą informacyjną". Oznacza on, że piramida informacyjna charakteryzująca ilość, szczegółowość i zakres informacji jest odwrotnością piramidy strukturalnej, opisującej obowiązki, uprawnienia i odpowiedzialności decydentów[14].

Ludzkość nieustannie wytwarza coraz więcej informacji. Świat cyfrowy, w którym żyjemy – zdaniem zastępcy dyrektora CIA Andrew Hallmana – podważa zasadę konspiracji działań wywiadowczych. Powoduje, że coraz trudniej jest utrzymać w tajemnicy oficera pod przykryciem, kiedy każdy ma w kieszeni studio telewizyjne[15]. Dynamika wzrostu zbioru danych Big Data[16], tj. zbioru danych o dużej objętości, różnorodności, zmienności i wartości – nieprzerwanie postępuje (od 40 do 60 proc. w ciągu roku). Zbiór osiąga rozmiary, których analiza jest nie lada wyzwaniem dla analityków. W połowie lat 80. XX w., gdy ośrodki naukowe i uniwersytety zaczęły doceniać możliwości płynące z Internetu, jedynie 6 proc. materiałów było zdigitalizowanych. Obecnie już niemal 99 proc. dorobku kultury i życia ma postać cyfrową. Ocenia się, że w 1992 r. powstawało na świecie 100 gigabajtów (GB)[17] danych dziennie, w 1997 r.tyle samo wytwarzano już w godzinę, a w 2002 r. – w ciągu sekundy. Dziś uznaje się, że co sekundę zostaje wytworzonych 50 tys. GB danych. Według szacunków w 2017 r. cyfrowy wszechświat osiągnął rozmiary 16 zettabajtów (ZB), a według prognoz Oracle Corporation do 2020 r. ludzkość wygeneruje w sieci ponad 45 ZB danych. Oznacza to, że na jednego mieszkańca kuli

[14] B. Nogalski, B.M. Surawski, *Informacja strategiczna i jej rola w zarządzaniu przedsiębiorstwem*, w: *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystywanie i ochrona (wybrane problemy teorii i praktyki)*, R. Borowiecki, M. Kwieciński (red.), Kraków 2003, s. 205–206.

[15] P. Tucker, *Meet the Man Reinventing CIA for the Big Data Era*, https://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/ [dostęp: 3 I 2018].

[16] Big Data definiuje się za pomocą czterech charakterystycznych czynników opisujących zbiory informacji, zwanych 4 V, tj.: **Volume** (ilość danych), **Variety** (różnorodność analizowanych danych i informacji), **Velocity** (przetwarzanie danych w czasie rzeczywistym) i **Value** (wartość, jaką możemy uzyskać z połączenia wszystkich poprzednio wymienionych czynników wspomagających proces analityczny i decyzyjny). Zob. T. Słoniewski, *Od BI do „Big Data*", w: *Nowa twarz Business Intelligence*, R. Jesionek (red.), http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf, s. 8–10, [dostęp: 7 V 2018].

[17] Jednostka używana w informatyce oznaczająca miliard (10^9) bajtów. W tekście występują jednostki używane w informatyce: terabajt, TB (10^{12}), petabajt, PB (10^{15}), eksabajt, EB (10^{18}) i zettabajt, ZB (10^{21}) – przyp. red.

ziemskiej przypadnie ponad 5,2 GB danych. Z kolei The Digital Universe – IDC szacuje, że w 2020 r. zostanie wytworzonych 44–47 ZB danych, a prawie 40 proc. informacji w świecie cyfrowym będzie dostępnych w *cloud computing*[18]. Podaje się ponadto, że w 2021 r. zarządzanie danymi wzrośnie o 50 proc. w stosunku do 2011 r.[19] Obliczono, że do 2025 r. zostanie wygenerowanych 163 ZB informacji.

Ocenia się, że ilość informacji cyfrowych wytworzonych do 2007 r. miała wielkość 281 EB, która na przestrzeni kilku lat nieprzerwanie rosła, i w 2011 r. wyniosła w przybliżeniu 1,8 ZB. Do takich wniosków doszli autorzy raportu[20] opublikowanego w 2014 r. przez Gabinet Prezydenta Stanów Zjednoczonych. W kategoriach ilościowych taka wielkość informacji zapełniłaby 57,5 mld urządzeń iPad z pamięcią 32 GB. Obrazując o zjawisko, można je porównać do zbudowania Wielkiego Muru Chińskiego o dwukrotnie większej średniej wysokości niż oryginał. Można również znaleźć informacje, że w 2011 r. w skali globalnej wytworzono 20 mld razy więcej informacji, czyli 988 EB, niż wszystko, co do tej pory napisano w historii ludzkości[21]. Jest to tyle informacji, ile obecnie obywatel rozwiniętego państwa ma do dyspozycji w ciągu jednej godziny, a dwa pokolenia wstecz – przez całe swoje życie. W 2013 r. wygenerowano już 4 ZB informacji w skali światowej. Ta liczba odpowiada sumie zdjęć zrobionych co sekundę przez każdego mieszkańca Stanów Zjednoczonych przez ponad cztery miesiące życia[22]. Dwa lata później ich wielkość wzrosła do 12 ZB. Amerykanie przeprowadzili badania, które pozwoliły wyliczyć, że w 2008 r. ludzkość wykorzystała średnio 34 GB informacji i 100,500 tys. słów dziennie. Około 35 proc. z nich pochodziło z TV, w tym 10 proc. z filmów, a 55 proc. z gier komputerowych. W stosunku do lat 80. XX w. wykorzystanie słów wzrosło o 140 proc., natomiast przyrost informacji cyfrowych zwiększył się o 350 proc. W 2008 r. media wykorzystały łącznie 3,6 ZB informacji i 1,080 trylionów (czyli ok. 1 EB) słów dziennie[23].

Tempo, w jakim następuje przyrost danych, wynika z potrzeby powszechnej komunikacji i rozwoju obszaru zwanego Internetem rzeczy (ang. *Internet of Things*, IoT), w którego zakresie coraz więcej urządzeń będzie gromadziło i przetwarzało dane w Internecie. W ciągu kilku lat ludzkość czeka eksplozja danych. Sami użytkownicy również uczestniczą w powielaniu informacji, kopiując wszelkiego rodzaju treści i komentarze oraz kwalifikując je jako kolejne, wtórne, źródło in-

[18] Czyli w tzw. chmurze. IBM definiuje to zjawisko jako model wykorzystywania i styl przetwarzania, w którym dane i zasoby IT są dostarczane w formie usług.

[19] Zob. J. Gantz, D. Reinsel, *Extracting Value from Chaos*, w: *IDC analyze the future,* https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf [dostęp: 4 VI 2018].

[20] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, The White House, Washington DC, May 2014, s. 7–8; informacje podane w raporcie pochodzą z publikacji: J. Gantz, D. Reinsel, *Extracting Value*…; M. Meeker, L. Yu, *Internet Trends*, Washington 2013.

[21] Zob. M. Karnowski, E. Mistewicz, *Anatomia władzy*, Warszawa 2010, s. 114.

[22] *Big Data: Seizing Opportunities*…, s. 8.

[23] R. Bohn, J. Short, *Measuring Consumer Information*, „International Journal of Communication" 2012, nr 6, s. 980–1000.

formacji. Jednocześnie nie podają źródła pierwotnego. To zjawisko jest nazywane „efektem echa" (ang. *echo effect*).

Jak zauważył noblista Herbert Simon, informacja skupia uwagę tych, którzy ją przyjmują. Może się przy tym pojawić stan napięcia, tzw. dysonans poznawczy, jeśli do odbiorcy dotrą informacje niezgodne z jego poglądami czy przekonaniami. Powoduje on, że te informacje się ignoruje, przypisuje się im mniejszą wagę lub je zniekształca. Każdy ma inny poziom absorbowania informacji, zależny w dużym stopniu od ilości i jakości informacji apriorycznych[24]. Z czasem pojawia się syndrom zmęczenia, nazwany z języka angielskiego *attention crash*, który ma związek nie z brakiem umiejętnej selekcji prostych komunikatów, a z ich zrozumieniem. J. Gleick nazywa ten czynnik *Devil of Information Overload*, czyli pojawiającym się natłokiem informacji (albo: *To much information*, TMI)[25]. Dzieje się tak również dlatego, że hipokamp[26], czyli „dysk twardy" ludzkiego mózgu, ma swoje biologiczne ograniczenia. W 1986 r. Thomas K. Landauer w swoich pracach zakładał, że mózg człowieka jest w stanie przechować ok. 11 TB informacji[27]. Według współczesnych badań ekspertów ze StorageCraft mózg człowieka może zapisać od 100 TB do 2,5 PB danych. Dla porównania, gdyby „ludzki dysk twardy" pracował jak cyfrowy rejestrator wideo w telewizorze, to ta wielkość wystarczyłaby do przechowania 3 mln godzin filmów. Aby wykorzystać całą pamięć, należałoby nieprzerwanie przez ponad 300 lat nie wyłączać telewizora. Natomiast badania amerykańskich uczonych pokazują, że biologiczny „komputer" człowieka jest w stanie przechować nie więcej niż około 1 PB danych. Według badań neurologów przeprowadzonych w ostatniej dekadzie przeciętny człowiek ma ponad 30 tys. myśli dziennie.

Nadmiar informacji sprawia ludziom trudności zarówno z ich przetworzeniem, jak i zrozumieniem, przez co przyczynia się do formułowania błędnych ocen. Dlatego trudno jest wybrać odpowiedniego analityka do danego zadania. Ogrom informacji przekazywanych przez pułkownika radzieckiego wywiadu wojskowego (GRU) Olega Pieńkowskiego, który podjął współpracę z Zachodem, spowodował, że Amerykanie (CIA) i Brytyjczycy (MI6) musieli zaangażować łącznie 30 tłumaczy i analityków[28]. Również niedokładny zapis rozmów oficerów CIA z agentem KGB Jurijem Iwanowiczem Nosenką, oferującym pomoc Zachodowi, spowodował, że został on uznany za kłamcę i wykluczony jako potencjalne, cenne źródło informacji. Wnioski zawarte w dokumencie analitycznym nie pozwoliły na dokonanie obiektywnej oceny radzieckiego kapitana. Większość jego zeznań została spisana na podstawie zapamiętanych wypowiedzi, które w połączeniu z brakami lingwistycznymi badających były inter-

[24] S.E. Zločevskij i in., *Informacja w badaniach naukowych*, Warszawa 1972, s. 231.

[25] J. Gleick, *Informacja – bit, wszechświat*…, s. 16.

[26] Element układu limbicznego u człowieka odpowiedzialny za pamięć, odgrywa główną rolę przy przenoszeniu informacji w mózgu, za: https://pl.wikipedia.org/wiki/Hipokamp [dostęp: 11 VI 2018] – przyp. red.

[27] T.K. Landauer, *How Much do People Remember? Some Estimates of the Quantity of Learned Information in Long-Term Memory*, „Cognitive Science" 1986, nr 10, s. 477–493.

[28] J. Larecki, *W kręgu tajemnic wywiadu*, Warszawa 2007, s. 157–158.

pretowane przez Amerykanów po macoszemu. Zniekształcono nazwę uczelni, której był absolwentem, i zamiast szkoły średniej marynarki wojennej im. gen. Frunzego, sowieckiego bohatera wojennego, wpisali, że ukończył Akademię Wojskową im. Frunzego, czyli sowieckie West Point. Po przeanalizowaniu obszernych akt archiwum CIA jej były funkcjonariusz John L. Hart stwierdził, że badania i analizy kontrwywiadu były tak długie i zawiłe, że niewielu przełożonych miało czas na przeczytanie i przeanalizowanie uzasadnienia dotyczącego rzekomej dwulicowości Nosenki[29]. Generał Robert Kehler, szef Zintegrowanego Dowództwa Operacyjnego Departamentu Obrony Stanów Zjednoczonych (United States Strategic Command), po latach doświadczeń dostrzegł, że Pentagon tonie w zalewie danych wywiadowczych. Coraz sprawniejsze i liczniejsze satelity zwiadowcze dają amerykańskiemu wywiadowi tyle informacji, że analitycy nie są w stanie ich opracowywać. Ilość danych zwiększyła się w ciągu pięciu lat o 1500 proc., a zdolności ich przetwarzania tylko o 30 proc.[30] Do takich samych wniosków doszedł funkcjonariusz NSA William Binney, który dodał, że gromadzenie przypadkowych informacji sprawia, że funkcjonariusze obciążeni nadmierną ilością danych zarzucili analizę kierunkową na rzecz prostego przeszukiwania baz danych po słowach kluczowych. To daje wiele nic nieznaczących „trafień" zamiast wiedzy o istotnych powiązaniach między tymi informacjami[31]. Być może to było powodem zwłoki Amerykańskiego Urzędu Imigracyjnego w poinformowaniu szkoły lotniczej Huffman Aviation International w Venice na Florydzie, że Mohammed Atta i Marwan Alshehi, dwaj późniejsi zamachowcy na World Trade Center, dostali wizy studenckie. Ta informacja dotarła do szkoły dopiero sześć miesięcy po atakach na WTC. Potwierdzeniem tych wniosków jest to, że 10 września 2001 r. NSA przechwyciła dwie informacje w języku arabskim, w których była mowa o tym, co miało się stać następnego dnia. Dopiero jakiś czas po zamachu na WTC informacje, o których mowa, zostały przetłumaczone. Ponadto w okresie letnim w 2001 r., kilka miesięcy przed 11 września, Osama bin Laden wraz ze swoimi dowódcami udzielił obszernego wywiadu dla Centrum Mediów Bliskiego Wschodu, w którym padły ogólne wskazówki dotyczące planowanych na dużą skalę ataków na amerykańskie obiekty[32]. Niektórzy eksperci szacują, że od 50 do 80 proc. informacji będących w kręgu zainteresowań służb specjalnych krajów zachodnich nie jest publikowanych w jęz. angielskim[33].

[29] J.L. Hart, *Walka wywiadów. Rosjanie w CIA*, Warszawa 2003, s. 155.

[30] T. Costlow*, Kehler raises trial balloon: Put STRATCOM in charge of all GEOINT PED*, http://defensesystems.com/articles/2011/10/19/geoint-kehler-stratcom-geospatial intelligence.aspx [dostęp: 2 V 2018].

[31] R. Koerner, *William Binney: NSA Claim Not to Be Mining Content Is an "Outright Lie"*, https://www.huffingtonpost.com/robin-koerner/nsa-whisteblower-nsa-clai_b_7837806.html [dostęp: 4 V 2018].

[32] P. Bergen, *Why U.S. can't find Osama bin Laden*, http://edition.cnn.com/2010/OPINION/10/19/bergen.finding.bin.laden/ [dostęp: 2 V 2018].

[33] M.M. Lowenthal, *Open Source Intelligence: New Myths, New Realitties*, w: *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, R.Z. George, R.D. Kline (eds.), Lanham 2006, s. 277.

Informacja to potęga wtedy, gdy może być dostępna tam, gdzie jest potrzebna, temu, komu jest potrzebna, i w celu, w jakim jest potrzebna. Natomiast mankamentem jest zbyt duża ilość informacji nieuporządkowanych. Im większe sukcesy osiąga się w gromadzeniu danych, tym bardziej zaczyna się pływać w ich morzu. David Foster Wallace określa to zjawisko mianem „tsunami dostępnych faktów, kontekstów i perspektyw"[34]. W wyniku operacji przeprowadzonej przez CIA na pograniczu dwóch stref okupacyjnych w Berlinie w latach 1954–1955 Amerykanie zarejestrowali 6 mln godzin ruchu telefonicznego oraz 40 tys. godzin rozmów telefonicznych na linii Moskwa–Karlshorst (w Karlshorst mieściła się główna rezydentura KGB działającego na terenie NRD) i Moskwa–Wünsdorf (w Wünsdorf, zgodnie z dostępną literaturą, znajdowała się kwatera główna wojsk radzieckich). Zgromadzone informacje tłumaczono i analizowano jeszcze przez kolejne dwa lata po zakończonych działaniach. Mimo upływu czasu z nadmiarem informacji borykały się następne służby. Kiedy w 1989 r. Niemiecka Republika Demokratyczna przestawała istnieć, Ministerstwo Bezpieczeństwa Państwowego, znane powszechnie jako Stasi (Ministerium für Staatssicherheit), analizowało materiał pochodzący z podsłuchów rozmów telefonicznych (z kontroli operacyjnej) zebrany w połowie lat 80. XX w.[35]

Podczas gromadzenia informacji ogólnodostępnych łatwo stracić orientację, zwłaszcza jeśli ich źródłem jest Internet, którego rozmiary Eric Schmidt oszacował na 5 mln TB. Systematycznie rosnąca liczba wniosków wizowych składana przez cudzoziemców w urzędach ds. imigracyjnych powoduje chaos przy weryfikacji rzeczywistego powodu, z jakiego decydują się oni na zmianę kraju pobytu. Procedura ma charakter administracyjny i w głównej mierze jest skupiona na kompletowaniu dokumentacji dzięki prowadzeniu wywiadu środowiskowego oraz sprawdzeniu przeszłości (tzw. ang. *background checks*). Brak danych o cudzoziemcu lub pobieżna weryfikacja otwartych źródeł informacji dokonana przez służby imigracyjne i FBI uczestniczące w ocenie pobytu takiej osoby pod kątem zagrożeń bezpieczeństwa wewnętrznego kraju pozwoliły na osiedlenie się w Stanach Zjednoczonych Tashfeen Malik. Emigrantka z Pakistanu od kilku lat otwarcie deklarowała na portalu społecznościowym poparcie dla dżihadu oraz głosiła antyamerykańskie hasła. W dniu 2 grudnia 2015 r. wraz z mężem dokonała ataku w ośrodku pomocy niepełnosprawnym w San Bernardino w Kalifornii, w którym zginęło 14 osób, a ponad 20 zostało rannych[36].

Dziewięćdziesiąt procent informacji wywiadowczych pochodzi z otwartych źródeł. Pozostałe dziesięć, które uzyskuje się w sposób bardziej widowiskowy, z utajnionych. Prawdziwym bohaterem pracy wywiadowczej jest Sherlock Holmes, a nie James Bond [37].

---

[34] J. Gleick, *Informacja – bit, wszechświat*…, s. 374.

[35] P. Żuk, *Demokracja pod kontrolą – czyli podsłuch non stop*, http://www.tygodnikprzeglad.pl/demokracja-pod-kontrola-czyli-podsluch-non-stop/ [dostęp: 15 VI 2018].

[36] M. Apuzzo, M.S. Schmidt, J. Preston, *U.S. Visa Process Missed San Bernardino Wife's Zealotry on Social Media*, http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html [dostęp: 6 V 2018].

[37] Cytat za gen. S.V. Wilsonem, dyrektorem Agencji Wywiadu Obronnego USA.

Możliwości płynące z OSINT-u (ang. *open source intelligence*[38]) – powszechnie rozumianego jako tzw. biały wywiad, czyli ogół publicznie dostępnych, jawnych informacji, które każdy w sposób legalny może pozyskać – były doceniane przez ludzkość od zarania dziejów, od czasów pojawienia się zrębów pierwotnej formy komunikacji[39]. Historia wykorzystywania informacji powszechnie dostępnych sięga okresu powstania wywiadu jako narzędzia gromadzenia istotnej wiedzy w celu wspierania procesu decyzyjnego władcy (rządu) w odniesieniu do bezpieczeństwa narodowego i obronności państwa. Środki wykorzystywane do pozyskiwania danych z otwartych źródeł[40] ewoluowały wraz z postępem technologicznym oraz wydarzeniami, a „National Geographic"[41] słusznie uznał je za te, które zmieniły, a nawet zrewolucjonizowały świat. Dostęp do nich zapoczątkowały i upowszechniły środki masowego przekazu[42] – prasa, radio i telewizja. Jednak największe piętno odcisnęła rewolucja komputerowa oraz internetowa umożliwiająca rozwój sieci, a zwłaszcza mediów społecznościowych[43].

[38] OSINT został zdefiniowany m.in. przez Dyrektora Wywiadu Narodowego USA (Director of National Intelligence, DNI) w: *National Defense Authorization Act for Fiscal Lear 2014* [Public Law 113–66 (26 XII 2013 r.)] oraz Wspólnotę Wywiadów Stanów Zjednoczonych (Intelligence Community), w: *Intelligence Community Directive Number 301*, National Open Source Enterprise 2006.

[39] Można wyróżnić trzy etapy analizowania otwartych źródeł informacji określone jako: ***Open Source Data*** (**OSD**) – **dane jawnoźródłowe**, będące niejako w „stanie surowym", pochodzące z pierwotnego źródła w postaci drukowanej, cyfrowej, mające formę zdjęć, nagrań, obrazów satelitarnych itp; ***Open Source Information*** (**OSIF**) – **informacja jawnoźródłowa**, szeroko opracowana, zebrana w jeden dokument, zredagowana, zweryfikowana, poddana filtracji z uwagi na jej prezentację (np. prasa, książki, publikacje, raporty); ***Validated Open Source Intelligence*** (**OSINT-V**) – **zweryfikowany biały wywiad** mający wysoki stopień wiarygodności dzięki analizie informacji pochodzących ze źródeł niejawnych, przeprowadzonej przez analityka. OSINT można rozszerzyć o następujące terminy: ***Open Source Acquisition*** – **pozyskwanie informacji jawnoźródłowej** z dostępnych źródeł otwartych, które wcześniej zostały zgromadzone i przekazane przez badacza; ***Open Source*** – **źródło otwarte**, którym może być zarówno pojedyncza osoba, jak i grupa dostarczająca informacje, sama zaś informacja oraz relacja łącząca ją z podmiotem, w którego kręgu zainteresowań leży jej uzyskanie, nie są objęte klauzulą tajności. Dane ze źródeł otwartych mogą być publicznie dostępne, ale nie wszystkie upublicznione informacje są źródłem otwartym. Pojęcie źródło otwarte odnosi się do środków publicznie dostępnych i nie należy go ograniczać tylko do osób fizycznych. ***Publicly available information*** – **informacje ogólnodostępne**, dane, fakty, instrukcje, materiały opublikowane bądź transmitowane do ogólnego użytku publicznego, prezentowane na żądanie każdego obywatela, uzyskane dzięki obserwacji, usłyszane bądź przekazane na spotkaniach otwartych dla ogółu społeczeństwa.

[40] W ramach OSINT-u można wyróżnić dwa obszary wywiadowcze: 1) ***Social Media Intelligence*** (**SOCMINT**) – skupiony na rozpoznaniu i monitorowaniu profili użytkowników portali społecznościowych i publikowanych przez nich postów oraz zbieraniu informacji z otwartych i zamkniętych grup społecznych, 2) ***Web Intelligence*** (**WEBINT**) – eksplorację danych oraz wyszukiwanie i magazynowanie informacji w Internecie.

[41] Zob. *100 Events That Changed the World*, „National Geographic" 2015, Special Issue.

[42] Radio potrzebowało 30 lat, aby zyskać 50 mln słuchaczy, telewizja 14 lat, aby zgromadzić taką liczbę widzów, Interent natomiast pozyskał taką liczbę użytkowników w ciągu zaledwie czterech lat.

[43] Zdefiniowane przez Howarda Rheingolda pierwotnie jako społeczności wirtualne, czyli

Biały wywiad jest prowadzony zarówno przez struktury wojskowe, jak i cywilne[44]. Jest domeną głównie instytucji państwowych odpowiedzialnych za zapewnianie bezpieczeństwa, ale coraz częściej jest „doceniany" i przez sektor prywatny, i organizacje terrorystyczne. W celu dokładniejszego zrozumienia istoty białego wywiadu należy określić jego role[45]. Biały wywiad:

- stanowi podstawę informacyjną na każdym etapie prowadzonych działań. Dostarcza tła przekazywanych informacji, które w zależności od kontekstu, m.in. społecznego, kulturowego, politycznego, mają różne znaczenie;
- odpowiada na wymagania wywiadowcze oraz informacyjne stawiane przez instytucje, bez konieczności wsparcia specjalistów czy techniki operacyjnej (metod niejawnych);
- pogłębia i weryfikuje dotychczas uzyskaną wiedzę;
- umożliwia decydentowi korzystanie ze wszystkich dostępnych źródeł informacji. przy podejmowaniu decyzji.

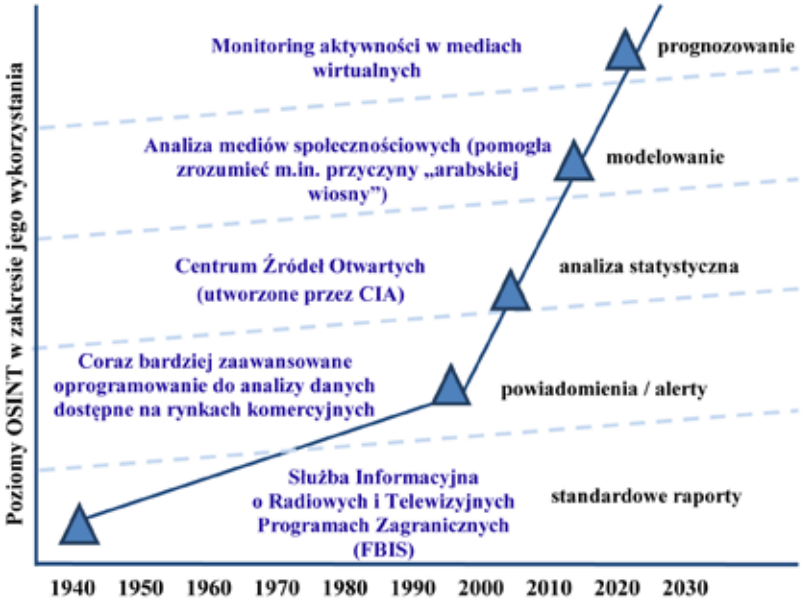
Historia wykorzystywania OSINT-u wiąże się w zasadzie z historią wywiadu Stanów Zjednoczonych. Ten typ wykorzystywania informacji był jednym z głównych źródeł informacji na temat zdolności wojskowych przeciwników oraz ich zamiarów politycznych (wczesne ostrzeganie i prognozowanie zagrożeń). Amerykanie byli pionierami w gromadzeniu danych dzięki rozwojowi zdolności samodzielnego monitorowania, filtrowania, tłumaczenia oraz archiwizacji wiadomości pochodzących z zagranicznych mediów. W monitorowaniu otwartych źródeł informacji, które w początkowej fazie oznaczało śledzenie doniesień prasowych, sektor komercyjny wyprzedzał działania rządowe. Przed profesjonalizacją i formalną instytucjonalizacją wywiadu jako niezbędnego elementu narodowego aparatu bezpieczeństwa w drugiej połowie XX wieku zbieranie i analizowanie otwartych źródeł przez rząd ewoluowało od procesu mało uporządkowanego do czynności o znaczeniu strategicznym, wymagających użycia określonych metod i narzędzi. Na schemacie przedstawiono kierunek zmian OSINT-u oraz wykorzystywanie jego głównych obszarów, pozwalające na opracowanie odpowiedniego produktu analitycznego w działalności wywiadowczej Stanów Zjednoczonych na przestrzeni wieków XX i XXI.

---

grupy ludzi, którzy mogą lub nie mogą spotkać się twarzą w twarz i którzy wymieniają myśli (idee) za pośrednictwem klawiatury i sieci. Ich cechą charakterystyczną jest to, że każdy ich uczestnik może stać się jednostką aktywną, przywódczą czy destrukcyjną. Nieobowiązująca zasada więzi sprzyja wolności słowa, debacie oraz ekshibicjonizmowi życia prywatnego czy zawodowego na forum publicznym. Zob. H. Rheingold, *The Virtual Community. Homesteading on the Electronic Frontier*, New York 1994.

[44] Poza tradycyjnymi otwartymi źródłami informacji należą do nich także: komercyjne bazy danych, takie jak informatory gospodarcze, statystyczne, publiczne rejestry, tzw. szara literatura, czyli raporty robocze, nieoficjalne dokumenty rządowe, przedruki, studia i badania rynkowe, raporty badawcze, indywidualni eksperci, wykładowcy akademiccy, literatura naukowa, materiały z konferencji i sympozjów, opracowania ośrodków badawczych.

[45] *Open Source Intelligence*, Headquarters, Department of Army, Army Techniques Publication, ATP 2-22.9, Washington, 2012, s. 2-2.



Schemat. Ewolucja wykorzystania możliwości OSINT.

Źródło: Opracowanie własne na podstawie: *Disruptive innovation*. *Case study: Intelligence – Open-source data analytics*, Washington, DC 2012, s. 3.

Wartość źródeł otwartych została dostrzeżona przez Georga Washingtona już w XVIII wieku podczas rewolucji amerykańskiej. Czerpał on aktualne informacje o sile brytyjskich wojsk i aktywności szpiegów z publikacji prasowych oraz wiadomości ogólnie dostępnych[46]. Kilkadziesiąt lat później, w 1808 r., brytyjski książę Wellington w bitwie prowadzonej przeciwko armii Napoleona na Półwyspie Iberyjskim zalecał swoim generałom lekturę codziennej prasy, m.in. dziennika „The Times", w której szeroko opisywano sposób organizacji nowych struktur francuskiej piechoty[47]. W 1863 r. w czasie kampanii gettysburskiej wywiad generała Roberta Lee monitorował ruchy wojsk Unii na północy dzięki śledzeniu doniesień prasowych[48]. W latach 1899–1902 podczas wojny filipińskiej amerykańscy stratedzy wojskowi opierali się na raportach wywiadowczych, które w zasadzie były kopiami artykułów z encyklopedii[49]. W czasie dwóch wojen światowych książki i gazety były źródłem cennych informacji wykorzystywanych przez wywiad wojskowy. Podczas ofensywy we Francji wojska generała

[46] *A Look Back … George Washington: America's First Military Intelligence Director*, https://www.cia.gov/news-information/featured-story-archive/2007-featured-storyarchive/george-washington.html [dostęp: 5 V 2018].

[47] S.D. Gibson, *Exploring the Role and Value of Open Source Intelligence*, w: *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014, s. 13.

[48] E.B. Coddington, *The Gettysburg Campaign: A Study in Command*, New York 1968, s. 19.

[49] B. McAllister Linn, *The Philippine War: 1899–1902*, Lawrence 2000.

George'a Pattona w celu rozpoznania geoprzestrzennego używały map Michelin dostępnych na stacjach benzynowych[50].

W 1939 r. brytyjski rząd zwrócił się do BBC o utworzenie komercyjnego serwisu podsumowującego zagraniczną prasę i audycje radiowe pod nazwą *Digest of Foreign Broadcasts* (*Przegląd Audycji Zagranicznych*), który w późniejszym czasie był nazywany *Summary of World Broadcasts* (*Podsumowanie Wiadomości ze Świata*), a obecnie jest emitowany jako *BBC Monitoring*. W podręczniku BBC z 1940 r. wskazano, że powstanie serwisu miało na celu stworzenie (…) *nowoczesnej Wieży Babel, gdzie słuchano głosów zarówno przyjaciół, jak i wrogów*[51]. W połowie 1943 r. BBC monitorowało dziennie 1,25 mln transmisji. Formalne partnerstwo między BBC i jego amerykańskim odpowiednikiem ustanowiono na przełomie lat 1947/1948 na podstawie porozumienia o pełnej wymianie informacji. W 1948 r. z Lotniczej Jednostki Badawczej (Aeronautical Research Unit) utworzono oddział Amerykańskiej Biblioteki Kongresu (US Library of Congress), który miał zapewnić niestandardowe badania i usługi analityczne wykorzystujące rozległe zasoby biblioteki. Obecnie funkcjonuje on jako Federalny Oddział Badawczy (Federal Research Division)[52].

W 1941 r. decyzją prezydenta Franklina Delano Roosevelta utworzono w USA Służbę Monitoringu Nadawców Zagranicznych (Foreign Broadcast Monitoring Service). Była ona odpowiedzialna za monitorowanie, tłumaczenie, transkrypcję i analizę informacji pochodzących z audycji radiowych państw Osi. Do końca 1942 r. służba osiągnęła sporą wydajność. Tłumaczyła ponad 500 tys. słów dziennie, które pochodziły z 25 stacji radiowych nadających w 15 językach[53]. W ramach powołanego Międzyresortowego Komitetu Nabywania Zagranicznych Publikacji (Interdepartmental Committee for the Acquisition of Foreign Publications) Amerykanie monitorowali i analizowali także prasę i książki ukazujące się w czasie wojny poza granicami kraju. Pod koniec wojny przesyłano tygodniowo do analizy astronomiczną liczbę 45 tys. stron tekstu. W ostatnich dniach wojny w Komitecie zgromadzono 300 tys. fotografii, 350 tys. numerów czasopism, 50 tys. książek oraz ponad milion map i 300 tys. innych dokumentów[54].

W okresie zimnowojennym amerykańskie Biuro Badań Strategicznych (Office of‒Strategic Research) uzyskiwało informacje na temat zagranicznych możliwości jądrowych innych państw (w kręgu zainteresowań znalazły się głównie ZSRR, Chiny i Francja). Te dane pochodziły z oficjalnych, ogólnodostępnych raportów rządów wymienionych krajów oraz z publikacji naukowców[55]. W tym samym okresie Biuro

[50] R.A. Norton, *Guide to Open Source Intelligence. A Growing Window into the World*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2011, nr 2, s. 66.

[51] F. Schaurer, J. Störger, *Guide to the Study of Intelligence*. *The Evolution of Open Source Intelligence (OSINT)*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2013, nr 3, s. 53.

[52] Tamże.

[53] K. Leetaru, *The Scope of FBIS and BBC Open-Source Media Coverage*, 1979–2008, „Studies in Intelligence" 2010, nr 1, s. 19.

[54] A. Olcott, *Open Source Intelligence in a Networked World*, London–New York 2012, s. 16.

[55] T.T. Stafford, *The U.S. Intelligence Community*, [b.m.w.] 1983, s. 58–60.

Badań Ekonomicznych (Office of Economic Research) wykorzystywało informacje jawne, ogólnodostępne, dotyczące m.in. produkcji ropy przez kraje OPEC, produkcji zboża w Związku Radzieckim, siły nabywczej obcych walut czy wartości nabycia zagranicznych firm[56]. Rozwój radzieckiego programu kosmicznego był również monitorowany przez CIA i Siły Powietrzne Stanów Zjednoczonych przy wykorzystaniu dostępnej literatury fachowej na ten temat[57].

W czasie zimnej wojny Stasi analizowało miesięcznie około tysiąca zachodnich czasopism i 100 książek, dziennie zaś – 12 godzin audycji emitowanych przez radio i telewizję w RFN[58]. Niemieckie służby do tej pory doceniają wartość białego wywiadu. W Departamencie BND uchodzącym za jego analityczne serce większą część analizowanego materiału (85 proc.) stanowią źródła otwarte (gazety, audycje radiowe, komunikaty medialne, ulotki, Internet). Zaledwie 10 proc. informacji pochodzi z rozpoznania technicznego, a tylko 5 proc. ze źródeł osobowych[59].

W latach 50. XX w. Sherman Kent, twórca amerykańskiej szkoły analizy wywiadowczej, zamówił u swoich uniwersyteckich kolegów historyków raport na temat stanu amerykańskich sił zbrojnych. Miał on być sporządzony wyłącznie na podstawie źródeł otwartych i dotyczyć wszystkich rodzajów broni, ich liczebności, stanu uzbrojenia oraz dyslokacji jednostek do poziomu dywizji włącznie. Po trzech miesiącach pracy Kent otrzymał kilkaset stron danych i analiz poprzedzonych 30-stronicowym streszczeniem. Okazało się, że raport w 90 proc. dawał właściwy obraz armii amerykańskiej, co spowodowało natychmiastowe utajnienie tego dokumentu[60].

Korzyści płynące z OSINT-u w działalności wywiadowczej oprócz Amerykanów i Europejczyków docenili także Chińczycy. W 1958 r. otworzyli oni Chiński Instytut Informacji Naukowo-Technicznej – centralny organ odpowiedzialny za koordynację pozyskiwania, przetwarzania i dystrybucji zagranicznych materiałów pochodzących ze źródeł otwartych. Przez osiem lat zbudowano ogromną jak na tamte czasy bazę informacji o charakterze naukowo-technicznym, pochodzących z ponad 50 krajów, która mieściła: 11 tys. różnych zagranicznych periodyków, 500 tys. raportów badawczych, publikacji rządowych, materiałów pokonferencyjnych i prac naukowych, ponad 5 mln zagranicznych patentów oraz kilka milionów próbek produktów przydatnych dla chińskiego przemysłu[61].

Znaczenie informacji pochodzących z białego wywiadu doceniały również sowieckie służby specjalne, o czym mogło się przekonać FBI po aresztowaniu w 1957 r. Williama Fishera, szpiega KGB, który działał pod zmienionymi personaliami jako Rudolf Abel. Po przeanalizowaniu materiałów dostarczanych przez niego do ZSRR okazało się,

---

[56] J.T. Richelson, *The U.S. Intelligence Community*, 4 wyd., Boulder 1999, rozdział 12.

[57] J.J. Bagnall, *The Exploitation of Russian Scientific Literature for Intelligence Purposes*, „Studies in Intelligence" 1958, nr 2, s. 45–49.

[58] F. Schaurer, J. Störger, *Guide to the Study of Intelligence*…

[59] U. Ulfkotte, *Pod osłoną mroku. Wielkie wywiady bez tajemnic*, Warszawa 2008, s. 292.

[60] W. Zajączkowski, *Zrozumieć innych. Metoda analityczna w polityce zagranicznej*, Warszawa 2011, s. 14.

[61] W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese industrial espionage: Technology acquisition and military modernization*, London–New York 2013, s. 19–20.

że ich podstawą były w znacznej mierze wiadomości zaczerpnięte z otwartych źródeł informacji: dziennika „The New York Times" oraz miesięcznika „Scientific American", i tylko w niektórych miejscach były uzupełnione informacją agenturalną[62].

Na gruncie polskim przykładem wykorzystania białego wywiadu w pracy wywiadowczej jest działalność płk. Mieczysława Wyżła-Śnieżyńskiego, attaché wojskowego w Czechosłowacji. Podstawą sporządzanych przez niego raportów operacyjnych kierowanych do Oddziału II Sztabu Generalnego WP były głównie prasa i katalogi czechosłowackich firm zbrojeniowych[63].

John L. Hart, były oficer operacyjny CIA mający kilkudziesięcioletnie doświadczenie w kierowaniu operacjami wywiadowczymi w różnych częściach świata, po przeanalizowaniu dokumentacji operacyjnej z archiwów amerykańskiej służby przyznał, że oficerowie wywiadu nauczyli się, że przekazanie swoim przełożonym „kartki papieru" z jakąkolwiek treścią jest lepsze niż nieprzekazanie niczego[64]. Jeden ze szpiegów, sowiecki oficer Piotr Popow, usłyszał od swoich przełożonych, że jego praca wywiadowcza nie przynosi efektów, ponieważ więcej można dowiedzieć się z gazet[65]. W 1983 r. japoński dziennikarz przeprowadził wywiad z oficerem KGB Stanisławem Lewczenką pracującym pod przykryciem reportera w Japonii, który w 1979 r. zbiegł do Stanów Zjednoczonych. Podczas 20 godzin rozmów przekazał on informacje na temat agentów oraz omówił warsztat pracy operacyjnej. Na ich podstawie powstała książka, odbywały się również konferencje prasowe z jego udziałem, na których, według oficera amerykańskiego wywiadu, ujawniał on więcej informacji, niż było ich zawartych w jego aktach zgromadzonych przez CIA[66].

Współcześnie „arabska wiosna" jest dowodem na to, że ogólnodostępne informacje, poglądy i oceny publikowane w Internecie są potężnymi narzędziami, które mogą wpływać na losy krajów i społeczeństw. Zastępca dyrektora CIA Christopher Sartinsky po latach doświadczeń w pracy wywiadowczej wyraził zdziwienie i jednocześnie zachwyt tym, że ludzie dobrowolnie ujawniają w Internecie wiedzę o sobie, swoim życiu prywatnym i najbliższych, dzięki czemu ułatwiają pracę agentom[67]. Eben Moglen w wywiadzie pt. *Who Needs the KGB when we have Facebook?*, powołując się na źródła w rosyjskiej służbie specjalnej, odpowiada na to pytanie pytaniem retorycznym: (…) *komu teraz potrzebna Łubianka* (potoczna nazwa siedziby Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej – dop. aut.), *skoro teraz mamy Facebook? Kiedyś wsadzano ludzi*

[62] W. Zajączkowski, *Zrozumieć innych. Metoda…* s. 14.

[63] A. Wojciulik, *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipowski, W. Mądrzejowski (red.), Warszawa 2012, s. 48.

[64] J.L. Hart, *Walka wywiadów, Rosjanie w CIA*, Warszawa 2008, s. 58.

[65] Tamże, s. 52.

[66] S.C. Mercado, *A Venerable Sailing the Sea of OSINT in the Information Age. A Venerable Source in a New Era*, „Studies in Intelligence" 2004, nr 3, s. 51, na podstawie książki S. Lewczenki, *On the Wrong Side: My Life in the KGB*, Washington 1988.

[67] J. Ortega Sim, *Facebook The Social Filter of World Intelligence*, http://thedailyjournalist.com/theinvestigative/facebook-the-social-filter-of-world-intelligence/ [dostęp: 2 V 2018].

do więzienia i próbowano uzyskać od nich informacje. Było to drogie i okrutne. W obecnych czasach jest to o wiele tańsze i łatwiejsze, ponieważ każdy może być szpiegiem, zbierać informacje o swoich znajomych. Trudno teraz wskazać w tej grze, kto jest wygranym, a kto przegranym, skoro wszyscy nawzajem mogą się szpiegować [68].

Wychodząc naprzeciw wyzwaniom, analitycy amerykańskiego Open Source Center, określani jako „wścibscy bibliotekarze", poza monitoringiem mediów i prasy, czytają codziennie nawet 5 mln postów na portalach społecznościowych. Sporządzają z nich raporty zawierające opisy bieżących nastrojów społecznych w wybranych krajach na świecie oraz przewidują możliwości wystąpienia danego zagrożenia[69].

Brytyjskie Rządowe Centrum Łączności również nie ustępuje w tym swojemu sojusznikowi dzięki Network Analysis Center, które codziennie gromadzi ponad 50 mld rekordów dotyczących wizyt użytkowników Internetu w serwisach informacyjnych i portalach z audycjami radiowymi online na całym świecie, powiązanych w większości z islamem[70]. Szef niemieckiego BfV Hans-Georg Maassen podkreśla, że chińskie służby wywiadowcze wykorzystują portale społecznościowe, m.in. Linkedln, za których pośrednictwem nawiązują kontakty rzekomo zawodowo-biznesowe, aby dotrzeć do pracowników niemieckich agencji rządowych[71]. Skuteczne wykorzystanie mediów społecznościowych obrazują chociażby działania izraelskiej służby Szin Bet, która dzięki śledzeniu wiadomości na komunikatorach internetowych udaremniła ataki terrorystyczne na Międzynarodowe Centrum Konferencyjne w Jerozolimie oraz na Ambasadę USA w Tel Awiwie[72]. Również europejskie służby odnoszą sukcesy na tym polu. Francuska Centralna Dyrekcja Wywiadu Wewnętrznego (Direction Centrale du Renseignement Intérieur, DCRI, a od 2014 r. Dyrekcja Generalna Bezpieczeństwa Wewnętrznego, Direction Générale de la Sécurité Intérieure, DGSI) zatrzymała w 2013 r. Romaina Letelliera, francuskiego konwertytę, moderatora dżihadystycznego forum internetowego Ansar Al-Haqq, posługującego się pseudonimem Abu Siyad Al-Normandy, który usłyszał zarzuty podżegania do terroryzmu i szerzenia propagandy terrorystycznej. Był on pierwszym francuskim dżihadystą skazanym na mocy nowej regulacji prawnej z 2012 r. mającej na celu zahamowanie zjawiska samoradykalizacji za pośrednictwem Internetu.

---

[68] A. Schechter, *Who Needs the KGB when we have Facebook? An Interview with Eben Moglen*, http://moglen.law.columbia.edu/publications/Who-needs-KGB-when-we-have-Facebook Schechter.pdf [dostęp: 1 V 2018].

[69] D. Goodin, *CIA 'Open Source Center' monitors Facebook, Twitter*, http://www.theregister.co.uk/2011/11/04/cia_open_source_center [dostęp: 7 V 2018].

[70] Zob. Broadcast/Internet Radio Exploitation and Analysis, 6 November 2009 – UK TOP SECRET/COMINT, https://theintercept.com/document/2015/09/25/broadcast-analysis/ [dostęp: 10 IV 2018].

[71] K. Grieshaber, *German intelligence warns of increased Chinese cyberspying*, https://www.seattletimes.com/business/german-intelligence-warns-of-increased-chinese-cyberspying [dostęp: 2 V 2018].

[72] M. Peck, *Israel Thwarts Al Qaeda Plot to Blow Up U.S. Embassy*, https://www.forbes.com/sites/michaelpeck/2014/01/22/israel-thwarts-al-qaeda-plot-to-blow-up-u-s-embassy/1 [dostęp: 2 V 2018].

Mohammed Emwazi, występujący jako Jihadi John, który skupiał uwagę mediów i służb w związku z tym, że był egzekutorem zakładników przetrzymywanych przez dżihadytów z Państwa Islamskiego, został zidentyfikowany, gdy robił zakupy w Internecie. Służby ustaliły jego personalia i miejsce pobytu w Syrii po podaniu przez niego swojego spersonalizowanego kodu, z którego korzystał jeszcze za czasów studiów[73]. Monitorowanie śladu cyfrowego w Internecie pozwala dotrzeć do jego źródła – użytkownika. W ocenie Paula Moore'a przerwy między naciskaniem poszczególnych klawiszy klawiatury komputera lub długość ich przyciskania są wartościami stałymi i unikatowymi, co czyni je cechą behawioralną człowieka. Dzięki takiej obserwacji i analizie można dokonać oceny profilu konkretnego użytkownika komputera. Z podobnych metod w czasie II wojny światowej miał korzystać brytyjski wywiad. Nasłuchiwał on niemieckich telegrafistów, a następnie na podstawie szybkości nadawania i charakterystycznych błędów, które ci żołnierze popełniali[74],tworzył profile niemieckich żołnierzy.

Twórczość literacka poza dostarczaniem wiedzy poszerzającej horyzonty i pobudzającej wyobraźnię swoich czytelników może także inspirować. Scenariusz stworzony dla widzów światowego kina może zostać przekuty w rzeczywistość, o czym świadczą wydarzenia z 11 września 2001 r. Porwanie samolotu przez terrorystę i dokonanie samobójczego ataku na amerykański parlament – Kapitol – w Waszyngtonie już pięć lat wcześniej opisał Tom Clancy na łamach swojej powieści *Dekret*. Również Timothy McVeigh, skazany za podłożenie bomby w rządowym budynku w Oklahoma City w 1995 r., inspirował się filmem *Red Dawn* (*Czerwony świt*, 1984 r.) oraz *Dziennikami Turnera* autorstwa Andrewa Macdonalda, członka Amerykańskiej Partii Nazistowskiej.

Opublikowanie w „The Washington Post" i „The New York Times" tzw. manifestu Kaczyńskiego dotyczącego zagrożeń wynikających z rozwoju technologicznego stało się przyczyną zatrzymania w 1996 r. przez FBI Theodora Johna Kaczynskiego. Amerykański terrorysta, znany jako „Unabomber", w ciągu prawie 18 lat zabił trzy osoby, a wiele ranił, 29 własnoręcznie wykonanymi bombami. Jego brat David rozpoznał w opublikowanym manifeście myśli swojego brata Theodora, o czym poinformował amerykańską służbę i tym samym przyczynił się do przerwania śledztwa nieprzynoszącego żadnych efektów.

Źródłem informacji zbieranych w ramach białego wywiadu są także metadane, czyli dane o danych, pozwalające na zidentyfikowanie i opisanie informacyjnego obiektu cyfrowego. Można w nich przechowywać informacje m.in. na temat okoliczności i lokalizacji wykonania zadania oraz praw autorskich. Metadane zdjęcia zamieszczonego na Instagramie przez rosyjskiego żołnierza w wojskowym transporterze ujawniły jego miejsce pobytu na Ukrainie, w okresie, gdy Rosja zaprzeczała swojej

[73] J. Murray, *Jihadi John exposed by web error: Killer downloaded software using student ID*, http://www.express.co.uk/news/uk/561135/Jihadi-John-Mohammed-Emwazi-identified-web-error-student-ID-Westminster-university [dostęp: 26 III 2018].

[74] Zob. P. Moore, *Behavioral Profiling: The password you can't change*, https://paul.reviews/behavioral-profiling-the-password-you-cant-change/ [dostęp: 8 IV 2018].

obecności na wschodzie tego kraju. Upublicznienie na Twitterze zdjęcia terrorysty z Państwa Islamskiego na tle jednego z centrów dowodzenia tej organizacji pozwoliło amerykańskim siłom lotniczym na lokalizację i zbombardowanie tego miejsca w ciągu 24 godzin od momentu pojawienia się fotografii w Internecie[75]. Powszechnie wiadomo, że są aplikacje, które dzięki funkcji geolokalizacji umożliwiają precyzyjne zapisywanie pokonywanych tras przez sportowców. Ich aktywność z opisem dystansu, jaki pokonali, jest odzwierciedlana na mapie, którą później chętnie dzielą się z innymi użytkownikami portali społecznościowych. Jak pokazuje przykład aplikacji Strava, analiza metadanych udostępnionych ścieżek biegaczy ujawniła lokalizację tajnych obiektów wojskowych, w tym obiektów służb specjalnych, w których służbę pełnili owi sportowcy.

Organizacje terrorystyczne również chętnie wykorzystują otwarte źródła[76] informacji w działalności, a zwłaszcza w procesie rekrutacji członków[77], ich radykalizacji, szkolenia, planowania zamachów[78] lub cyberataków[79]. W podręczniku Al-Kaidy oceniono, że (…) *publiczne, jawne źródła pozwalają zebrać co najmniej 80% informacji o wrogu*[80]. Peter Bergan doszedł do wniosku, że walka z Al-Kaidą i jej sojusznikami jest w rzeczywistości pierwszą wojną źródeł otwartych[81]. Do tej pory żadna organizacja terrorystyczna nie wykorzystywała mediów społecznościowych w takim stopniu, jak Państwo Islamskie. W ocenie dyrektora FBI Jamesa Comeya członkowie

[75] W. Castillo, *Air Force intel uses ISIS* 'm*oron' post to track fighters*, CNN, https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html [dostęp: 13 IV 2018].

[76] Idąc z duchem czasu, organizacje terrorystyczne stosowały różne narzędzia medialnej aktywności. Od połowy lat 80. XX w. były to transmisje i nagrania VHS z kazaniami, wykładami, zdjęciami z walk oraz artykuły w magazynach i gazetach, w połowie lat 90. XX w. – strony internetowe tworzone i kontrolowane przez prominentnych działaczy organizacji, na początku XXI wieku fora internetowe, a obecnie media społecznościowe. Zob. A.Y. Zelin, R. Borow Fellow, *The State of Globar Jihad Online*, Washington Institute for Near East Policy, January 2013.

[77] W ocenie Elizabeth Kendall istotnym narzędziem rekrutacji może być poezja, która porusza emocje arabskich słuchaczy i czytelników, tworząc aurę tradycji, autentyczności i prawomocności opartej na ideologii. Nawet Osama bin Laden skomponował odę, w której opiewał zniszczenie przez Al-Kaidę okrętu USA „Cole" w 2000 r.

[78] Za pierwszy rozkaz dla terrorystów wydany w Internecie uznaje się wypowiedź członka Al-Kaidy Abu Muhammada al-Hilali, który 25 października 2005 r. wezwał do przeprowadzania zamachów na półwyspie Synaj. Ale już wcześniej, w 1995 r., stwierdzono, że Abd-al-Rahman Zaydan, zatrzymany aktywista Hamasu, przy którym znaleziono komputer, kontaktował się przez Internet z innymi członkami tej organizacji, zob. K. Soo-Hoo, S. Goldman, L. Greenberg, *Information Technology and the Terrorist Threat*, „Survival" 1997, nr 3, s. 139.

[79] Otwarte źródła informacji są narzędziem umożliwiającym rozgłos, który niezależnie, czy jest formą gloryfikacji, czy pogardy dla aktów terrorystycznych, zawsze przynosi pożądany efekt i wpisuje się w scenariusz strategii terrorystów (tzw. terror medialny). Ponadto pozwalają na prowadzenie operacji psychologicznych, dezinformacyjnych i kampanii propagandowych w Internecie.

[80] Zob. podręcznik Al-Kaidy *Al Qaeda Training Manual* z XII 2001 r. Wspomniał o nim m.in. sekretarz obrony USA Donald Rumsfeld w przemówieniu z 15 I 2003 r.

[81] P. Bergen, *Why U.S. can't find Osama bin Laden*…

tej organizacji opanowali Internet[82] do perfekcji i tym samym zrewolucjonizowali zjawisko terroryzmu[83]. Stworzyli tzw. Open Source Jihad[84], czyli szeroko dostępne i łatwe do wyszukania informacje związane z działalnością terrorystyczną. Wzmożone działania islamskich ekstremistów odnotowała również niemiecka BND, według której i Al-Kaida, i Państwo Islamskie prowadzą propagandową wojnę internetową na niespotykaną wcześniej skalę. W niektórych analizach podkreśla się, że nawet 90 proc. treści tworzonych przez terrorystów w Internecie jest rozprzestrzenianych za pośrednictwem mediów społecznościowych[85]. W Internecie znajduje się mnóstwo darmowych książek[86], które są przewodnikami oraz instrukcjami dla potencjalnych zamachowców – „samotnych wilków".

Amerykański wywiad informował, że Osama bin Laden w swojej siedzibie w afgańskich górach miał centrum komputerowe, z którego – wykorzystując czat oraz grupy dyskusyjne – przekazywał informacje członkom Al-Kaidy[87]. Internet prawdopodobnie służył do opracowania szczegółów ataku z 11 września 2001 r. i jego koordynacji. Po aresztowaniu w marcu 2002 r. Abu Zubaydaha, uznawanego za szefa operacyjnego Al Kaidy, w jego komputerze znaleziono prawie 2300 zaszyfrowanych wiadomości i plików ściągniętych z islamskiej strony internetowej. Analiza danych wykazała, że informacje były systematycznie wymieniane pomiędzy członkami ugrupowania od maja 2000 r. do 9 września 2011 r., a częstotliwość korespondencji wzrosła miesiąc przed zamachem[88]. Saudyjski terrorysta doceniał także wartość mediów. W 2002 r. w liście do przywódcy talibańskiego mułły Muhammeda Omara pisał: *Jest oczywiste, że w tym wieku walka przy użyciu mediów jest jedną z najmocniejszych*

[82] Za ojca internetowego dżihadu uznaje się Brytyjczyka z pakistańskimi korzeniami – Babara Ahmada. W 1996 r. ten wówczas 22-letni student jednego z londyńskich uniwersytetów założył pierwszą stronę internetową dla islamskich ekstremistów i dedykował ją Osamie bin Ladenowi oraz jednemu z założycieli Al-Kaidy, Abdullahowi Azzamowi.

[83] J. Ax, *No evidence California attackers were part of terrorist cell – FBI head*, https://in.reuters.com/article/usa-security-idINKBN0TZ29G20151216 [dostęp: 17 IV 2018].

[84] Analiza aktywności terrorystów na portalach społecznościowych, przeprowadzona przez Brytyjskie Międzynarodowe Centrum Studiów nad Radykalizacją i Przemocą Polityczną, wskazuje, że są one wykorzystywane do informowania (raportowania) o bieżącej sytuacji (w rzeczywistym czasie) na froncie walki.

[85] Zob. D. Bieda, E. Riddle, *Cyberspace: A Venue for Terrorism*, „Issues in Information Systems" 2015, nr 16.

[86] Zob. *The Terrorist's Handbook* oraz *The Anarchist Cookbook* – podręczniki, w których opisano, jak skonstruować ładunki wybuchowe przy użyciu domowych środków chemicznych; *Military Studiem in the Jihad Against the Tytants* oraz *How to survive in the west* – analizy zasad organizowania i prowadzenia działań zbrojnych według dżihadystycznej myśli wojskowej; *The Mijahedeen Poisons Handbook* – procedury wytwarzania trucizn; *Safety and Security guidelines for Lone Wolf Mujahideen and small cells* – informacje dotyczące szyfrowania wiadomości w Internecie, metod wywiadowczych i kontrwywiadowczych oraz tworzenia tajnych komórek dzihadu.

[87] D.E. Denning, *Ativism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, w: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica 2001, s. 259.

[88] J. Kelly, *Militants wire Web with links to jihad*, „USA Today" z 10 lipca 2002 r., http://usatoday30.usatoday.com/news/world/2002/07/10/web-terror-cover.htm [dostęp: 20 IV 2018].

metod, właściwie może ona stanowić 90 proc. przygotowań do walk. Przygotowując zamachy w Bombaju w listopadzie 2008 r., terroryści korzystali z wyszukiwarki Google Earth – uczyli się na pamięć topografii miasta, nazw ulic i rozmieszczenia najważniejszych obiektów ataku. W 2009 r. w Pakistanie zatrzymano grupę mężczyzn z Waszyngtonu, nazwanych później „Virginia Five", którzy chcieli dołączyć do bojowników walczących przy granicach z Afganistanem. Ich przyjazd zainspirował talibański rekrut, który znalazł na YouTube komentarz jednego z tych mężczyzn do filmu o ataku na amerykańskie wojska, który miał dla talibów wydźwięk pozytywny. Osoby, które napotykają ograniczenia w bezpośrednim procesie komunikacji, chociażby ze względu na uwarunkowania społeczno-kulturowe, w środowisku wirtualnym mogą je obejść. Aktywność internetowa holenderskich muzułmanek nie umknęła uwadze grup terrorystycznych, które rekrutowały te kobiety jako tłumaczki, programistki i twórczynie holenderskich stron internetowych dotyczących dżihadu[89].

Pomiędzy białym wywiadem a działalnością terrorystyczną można zauważyć synergię[90]. Już w 1976 r. Walter Laquer w magazynie „Harpers" wyraził opinię, że media są najlepszym przyjacielem terrorystów, akt terroru sam w sobie zaś nic nie znaczy bez nagłośnienia całego wydarzenia. To media dostarczają im tlen, od którego są uzależnieni, jak mawiała ponad 30 lat temu Margaret Thatcher. Słusznie określił to Ted Kepel: (…) *bez telewizji terroryzm przypomina drzewo w środku lasu: jeśli runie, nikt tego nie zauważy*[91]. Chciałoby się powiedzieć, że media wykreowały terrorystów, robiąc z nich gwiazdy. Świadczy o tym to, że w ciągu 10 tygodni od wydarzeń z 11 września „Times" na swoich okładkach trzy razy umieścił podobiznę bin Ladena, a tyko dwa razy wizerunek ówczesnego prezydenta USA George'a W. Busha.

W jaki sposób można wykorzystać biały wywiad, pokazuje brytyjski bloger Eliot Higgins, który śledząc aktywność na portalach internetowych, wyciąga zaskakujące wnioski. Po analizie filmu, na którym bojownicy Państwa Islamskiego dokonują egzekucji brytyjskiego dziennikarza Jamesa Foleya, wskazał, że miejscem, w którym to się stało, były wzgórza w pobliżu Ar-Rakka, choć tłem było zupełne pustkowie[92]. Kiedy w sierpniu 2013 r. na syryjskie miasta spadły pociski, a inspektorzy ONZ nie mieli możliwości ich zbadania, w tym samym dniu kiedy to się wydarzyło, Higgins opublikował zdjęcia i filmy odnalezione na YouTubie, na których było widać, że rakiety nie eksplodowały od razu, ale padały nienaruszone, uwalniając z głowic gaz (jak się potem okazało – sarin). Podobnie było w przypadku wschodniej Ukrainy. Wystarczyło przejrzeć portale społecznościowe, aby znaleźć zdjęcia z tego terenu umieszczone

[89] *Jihadis and the Internet. 2009 update*, National Coordinator for Counterterrorism (NCTb), V 2010 r., s. 65–66.

[90] Według raportu United States Institute of Peace w 1998 r. zaledwie co trzecia organizacja terrorystyczna miała własną stronę interentową, a już w 2002 r. miały ją w zasadzie wszystkie.

[91] P. Rees, *Kolacja z terrorystą. Spotkania z najbardziej poszukiwanymi bojownikami na świecie*, Kraków 2008, s. 27.

[92] J. Ensor, *Is this where James Foley was beheaded?*, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11053544/Is-this-where-James-Foley-was-beheaded.html [dostęp: 4 V 2018].

przez żołnierzy 53 Rakietowej Brygady Przeciwlotniczej z obwodu kurskiego, na których były widoczne rakiety Buk. Dowodziły one, że separatystów regularnie wspierały siły zbrojne Federacji Rosyjskiej. Higgins dowiódł również, że pasażerski samolot linii lotniczych Malaysia Airlines został zestrzelony nad Ukrainą przez rakietę Buk należącą do rosyjskiego wojska[93].

Jak ogromnymi zasobami wiedzy są otwarte źródła informacji, w których można odnaleźć również wiadomości ściśle tajne, pokazuje kuriozalna wpadka agenta FBI, pełniącego wcześniej funkcję szefa wydziału antyterrorystycznego. W 2010 r. postanowił on zastrzec prawa autorskie do podręcznika napisanego dla agentów przesłuchujących podejrzanych. Nie zdawał sobie jednak sprawy, że wraz z wpisem do rejestru ten dokument zostanie udostępniony szerokiemu gronu odbiorców. W celu zarejestrowania podręcznika złożył w urzędzie patentowym jego kopię, z którą obecnie każdy może się zapoznać w Bibliotece Kongresu[94]. Błąd popełniony przez funkcjonariusza służb specjalnych, pomimo że wydaje się, że nie był celowy z punktu widzenia zasad ochrony informacji niejawnych, niczym się nie różni od przecieku dokonanego przez Edwarda Snowdena – informacje niejawne zostały udostępnione osobom nieupoważnionym. Wniosek z tego jest jeden: najsłabszym ogniwem w zapewnianiu bezpieczeństwa informacji przed ich nieuprawnionym wyciekiem jest nie technika, ale człowiek. Przykładem tego może być zdekonspirowanie przez Biały Dom swojego szpiega w Afganistanie. Ze względu na pełnioną funkcję dysponował on z pewnością wiedzą, której ujawnienie mogło rodzić niebezpieczne w skutkach konsekwencje dla bezpieczeństwa USA oraz ich sojuszników. Nazwisko i funkcja „Chief of Stadion" (szefa placówki CIA) pojawiło się na liście rozesłanej dziennikarzom w związku z wizytą Baracka Obamy w bazie Bagram w Afganistanie. Ta informacja natychmiast trafiła na Twittera, gdzie była głośno komentowana[95].

Nawet osoby świadome wartości OSINT w działalności wywiadowczej mają konta na portalach społecznościowych, a ich identyfikacja, mimo jakichkolwiek prób ukrywania się, nie jest trudna, wymaga jedynie czasu i determinacji. Przekonał się o tym sam dyrektor FBI James Comey, którego konta na Twitterze i Instagramie zostały ujawnione w krótkim czasie po tym, jak publicznie wspomniał, że z nich korzysta. Dziennikarka Ashley Feinberg zaczęła od prób zlokalizowania kont jego rodziny, które – jak słusznie założyła – są łatwiejsze do odnalezienia. Za główny cel wybrała jego syna Briena, koszykarza drużyny uniwersyteckiej. Pośród opublikowanych tweetów jego drużyny znalazła odniesienia do konta Briena i jego zdjęcia wraz z linkiem do tego zdjęcia na Instagramie, które – jak się okazało – było zablokowane. Korzystając

[93] *The lost digit – Buk 3x2*, „A bell¿ngcat Investigation" 2014, https://www.bellingcat.com/wp-content/uploads/2016/05/The-lost-digit-BUK-3x2_EN_final-1.pdf, s. 2 [dostęp: 1 V 2018].

[94] Zob. J. Baumann, *You'll Never Guess Where This FBI Agent Left a Secret Interrogation Manual*, http://www.motherjones.com/politics/2013/12/fbi-copyrightedinterrogation-manual-unredacted-secrets/ [dostęp: 1 V 2018].

[95] G. Miller, *White House to investigate inadvertent naming of CIA officer*, http://www.washingtonpost.com/world/national-security/white-house-to-investigate-inadvertent-naming-of-cia-officer/2014/05/27/5d5f41f0-e5e6-11e3-afc6-a1dd9407abcf_story.html [dostęp: 4 IV 2018].

z fikcyjnego konta, poprosiła o dodanie jej do znajomych. Portal automatycznie zaproponował kolejne konta osób, które może znać dziennikarka. Wśród nich znalazła kilku krewnych dyrektora FBI, w tym jego żonę, Patrice Comby, oraz tajemniczego Reinholda Niebuhra. Ten ostatni miał tylko kilku znajomych na swoim koncie, a o takiej możliwości Comey wspominał podczas wywiadu. Po przeszukaniu zasobów Internetu Feinberg ustaliła, że Comey na studiach pisał pracę na temat teologa Reinholda Niebuhra, co utwierdziło ją w przekonaniu, że zidentyfikowała konto Comeya. Po tym samym pseudonimie „Reinhold Niebuhr" pośród kilku kont na Twitterze wyszukała jedno, którego nick: projectexile7 nawiązywał do projektu realizowanego przez Comeya w poprzedniej pracy[96], co ostatecznie potwierdziło jej przypuszczenia.

Podsumowując rozważania o OSINT i płynących z niego wymiernych korzyściach w działalności wywiadowczej, autor chciałby zaznaczyć, że dzięki postępowi technologicznemu i nieustającemu rozwojowi infrastruktury informatycznej otwarte źródła informacji, a zwłaszcza wirtualne, coraz silnej oddziałują na globalną rzeczywistość. Amerykanie dostrzegają ten trend, dlatego w strukturach Biura Dyrektora Wywiadu Krajowego, podmiotu odpowiedzialnego za opracowanie i badanie projektów w zakresie działalności wywiadowczej, uruchomili w 2011 r. projekt *Open Source Indicators*. W ramach tego projektu jest monitorowana aktywność w wirtualnych, ogólnie dostępnych źródłach otwartych. To pozwala na łączenie wspólnych wskaźników w sieci, a następnie – na prognozowanie i wczesne wykrycie istotnych zdarzeń społecznych, które mogą nieść za sobą niebezpieczeństwo.

Dyrektor Wywiadu Narodowego USA James R. Clapper w lutym 2016 r. podczas posiedzenia senackiej komisji ds. wywiadu, oceniając globalne zagrożenia w dzisiejszych czasach, wskazał, że poza OSINT-em służby mogą zacząć wykorzystywać w działalności wywiadowczej wspomniany już tzw. *Internet of Things*, czyli monitorować i pozyskiwać informacje z urządzeń podłączonych do Internetu. Robert Steele poszedł dalej w swoich przemyśleniach i stwierdził, że służby w XXI wieku będą skoncentrowane w dużej mierze na każdym dostępnym źródle – *Open Source Everythings*.Tego typu źródła mogą dostarczać drobnych, szczątkowych informacji, ale dających punkt zaczepienia, odpowiadających na pytania, które z perspektywy prowadzonych działań są nie tylko podstawą analizy, jej „chlebem i masłem" – jak uważał Arthur S. Hulnick[97], lecz także priorytetowym narzędziem w działalności wywiadowczej na każdym etapie jej realizacji. Pozwalają też zarówno zweryfikować i pogłębić dotychczasową wiedzę, jak i szerzej spojrzeć na badane zjawisko.

[96] A. Feinberg, *This Is Almost Certainly James Comey's Twitter Account*, https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641 [dostęp: 10 IV 2018].

[97] A.S. Hulnick, *The Downside of Open Source Intelligence*, „International Journal of Intelligence and Counter Intelligence" 2002–2003, nr 4, s. 565.

Bibliografia:

100 Events That Changed the World, „National Geographic" 2015, Special Issue.

A Look Back… George Washington: America's First Military Intelligence Director, https://www.cia.gov/news-information/featured-story-archive/2007-featured-story-archive/george-washington.html [dostęp: 5 V 2018].

Apuzzo M., Schmidt M.S., Preston J., *U.S. Visa Process Missed San Bernardino Wife's Zealotry on Social Media*, http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html [dostęp: 6 V 2018].

Ax J., *No evidence California attackers were part of terrorist cell – FBI head*, http://in-.reuters.com/article/usa-security-idINKBN0TZ29G20151216 [dostęp:17 IV 2018].

Bagnall J.J., *The Exploitation of Russian Scientific Literature for Intelligence Purposse*, „Studies in Intelligence" 1958, nr 2.

Baumann J., *You'll Never Guess Where This FBI Agent Left a Secret Interrogation Manual*, http://www.motherjones.com/politics/2013/12/fbi-copyrighted-interrogation-manual-unredacted-secrets/ [dostęp: 12 VIII 2017].

Bergen P., *Why U.S. can't find Osama bin Laden*, http://edition.cnn.com/2010/OPINION/10/19/bergen.finding.bin.laden/ [dostęp: 2 VIII 2017].

Bieda D., Riddle E., *Cyberspace: A Venue for Terrorism*, „Issues in Information Systems" 2015, nr 16, International Association of Computer Investigative Specialists (IACIS), Leesburg 2015.

Big Data: Seizing Opportunities, Preserving Values, Executive Office of the President, The White House, Washington DC, V 2014 r., s. 7–8.

Bohn R., Short J., *Measuring Consumer Information*, „International Journal of Communication" 2012, nr 6, University of California, s. 980–1000.

Broadcast/Internet Radio Exploitation and Analysis, 6 November 2009 – UK TOP SECRET/COMINT, https://theintercept.com/document/2015/09/25/broadcast-analysis/ [dostęp: 10 IV 2018].

Castillo W., *Air Force intel uses ISIS 'moron' post to track fighters*, https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html [dostęp: 13 IV 2018].

Church G.M., Gao Y., Konsuri S., *Next-Generation Digital Information Storage in DNA*, Sciencexpress, 16 VIII 2012 r., [dostęp: 4 IV 2018].

Coddington E.B., *The Gettysburg Campaign: A Study in Command*, New York 1968, Charles Scribner's Sons.

Costlow T., *Kehler raises trial balloon: Put STRATCOM in charge of all GEOINT PED*, http://defensesystems.com/articles/2011/10/19/geoint-kehler-stratcom-geospatial intelligence.aspx [dostęp: 9 VII 2017].

Denning D.E., *Ativism, Hactivism and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy*, w: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica 2001.

Disruptive innovation. Case study: Intelligence – Open-source data analytics, Washington, 2012, Deloitte.

Ensor J., *Is this where James Foley was beheaded?*, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11053544/Is-this-where-James-Foley-was-beheaded.html [dostęp: 4 VIII 2017].

Feinberg A., *This Is Almost Certainly James Comey's Twitter Account*, https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641 [dostęp: 10 IV 2018].

Gantz J., Reinsel D., *Extracting value from chaos*, w: *IDC analyze the future,* https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf [dostęp: 4 VI 2018].

Gibson S.D., *Exploring the Role and Value of Open Source Intelligence*, w: *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014.

Gleick J., *Informacja – bit, wszechświat, rewolucja*, Kraków 2012.

Goodin D., *CIA 'Open Source Center' monitors Facebook, Twitter*, http://www.theregister.co.uk/2011/11/04/cia_open_source_center [dostęp: 7 VIII 2017].

Grieshaber K., *German intelligence warns of increased Chinese cyberspying*, https://www.seattletimes.com/business/german-intelligence-warns-of-increased-chinese-cyberspying/ [dostęp: 2 V 2018].

Hannas W.C., Mulvenon J., Puglisi A.B., *Chinese industrial espionage: Technology acquisition and military modernization*, London–New York 2013.

Harmon G., *The measurement of information*, „Information Processing and Management" 1984, nr 1–2.

Hart J.L., *Walka wywiadów, Rosjanie w CIA*, Warszawa 2008, Bellona.

Hulnick S., *„The Downside of Open Source Intelligence"*, „International Journal of Intelligence and Counter Intelligence", 2002–2003, nr 4.

Intelligence Community Directive Number 301, NATIONAL OPEN SOURCE ENTERPRISE 2006, https://www.fas.org/irp/dni/icd/icd-301.pdf [dostęp: 6 VII 2017].

ISO 22320:2011, *Societal security – Emergency management – Requirements for incident response*, November 2011.

ISO 2382-1:1993, *Information technology – Vocabulary – Part 1: Fundamental terms*, November 1993.

Karnowski M., Mistewicz E., *Anatomia władzy*, Warszawa 2010, Czerwone i Czarne.

Kelly J., *Militants wire Web with links to jihad*, „USA Today" z 10 lipca 2002 r., http://usatoday30.usatoday.com/news/world/2002/07/10/web-terror-cover.htm [dostęp: 20 IV 2018].

Koemer R., *William Binney: NSA Claim Not to Be Mining Content Is an* "*Outright Lie*", https://www.huffingtonpost.com/robin-koerner/nsa-whisteblower-nsa-clai_b_7837806.html [dostęp: 4 V 2018].

Landauer T.K., *How Much do People Remember? Some Estimates of the Quantity of Learned Information in Long-Term Memory*, „Cognitive Science" 1986, nr 10, s. 477–493.

Larecki J., *W kręgu tajemnic wywiadu*, Warszawa 2007, WNT.

Leetaru K., *The Scope of FBIS and BBC Open-Source Media Coverage*, *1979–2008*, „Studies in Intelligence" 2010, nr 1, s. 17–37.

Levinson P., *Nowe nowe media*, Kraków 2010, Wydawnictwo WAM.

Lowenthal M.M., *Open Source Intelligence: New Myths, New Realitties,* w: *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, R.Z. George, R.D. Kline (eds.), Lanham 2006.

McAllister Linn B., *The Philippine War, 1899–1902*, Lawrence 2000, University Press of Kansas.

Meeker M., Yu L., *Internet Trends*, Washington 2013, Kleiner Perkins Caulfield Byers.

Mercado S.C., *Sailing the Sea of OSINT in the Information Age. A Venerable Source in a New Era*, „Studies in Intelligence" 2004, nr 3; na podstawie książki S. Lewczenki, *On the Wrong Side: My Life in the KGB*, Washington 1988, Pergamon-Brassey's,

Miller G., *White House to investigate inadvertent naming of CIA officer*, http://www.washingtonpost.com/world/national-security/white-house-to-investigate-inadvertent-naming-of-cia-officer/2014/05/27/5d5f41f0-e5e6-11e3-afc6-a1dd9407abcf_story.html [dostęp: 4 IV 2018].

Moore P., *Behavioral Profiling: The password you can't change*, https://paul.reviews/behavioral-profiling-the-password-you-cant-change/ [dostęp: 8 IV 2018].

Murray J., *Jihadi John exposed by web error: Killer downloaded software using student ID*, http://www.express.co.uk/news/uk/561135/Jihadi-John-Mohammed-Emwazi-identified-web-error-student-ID-Westminster-university [dostęp: 26 III 2018].

National Coordinator for Counterterrorism (NCTb), Jihadis and the Internet, 2009.

National Defense Authorization Act for Fiscal Year 2014, Public Law 113–66 (26 XII 2013 r.).

Nogalski B., Surawski M.B., *Informacja strategiczna i jej rola w zarządzaniu przedsiębiorstwem*, w: *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystywanie i ochrona (wybrane problemy teorii i praktyki)*, R. Borowiecki, M. Kwieciński (red.), Kraków 2003.

Norton R.A., *Guide to Open Source Intelligence. A Growing Window into the World*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2011, nr 2.

Olcott A., *Open Source Intelligence in a Networked World*, London–New York 2012, The Continuum International Publishing Group.

Open Source Intelligence, Headquarters, Department of Army, Army Techniques Publication, ATP 2-22.9, Washington 2012.

Ortega Sim J., *Facebook The Social Filter of World Intelligence*, http://thedaily-journalist.com/theinvestigative/facebook-the-social-filter-of-world-intelligence/ [dostęp: 26 V 2018].

Peck M., *Israel Thwarts Al Qaeda Plot to Blow Up U.S. Embassy*, https://www.forbes.com/sites/michaelpeck/2014/01/22/israel-thwarts-al-qaeda-plot-to-blow-up-u-s-embassy/1 [dostęp: 2 V 2018].

Polańska K., *Informacja, jej wiarygodność i co z nich dla nas wynika*, w: *Informacja – dobra lub zła nowina*, A. Szewczyk (red.), Szczecin 2004, Uniwersytet Szczeciński.

Rees P., *Kolacja z terrorystą*. *Spotkania z najbardziej poszukiwanymi bojownikami na świecie*, Kraków 2008, Uniwersum.

Report of the Human Rights Council on its thirty-second session, General Assembly United Nations, Human Rights Council, Thirty-second session, A/HRC/32/L.20, 14 XI 2016 r.

Rheingold H., *The Virtual Community. Homesteading on the Electronic Frontier*, New York 1994.

Schaurer, F., Störger J., *Guide to the Study of Intelligence*. *The Evolution of Open Source Intelligence (OSINT)*, „The Intelligencer. Journal of U.S. Intelligence Studies" 2013, nr 3.

Schechter A., *Who Needs the KGB when we have Facebook? An Interview with*

Eben Moglen, http://moglen.law.columbia.edu/publications/Who-needs-KGB-when-we-have-Facebook-Schechter.pdf [dostęp: 1 V 2018].

Sienkiewicz P., *10 wykładów*, Warszawa, 2005, AON.

Słoniewski T., *Od BI do „Big Data*", w: *Nowa twarz Business Intelligence*, R. Jesionek (red.), http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf [dostęp: 7 V 2018].

Soo Hoo K., Goodman S., Greenberg L., *Information Technology and the Terrorist Threat*, „Survival" 1997, nr 3.

Stafford T.T., *The U.S. Intelligence Community*, [b.m.w] 1983, University Press of America.

Słownik języka polskiego, t. 1–3, M. Szymczak (red.), Warszawa 1978–1981, PWN.

Stankiewicz K., *Wpływ Internetu na percepcję wiarygodności informacji*, w: *Społeczeństwo informacyjne – wizja czy rzeczywistość?*, L.H. Haber (red.), Kraków 2003, Akademia Górniczo-Hutnicza im. Stanisława Staszica w Krakowie.

Stefanowicz B., *Informacja. Wiedza. Mądrość*, seria: Biblioteka Wiadomości Statystycznych, t. 66, Warszawa 2013, GUS.

Taycher L., *Books of the world, stand up and be counted! All 129,864,880 of you*, booksearch.blogspot.com/.

The lost digit – Buk 3x2, „A bellingcat Investigation" 2014, https://www.bellingcat.com/wp-content/uploads/2016/05/The-lost-digit-BUK-3x2_EN_final-1.pdf [dostęp: 1 V 2018].

Tucker P., *Meet the Man Reinventing CIA for the Big Data Era*, http://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/ [dostęp: 3 I 2018].

Ulfkotte U., *Pod osłoną mroku. Wielkie wywiady bez tajemnic*, Warszawa 2008, KiW.

Volkoff V., *Dezinformacja: oręż wojny*, Warszawa 1991, Antyk.

Wojciulik A., *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*, w: *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, W. Filipowski, W. Mądrzejowski (red.), Warszawa 2012, C.H. Beck.

Zagrożenia dla bezpieczeństwa informacyjnego państwa. Identyfikacja, analogia zagrożeń i ryzyka, t. 1: *Raport z badań*, T. Jemioło, P. Sienkiewicz (red.), Warszawa 2004, AON.

Zajączkowski W., *Zrozumieć innych. Metoda analityczna w polityce zagranicznej*, Warszawa 2011, KSAP.

Zelin A.Y., Borow Fellow R., *The State of Global Jihad Online*, Washington Institute for Near East Policy, I 2013.

Zločevskij S.E. i in., *Informacja w badaniach naukowych*, Warszawa 1972, WKiŁ.

Żuk P., *Demokracja pod kontrolą – czyli podsłuch non stop*, http://www.tygodnikprzeglad.pl/demokracja-pod-kontrola-czyli-podsluch-non-stop/ [dostęp: 15 VI 2018].

Abstrakt

Artykuł jest poświęcony istocie, funkcji i wartości informacji pochodzących ze źródeł otwartych w kontekście działalności wywiadowczej. Analiza wybranych przykładów wykorzystania informacji ogólnodostępnych pokazuje, że niezależnie od zmieniających się czasów w sposób wymierny uzupełniają one wiedzę uzyskaną innymi metodami, określanymi jako niejawne. Autor dochodzi do wniosku, że w obecnych czasach zdobycie pożądanych informacji jest coraz trudniejsze ze względu na ich ilość, która systematycznie rośnie. Lawinowy wzrost informacji wielośródłowych powoduje przeciążenie możliwości analitycznych, którym te informacje są poddawane, oraz chaos informacyjny, przez co wymagają one dodatkowej weryfikacji i oceny ich wiarygodności. Zasadne wydaje się stwierdzenie, że z uwagi na swoją właściwość, po uwzględnieniu wyzwania dzisiejszych czasów, informacja stanowi „broń masowego rażenia". Może ona być wykorzystywana dwojako: albo jako narzędzie dezinformujące wobec przeciwnika, albo – w przypadku jej pozytywnej weryfikacji – może przyczyniać się do podjęcia działań wyprzedzających, dających przewagę w środowisku bezpieczeństwa.

Słowa kluczowe: informacja, OSINT, otwarte źródła informacji, media społecznościowe, biały wywiad, działalność wywiadowcza, terroryzm.

Piotr Karasek

Analiza informacji z mediów społecznościowych jako narzędzie wspierające kontrolę bezpieczeństwa w procedurach migracyjnych[1]

Wstęp

Wczesne wykrywanie ataków terrorystycznych, zapobieganie im oraz utrzymywanie właściwego poziomu bezpieczeństwa granic państwowych – to jedne z najaktualniejszych zagadnień w bieżącej debacie publicznej i eksperckiej. Obecnie wzrasta rola mediów społecznościowych we wspieraniu realizacji wyżej wymienionych działań. Chociaż działalność stricte antyterrorystyczna jest domeną poszczególnych wyspecjalizowanych służb państwowych, to w obliczu powagi zagrożeń o charakterze terrorystycznym jest niezbędne szerokie wykorzystanie wszystkich możliwych sposobów przeciwdziałania terroryzmowi. Ma to szczególne znaczenie, gdy bierze się pod uwagę, że współcześni sprawcy aktów terrorystycznych nader często działają samodzielnie i nie utrzymują stałych kontaktów z grupami zorganizowanymi, co czyni zagrożenie z ich strony znacznie trudniejszym do wczesnego wykrycia z wykorzystaniem metod tradycyjnych.

Istotną rolę w szeroko rozumianym zapewnianiu bezpieczeństwa wewnętrznego powinny odgrywać m.in. osoby bezpośrednio odpowiedzialne za przyznawanie wiz wjazdowych. Mając dostęp do prawdziwych, weryfikowalnych danych osób starających się o wizę, w celu wykrycia zagrożenia i podjęcia decyzji dotyczącej ewentualnej odmowy prawa wjazdu, gdy jest to niezbędne do zapewnienia bezpieczeństwa, można wykorzystać informacje ze źródeł otwartych, w tym zwłaszcza z mediów społecznościowych. Co więcej, wykorzystanie tej możliwości w czasie przeprowadzania procedur migracyjnych może pozwolić na uzyskanie wielu innych ważnych informacji na temat starających się o wjazd. Takie narzędzia, jak media społecznościowe, są coraz częściej oficjalnie wykorzystywane przez agencje bezpieczeństwa w różnych krajach, a przede wszystkim w Stanach Zjednoczonych[2], do wczesnego wykrywania zagrożeń. O ile rzeczywiste efekty wykorzystywania informacji z mediów społecznościowych są w chwili obecnej trudne do oszacowania, o tyle istnieje wiele wyraźnych ograniczeń, które należy brać pod uwagę przy projektowaniu rozwiązań opierających się na technikach prowadzenia białego wywiadu.

Niniejszy artykuł, na podstawie danych pochodzących z literatury przedmiotu oraz danych medialnych i pomocniczych wywiadów badawczych z funkcjonariusza-

[1] Artykuł został przygotowany na podstawie materiałów zgromadzonych w ramach realizacji projektu PRIME finansowanego ze środków 7. Programu Ramowego Komisji Europejskiego (umowa grantowa nr 608354).

[2] B.O'Brien, *U.S. visa applicants to be asked for social media history: State Department*, https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P/ [dostęp: 15 IV 2018].

mi służb różnych państw, ma na celu przedstawienie możliwości, zagrożeń i ograniczeń wynikających ze stosowania technik białowywiadowczych w środowisku mediów społecznościowych w kontekście utrzymywania bezpieczeństwa wewnętrznego państw i bezpieczeństwa procesów migracyjnych.

Państwowe służby bezpieczeństwa, terroryzm, Internet

Możliwości związane z szybkim rozwojem Internetu bywają przedstawiane jako jednoznacznie sprzyjające także rozwojowi przestępczości, w tym terrorystycznej. Takie podejście jednak nie jest prawidłowe. Częściowa anonimowość, zdecentralizowane czarne rynki, przestępcze fora w sieci ukrytej, cała gama niebezpiecznych i niedozwolonych treści, które bez problemu można odnaleźć – wszystkie te elementy współczesnego Internetu rzeczywiście mogą wspierać rozwój działalności przestępczej. Zarazem Internet jest narzędziem pomocnym przy realizacji czynności wykrywczych w odniesieniu do przestępczości kryminalnej i terrorystycznej. Niektórzy badacze twierdzą wręcz, że współczesne technologie komunikacyjne jednak bardziej wspierają działania służb państwowych niż organizacji terrorystycznych[3].

Zarówno praktycy, jak i przedstawiciele świata nauk o bezpieczeństwie wskazują na szerokie możliwości związane z poszukiwaniem informacji w publikatorach otwartych. Zwłaszcza media społecznościowe są postrzegane jako źródła danych i de facto stanowią skarbnicę nowego typu szeroko rozumianego „białego wywiadu" (*Open-Source Intelligence* – OSINT), któremu nadają nazwę SOCMINT (*Social Media Intelligence)*[4]. To ostatnie pojęcie zostało wstępnie opisane w literaturze, podobnie jak różnego rodzaju techniki możliwe do wykorzystania w celu prowadzenia rozpoznania za pomocą takich metod. Szczegółowe zastosowania, szanse i zagrożenia związane z prowadzeniem SOCMINT-u wciąż jednak pozostają tematem stosunkowo mało zeksplorowanym. Same zaś media społecznościowe, niezależnie od ich definicji[5], stały się na dobre zjawiskiem globalnym i zawierają ogromną liczbę dobrowolnie publikowanych informacji o jednostkach oraz ich grupach. Skuteczność technik SOCMINT-u wynika częściowo z tego, że użytkownicy mediów społecznościowych, publikując informacje o sobie w Internecie (w celu szeroko pojętej samoekspresji, np. artystycznej czy towarzyskiej), jednocześnie przekazują wiele danych, których by nie przekazali, zapytani o nie wprost[6] (zwłaszcza gdyby byli pytani przez służby państwowe).

[3] D.C. Benson, *Why the Internet is not increasing terrorism,* „Security Studies" 2014, nr 23/2, s. 308, 311, 328.

[4] A.N. Liaropoulos, *The challenge of social media for the Intelligence community,* „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1, s. 6.

[5] Media społecznościowe mogą być definiowane jako (…) *aplikacje internetowe skonstruowane w oparciu o założenia technologiczno-ideowe tzw. Sieci 2.0 i pozwalają użytkownikom na kreowanie i wymianę treści*, w przypadku gdy „strony internetowe" są wykorzystywane wyłącznie w charakterze infrastruktury pozwalającej użytkownikom na dzielenie się własną treścią. Zob. A. Kaplan, M. Haenlein, *Users of the world, Unite!*, „Business Horizons" 2010, nr 53/1, s. 61.

[6] C. Arslan, M. Yanuk, *A New Discipline of Intelligence: Social Media*, Istanbul 2015, s. 69–70.

W przeciwieństwie do forów tematycznych działających w Internecie od wielu lat, media społecznościowe zostały zaprojektowane w taki sposób, aby pobudzać swobodną, publiczną ekspresję użytkowników, szczególnie w zakresie informacji dotyczących stylu życia, tj. zachęcać ich do publikowania własnych myśli, planów, opinii, zdjęć i faktów z ich życia. Wynika z tego obserwowalna tendencja użytkowników mediów społecznościowych do tzw. naddzielenia się (ang. o*ver-sharing)* informacjami prywatnymi. Miewa to groźne konsekwencje, gdyż zwiększa ryzyko stania się ofiarą różnych typów przestępstw[7]. Zwykle w tym właśnie kontekście było to opisywane. Z drugiej jednak strony dokładnie to samo zjawisko wpływa na dużą skuteczność technik SOCMINT-u, które są wykorzystywane do ochrony szeroko rozumianego bezpieczeństwa wewnętrznego.

Media społecznościowe są więc źródłami danych, które mogą służyć pracy wykrywczej. Ponad 81 proc. funkcjonariuszy amerykańskich organów ścigania wykorzystuje tego typu źródła jako narzędzia pozyskiwania informacji na temat osób występujących w prowadzonych przez siebie sprawach. Dzieje się tak pomimo tego, że w 48 proc. przypadków jest to praktyka niezalecana przez przełożonych[8]. Należy podkreślić, że część informacji pochodzących z mediów społecznościowych jest dostępna dla każdego, nawet niezalogowanego użytkownika sieci, bez konieczności występowania z jakimkolwiek wezwaniem czy nakazem sądowym. Wykorzystując specjalistyczne narzędzia, np. oparte na technologii „geofencingu" (choćby Geofeedię, która pozwala na zarządzanie zagrożeniami w czasie niemalże rzeczywistym[9])[10], można pozyskać wiele cennych informacji.

Trzeba też zaznaczyć, że wszystkie metody pracy stosowane przy zwalczaniu zwykłej przestępczości kryminalnej są przydatne również w zwalczaniu przestępstw terrorystycznych i zapobieganiu im. Dotyczy to zwłaszcza tzw. monitoringu Internetu. Podczas badań prowadzonych w ramach projektu 7. Programu Ramowego Komisji Europejskiej „PRIME"[11] ustalono, że metody stosowane przez organy ścigania i służby bezpieczeństwa w celu zwalczania terroryzmu sprawców indywidualnych właściwie nie różnią się w sposób istotny od tych stosowanych przeciwko grupom terrorystycznym czy zorganizowanym grupom przestępczym o charakterze kryminalnym[12]. Na podstawie wyników badań ankietowych przeprowadzonych z doświadczonymi

[7] K. Paullet, J. Pinchot, *Cybercrime: the unintentional effects of oversharing information on Facebook,* Proceedings of the Conference on Information Systems Applied Research, New Orleans 2012, s. 1–7.

[8] *Social media use in law enforcement: crime prevention and investigative activities continua to driver usage*, https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf [dostęp: 15 IV 2018].

[9] K. Cooke, *US Police used Facebook, Twitter data to track protesters*, http://www.reuters.com/article/social-media-data-idUSL4N1CH4J1 [dostęp: 15 IV 2018].

[10] M.D. Dabhi, *Geofencing: a generic approach to Real time location based tracking system*, „International Journal of Computer Networks and Wireless Communications" 2016, nr 6, s. 35–37.

[11] http://www.fp7-prime.eu/home_page [dostęp: 15 IV 2018].

[12] FP7 PRIME WP7 Deliverable D7.1, *Counter-measures review report*, niepubl.

funkcjonariuszami służb (policji, agencji antyterrorystycznych właściwych w danym kraju i służb ochrony granic) w Europie, Ameryce Północnej oraz w Indiach utworzono hierarchiczne zestawienie najskuteczniejszych i zarazem najmniej kosztownych metod zwalczania zagrożeń terrorystycznych[13]. Monitoring Internetu został przy tym określony przez respondentów jako najbardziej przydatna, skuteczna i zarazem najtańsza metoda pracy (takiej odpowiedzi udzieliło 94 proc. badanych praktyków).

Przy omawianiu i ocenie skuteczności metod zwalczania zagrożeń terrorystycznych w kontekście Internetu i monitoringu mediów społecznościowych istotne jest także zrozumienie specyficznego charakteru przestępczości terrorystycznej tzw. samotnych wilków oraz tego, w jaki sposób treści zamieszczone w mediach społecznościowych mogą wskazywać na przyszłe zagrożenia. Mimo że sformułowanie ścisłej definicji „samotnego wilka" przez kryminologów wciąż napotyka ogromne trudności, to osoby określane w ten sposób bywają na ogół opisywane jako pojedynczy sprawcy działający bez formalnych powiązań z jakąkolwiek grupą terrorystyczną, dokonujący (lub planujący dokonanie) aktu terrorystycznego, będąc zmotywowanymi przez ideologię ekstremistyczną. Wzorcowy „samotny wilk" realizuje schemat działania w kolejnych etapach: od fazy radykalizacji, przez przygotowanie ataku, aż po sam atak – bez pomocy z zewnątrz. Sprawcy takich czynów często (choć niekoniecznie świadomie czy celowo) komunikują otoczeniu swoje intencje na kilka godzin, dni czy nawet tygodni przed dokonaniem ataku. Według części badaczy spośród wszystkich tego typu aktów dokonanych lub planowanych w Stanach Zjednoczonych po 11 września 2001 r. aż w 76 proc. sprawca publikował informację o przyszłym zamachu (niekiedy więcej niż jednokrotnie) z wykorzystaniem mejla, wiadomości tekstowych, ale również mediów społecznościowych – za pośrednictwem Facebooka czy Twittera[14]. Nawet wtedy, gdy zamiar ataku nie był przez sprawcę wskazany wprost, jego zachowanie w mediach społecznościowych często wskazywało na radykalizację w jakimś kierunku. Niestety, tego typu informacje nie zawsze są właściwie odczytywane[15].

Media społecznościowe a procedura wizowa

Przy uwzględnieniu wspomnianych powyżej zalet zastosowania technik SOCMINT-u w zwalczaniu przestępczości kryminalnej i terrorystycznej warto rozważyć, czy i ewentualnie w jaki sposób mogłyby one być wykorzystywane przy wzmacnianiu bezpieczeństwa w ramach procedur migracyjnych. Lub też szerzej: w jaki sposób OSINT, a zwłaszcza SOCMINT, mogą wspomóc rolę procedur migracyjnych w zapewnianiu i utrzymywaniu bezpieczeństwa wewnętrznego.

[13] Tamże.

[14] M. Hamm, R. Spaaij, *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*, Waszyngton 2015, s. 9.

[15] Na przykład: George Sodini (znany jako „the Gym Killer") szczegółowo opisywał plan swojego ataku na osobistym blogu przez wiele miesięcy pomiędzy 2008 a 2009 rokiem. Zob. *Full text of Gym Killer's blog,* http://nypost.com/2009/08/05/full-text-of-gym-killers-blog/ [dostęp: 15 IV 2018].

Znaczenie prawidłowej weryfikacji osób starających się o wjazd na teren danego państwa dobrze ilustruje zamach w San Bernardino z grudnia 2016 r. Wkrótce po dokonaniu ataku podano informację, że kobieta – napastnik, Tashfeen Malik, przebywała w Stanach Zjednoczonych na podstawie wizy narzeczeńskiej. Jednocześnie publikowała ze swojego konta w mediach społecznościowych dżihadystyczną propagandę jeszcze zanim tę wizę otrzymała[16]. Należy podkreślić, że ta informacja okazała się później nie w pełni prawdziwa[17], chociaż doskonale ilustruje to, jakie problemy mogą wyniknąć w przypadku nieprawidłowego lub niepełnego sprawdzenia osób starających się o wizy pobytowe[18].

Dokonywanie bieżącej weryfikacji kandydatów do otrzymania wizy co prawda nie powinno należeć do najważniejszych zadań głównych instytucji zajmujących się bezpieczeństwem państwa, ale nie koliduje z ich kompetencjami. W praktyce udział tych struktur w procedurze wizowej jest ograniczony. Dostępne dane wywiadowcze na temat osób starających się o wizę są dostarczane decydentom przez narodowe służby bezpieczeństwa (np. w formie odpowiednich list czy baz danych prowadzonych przez wyspecjalizowane jednostki, takie jak np. Terrorist Screening Center w Stanach Zjednoczonych[19] lub System Informacyjny Schengen w Europie[20]). Jednak ze względu na decentarlizację współczesnego terroryzmu, zwłaszcza indywidualnego, oparcie systemu bezpieczeństwa na jednym, scentralizowanym źródle informacji nie jest wystarczające. O ile bowiem sukcesy organów zapewniających bezpieczeństwo w wykrywaniu powiązań jednostek z grupami zorganizowanymi oraz w ich ramach są niezaprzeczalne, o tyle pojedynczy zradykalizowani sprawcy mogą ujść ich uwadze. Co więcej, jest wiele innych elementów niebędących domeną organów ścigania i organów ochrony bezpieczeństwa, które należy brać pod uwagę podczas weryfikacji podania wizowego. Dotyczy to np. weryfikacji specyficznych wymogów wizowych w zakresie podania informacji o niekaralności czy stanie zdrowia. Takie dane mogą mieć istotne znaczenie dla podjęcia decyzji w sprawie wydania wizy, gdyż mają związek z szeroko rozumianym bezpieczeństwem publicznym. Niekoniecznie jednak mają jakiekolwiek znaczenie dla instytucji zajmujących się bezpieczeństwem państwa.

Wykorzystywanie technik tzw. białego wywiadu, zwłaszcza OSINT, może więc być postrzegane jako element szerokiego zarządzania bezpieczeństwem i zostać

[16] M. Apuzzo, M.S. Schmidt, J. Preston, *U.S. Visa Process Missed San Bernardino Wife's Online Zealotry*, http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html?_r=0 [dostęp: 15 IV 2018].

[17] R.A. Serrano, *FBI chief: San Bernardino shooters did not publicly promote jihad on social media*, http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html [dostęp: 15 IV 2018].

[18] Por. B. Ross i in., *Secret US Policy blocks agents from looping at social media of visa applicants, former official says,* http://abcnews.go.com/US/secret-us-policy-blocks-agents-social-media-visa/story?id=35749325 [dostęp: 15 IV 2018].

[19] Zob. *Terrorist Screening Center,* https://www.fbi.gov/about-us/nsb/tsc/tsc [dostęp: 15 IV 2018].

[20] Zob. *Schengen Information System*, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm [dostęp: 15 IV 2018].

uwzględnione w procedurach migracyjnych, tak aby w ten sposób móc realizować przynajmniej dwa cele: 1 – wcześnie wykrywać jednostki zradykalizowane i ekstremistów skłonnych do popełniania przestępstw, w tym terrorystycznych, 2 – wykrywać inne okoliczności, które mogą stanowić podstawę do odmowy prawa wjazdu na dany teren lub pobytu na tym terenie. Istnieje jednak wiele ograniczeń i zagrożeń, które należy uwzględniać przy ewentualnym wykorzystaniu tego rodzaju narzędzi. Pozyskiwanie i analiza informacji ze źródeł otwartych powinny być prowadzone w sposób zorganizowany, co nie zawsze jest przestrzegane[21]. W dalszej części artykułu zostaną przedstawione najważniejsze elementy omawianej koncepcji, tj. pozyskiwanie istotnych danych ze źródeł jawnych. Po pierwsze konieczne jest bliższe określenie sposobu, w jaki może być prowadzone sprawdzanie mediów społecznościowych przez służby migracyjne. Po drugie równie istotne jest zidentyfikowanie konkretnych problemów i ograniczeń wynikających ze stosowania takiej metody.

Dane wejściowe

Oczywiste może się wydać porównanie poszukiwania w Internecie potencjalnych sprawców ataków terrorystycznych z szukaniem igły w stogu siana. Częstym problemem z technikami opartymi na narzędziach SOCMINT jest konieczność przebrnięcia przez ogromną liczbę danych, aby podczas ich analizy móc wyodrębnić informacje nadające się do wykorzystania[22]. Osoby zatrudnione do obsługi procesów migracyjnych (m.in. do decydowania o wydaniu wizy) mają jednak w tym zakresie ogromną przewagę w postaci dostępu do pewnych, weryfikowalnych i relatywnie kompletnych danych na temat osoby starającej się o wjazd (podanych przez nią osobiście w urzędowych formularzach). Takie informacje można wykorzystać jako dane wstępne w celu stworzenia „filtra" danych służących de facto odwróceniu procesu monitoringu Internetu – zamiast poszukiwania „niebezpiecznych" treści w celu ich przypisania do konkretnego autora, przeszukiwanie zasobów otwartych może polegać na poszukiwaniu treści związanych z konkretnymi i znanymi osobami w celu ich sprawdzenia. W ten sposób proces wykrywczy ulega transformacji – zamiast poszukiwania informacji o charakterze zmiennej „nieznanej nieznanej" (tj. o zagrożeniach nieznanych pochodzących od osób nieznanych) poszukuje się informacji o cechach „znanej nieznanej" (tj. o zagrożeniach nieznanych, ale pochodzących od osób znanych), co jest relatywnie skuteczniejsze i prostsze w wykonaniu[23].

[21] Część funkcjonariuszy australijskich służb granicznych podczas poufnych wywiadów badawczych przyznaje, że chociaż nie istnieje tam oficjalna procedura korzystania z informacji pochodzących z mediów społecznościowych, to stosują te techniki z własnej inicjatywy, w celu zweryfikowania osób wjeżdżających do kraju.

[22] D. Omand, J. Bartlett, C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 3, s. 6–7.

[23] Zob. N.N. Taleb, *Black Swan. The impact of the highly improbable*, New York 2007, s. 127, 272.

Konkretne dane wejściowe dostępne służbom migracyjnym różnią się w zależności od szczegółowych rozwiązań prawnych obowiązujących w różnych krajach. Przykładowo więc obywatel zachodniej Europy podróżujący do Australii w celu uzyskania tzw. wizy elektronicznej musi podać tamtejszym służbom swoje podstawowe dane osobowe (tj. imię, nazwisko, płeć, datę urodzenia, dane paszportowe i kraj zamieszkania) oraz działający adres mejlowy. Obywatel Egiptu chcący odwiedzić Polskę musi natomiast przekazać również swój wizerunek (zdjęcie) i wiele innych dokumentów, o które może go poprosić konsulat RP (np. zaświadczenie o niekaralności)[24]. W przypadku wiz na pobyty długoterminowe wymogi we wszystkich krajach są zwykle większe. Z założenia jednak podstawowy zestaw danych na temat osoby starającej się o legalny wjazd na podstawie wizy, który może być wykorzystany przy przeszukiwaniu zasobów otwartych i który jest dostępny dla służb, obejmuje co najmniej najważniejsze dane osobowe, adres mejlowy, adres domowy, zdjęcie itp. Często są to wystarczające dane, aby skutecznie zidentyfikować i zweryfikować tożsamość internetową konkretnej osoby – o ile nie stara się ona aktywnie zamaskować swoich aktywności.

Dostęp

Po utworzeniu „filtra" danych wejściowych konieczne jest ustanowienie odpowiedniego dostępu do adekwatnych źródeł danych online. Jedną z możliwości jest zwrócenie się o pomoc wprost do usługodawców prowadzących media społecznościowe. Jednak zazwyczaj nie są oni otwarci na dobrowolną współpracę, zwłaszcza z zagranicznymi (z ich perspektywy) instytucjami rządowymi. Jeżeli uzyskanie danych bezpośrednio od usługodawców jest w ogóle możliwe, to zwykle jest konieczne pozyskanie odpowiednich (tj. respektowanych przez adresata) nakazów władz[25]. Niektórzy dostawcy usług aktywnie zwalczają tego rodzaju próby pozyskiwania informacji przez służby[26] lub publikują „raporty transparentności" na temat ich żądań[27]. Jakkolwiek pozytywnie można by było to oceniać z perspektywy prawa jednostek do prywatności, to faktem jest, że takie działania stanowią przeszkodę w prowadzeniu czynności wywiadowczych. Obecnie jest za wcześnie, aby ocenić, w jaki sposób w dłuższej perspektywie będzie się zmieniać podejście i usługodawców, i użytkowników do prywatności ich

[24] Ministerstwo Spraw Zagranicznych RP, system eKonsulat, https://secure.ekonsulat.gov.pl/Uslugi/RejestracjaTerminu.aspx?IDUSLUGI=1&IDPlacowki=157 [dostęp: 15 IV 2018].

[25] Zob. m.in.: Facebook, *Information for law Enforcement Authorities*, https://scontentfra31.xx.fbcdn.net/hphotosxfp1/t39.23656/12532957_530107840495531_2074830868_n.pdf [dostęp: 15 IV 2018]; Twitter, *Guidelines for law enforcement*, https://support.twitter.com/articles/41949# [dostęp: 15 IV 2018].

[26] A. Fine, *Twitter appeals ruling in bat tle over occupy Wall Street protester's information*, https://www.aclu.org/blog/twitter-appeals-ruling-battle-over-occupy-wall-street-protesters-information?redirect=blog/technology-and-liberty-national-security-free-speech/twitter-appeals-ruling-battle-over-occupy [dostęp: 15 IV 2018].

[27] Zob. *Google Transparency Report*, https://www.google.com/transparencyreport/userdatarequests/#! [dostęp: 15 IV 2018].

danych, chociażby w kontekście głośnej sprawy udostępniania informacji podmiotom trzecim przez Facebook[28].

Pozyskiwanie danych ze źródeł otwartych nie opiera się jednak na zdobywaniu dostępu do nich kanałami oficjalnymi ani na gromadzeniu informacji, do których dostęp jest przez użytkowników zastrzeżony. Opiera się na założeniu, że wiele przydatnych i znaczących informacji jest dostępnych publicznie. Podobnie rzecz się ma w odniesieniu do profili w mediach społecznościowych. Oczywiście, użytkownicy świadomi swojej prywatności i potrzeby jej ochrony nie korzystają z takich mediów ani nie publikują treści, które mogą ich w jakikolwiek sposób narazić na niebezpieczeństwo, albo korzystają z „ustawień prywatności" skonfigurowanych tak, aby osoby trzecie nie miały bezpośredniego dostępu do publikowanych informacji. Takie działanie stanowi kolejną przeszkodę w zastosowaniu technik SOCMINT. Równocześnie jednak zaskakująco wysoka liczba użytkowników mediów społecznościowych utrzymuje swoje profile w całości, lub przynajmniej częściowo, widoczne – nawet dla osób niezarejestrowanych.

Możliwości w zakresie dostępu do danych źródłowych mogą być zwiększone dzięki wykorzystaniu szczególnych metod i narzędzi oraz rozbudowanych zintegrowanych systemów pozyskiwania informacji ze źródeł otwartych. W zasadzie głównym narzędziem jest zakładanie „fałszywych kont" w mediach społecznościowych w taki sposób, aby pozyskujący dane mógł się uwierzytelnić na platformie społecznościowej jako użytkownik zarejestrowany, a tym samym – zyskać większy dostęp do przetwarzanych wiadomości. Pomimo tego, że jest to na ogół wbrew regulaminom poszczególnych usług społecznościowych[29] i wytycznym przełożonych, taka metoda jest relatywnie często wykorzystywana przez funkcjonariuszy organów ścigania[30]. Przy czym, uzyskiwanie dostępu do informacji oraz ich zdobywanie może następować kompleksowo lub częściowo, w formie procesu zautomatyzowanego, bez konieczności uciążliwego ręcznego „klikania" w treści na portalu społecznościowym. Na rynku działa już wiele systemów i programów komercyjnych wyspecjalizowanych w zbieraniu informacji z internetowych źródeł otwartych. Tego typu systemy oraz programy są w pełni dostępne także dla instytucji państwowych. Mogą one być dostosowywane na zamówienie w celu spełnienia ich określonych potrzeb i zapewnienia tym samym możliwości efektywnego kosztowo zbierania informacji wywiadowczych[31].

---

[28] D. Ingram, *Facebook says data leak hits 87 million sers, widening privacy skandal*, https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM [dostęp: 15 IV 2018].

[29] Teoretycznie wszyscy użytkownicy Facebooka są zobowiązani regulaminem do używania swoich prawdziwych imion i nazwisk. Zob. *Facebook community standards*, https://www.facebook.com/communitystandards [dostęp: 15 IV 2018].

[30] W początkowo niejawnych wytycznych Facebooka dla organów ścigania zawarto prośbę o niekorzystanie z fałszywych kont w celu prowadzenia postępowań. Zob. *Facebook law enforcement guidelines*, 2010, https://info.publicintelligence.net/Facebook2010-2.pdf [dostęp: 15 IV 2018].

[31] Kilku dużych dostawców oprogramowania, m.in. Symantec, Oracle czy Wynyard, oferuje „systemy pozyskiwania danych" (producenci stosują tu różną terminologię, jednak w każdym przy-

Ocena i weryfikacja

Po utworzeniu wstępnego filtra danych wejściowych i uzyskaniu dostępu do źródeł informacji o jednostce weryfikowanej najważniejszą fazą sprawdzania bezpieczeństwa jest ocena wiedzy zgromadzonej w ten sposób. Dokonując jej, należy mieć na uwadze treść i rodzaj pozyskanych informacji oraz zakładane wymogi bezpieczeństwa i kryteria przyznania prawa wjazdu do kraju.

Wiele wymogów wizowych (np. dotyczących stanu zdrowia czy niekaralności) może być weryfikowanych dzięki informacjom pozyskanym ze źródeł otwartych. Istotne jest przy tym zwracanie uwagi na to, które dane mogą być w takiej weryfikacji pomocne i gdzie ich szukać. Przede wszystkim należy zwrócić uwagę na treści zamieszczone na profilu społecznościowym przez osobę sprawdzaną. Ze względu na wspomniane wcześniej zjawisko „naddzielenia się" przez użytkowników informacjami prywatnymi treści przez nich publikowane nierzadko mogą dostarczyć wiarygodnych i rzetelnych podstaw do odmowy prawa wjazdu (na przykład, gdy są wymagane przymioty niekaralności za przestępstwa i niebycia podmiotem bieżących postępowań karnych). Niekiedy oświadczenia w tym zakresie mogą być negatywnie zweryfikowane na podstawie publikowanych treści wskazujących na przeszłe lub bieżące problemy z prawem. Wielokrotnie się zdarzało, że zdjęcie umieszczone w mediach społecznościowych, a odnalezione przez organy ścigania, stanowiło podstawę do wszczęcia stosownego postępowania[32]. Nie ma więc powodu, aby nie korzystać z tego narzędzia podczas procedur migracyjnych i wizowych.

Oprócz treści wytworzonych i publikowanych bezpośrednio przez użytkowników należy zwrócić uwagę na informacje pośrednie: treści „udostępnione", strony „polubiane", statusy, zdjęcia, grupy, do których należy użytkownik itp. (dotyczy to takich stron, jak Facebook i Twitter, ale też innych platform z mikroblogami czy mediów społecznościowych, choć szczegółowa terminologia dotycząca m.in. „udostępniania" i „polubień" będzie się różniła w odniesieniu do poszczególnych z nich). Takie treści mogą wskazywać na zainteresowania i poglądy, które mogą wywołać uzasadnione podejrzenie co do intencji danej osoby. Zwłaszcza w przypadku potencjalnych sprawców przestępstw terrorystycznych znaczenie może mieć wczesne ujawnienie oznak radykalizacji; osoba, która śledzi strony publikujące propagandę terrorystyczną, może być podejrzewana o zainteresowanie działalnością o takim charakterze[33].

Dokonując oceny i selekcji zgromadzonych informacji na podstawie analizy profili w mediach społecznościowych w kontekście zagrożenia ze strony terrorystów indywidualnych, w odpowiedni sposób należy oceniać również mniej niebezpieczne

padku chodzi o oprogramowanie wywiadowcze dostępne na rynku komercyjnym).

[32] Istnieje wiele rodzajów i przykładów takich zachowań. Zob. A. Shontell, *7 People who were arrested because of something they wrote on Facebook*, http://www.businessinsider.com/people-arrested-for-facebook-posts-2013-7?IR=T [dostęp: 15 IV 2018].

[33] Zob. J. Klausen, *Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq*, „Studies in Conflict and Terrorism" 2015, nr 38, s. 1–22.

treści. Dotychczasowe badania przeprowadzone w tym zakresie wskazują na wiele tzw. zachowań ostrzegawczych w Internecie i mediach społecznościowych, których wystąpienie może sugerować skłonność lub planowanie agresji (zostały one szczegółowo opisane)[34]. To, czy wystąpienie tego rodzaju „znaku ostrzegawczego" powinno skutkować odmową wjazdu na teren kraju (a niekiedy również innymi konsekwencjami, np. objęciem danej osoby kontrolą operacyjną), musi jednak być zależne od przyjętej polityki wewnętrznej.

Zagrożenia i przeszkody

Wykorzystywanie informacji zgromadzonych w wyniku przeszukiwania mediów społecznościowych przy ocenie aplikacji wizowych jest związane z wieloma poważnymi zagrożeniami i przeszkodami. Wiedza o nich oraz spójne zasady wewnętrzne określające metody prowadzenia działań i reagowania na poszczególne zagrożenia muszą być istotnym elementem wdrażania technik SOCMINT. Spośród najistotniejszych zagadnień należy wymienić weryfikację tożsamości online, bariery językowe i kulturowe oraz problemy organizacyjne, prawne, etyczne, a także związane z podejmowaniem decyzji ostatecznych.

Prawdziwa tożsamość

Pomimo tego, że teoretycznie dostawcy usług mediów społecznościowych wymagają od swoich użytkowników posługiwania się prawdziwymi danymi osobowymi, w praktyce jest to zasada nagminnie nieprzestrzegana[35]. Stąd wynika jeden z najpoważniejszych problemów związanych z próbą precyzyjnego zebrania informacji z tego typu źródeł. Alias może być używany ze względu na chęć ochrony prywatności – jako dokładnie przemyślana lub intuicyjna decyzja dotycząca niepublikowania w Internecie własnych danych (co skądinąd zasługuje na pochwałę z punktu widzenia indywidualnych zasad bezpieczeństwa). Niektóre fałszywe profile są tworzone celowo, aby móc podszywać się pod inną osobę albo dręczyć innych użytkowników i popełniać przestępstwa. Niezależnie od powodu używania aliasu, ogranicza on możliwość rzetelnego ustalenia tożsamości autora treści wyłącznie na podstawie danych otwartych. Osoba prowadząca czynności wywiadowcze musi brać pod uwagę, że nawet jeśli dane osobowe wskazane w profilu są prawdziwe, to nie musi to oznaczać, że ten profil należy

[34] Istotne jest to, że istnieje możliwość wykrycia niektórych rodzajów „zachowań ostrzegawczych" w Internecie dzięki szczegółowej analizie mediów społecznościowych (np. przez wykrywanie specyficznych konstrukcji językowych świadczących o poszczególnych zachowaniach). Zob. K. Cohen i in., *Detecting linguistic markers for radical violence in social media*, „Terrorism and Political Violence" 2014, nr 26/1, s. 246–256; J. Reid Meloy, *Identifying warning behaviors of the individual terrorist*, http://drreidmeloy.com/wp-content/uploads/2016/05/2016_Individual-Terrorist.pdf [dostęp: 15 IV 2018].

[35] Zob. K. Raynes-Goldie, *Aliases, creeping and wall clearing: understanding privacy in the age of Facebook,* „First Monday" 2010, nr 1–4 (sic!).

do osoby sprawdzanej. Szczególnie mylące i niepozwalające na rzetelną weryfikację są imiona i nazwiska – w takim samym zestawieniu może je bowiem nosić wiele osób. Przykładowo, wyszukanie imienia i nazwiska konkretnej osoby wśród kont na Twitterze ujawni co najmniej kilka kont, z których żadne może nie być kontem tej osoby[36].

Niestety, nie ma idealnej metody weryfikacji wątpliwych tożsamości online wyłącznie na podstawie źródeł otwartych i bez konfrontowania danej osoby z nimi (lub sięgania po dodatkowe dane spoza źródeł otwartych). Najlepsze możliwe rozwiązania tego problemu opierają się na tym, aby: 1 – zdobyte informacje weryfikować krzyżowo z posiadanymi już danymi o wyszukiwanej osobie (istotne mogą być także dane dotyczące relacji tej osoby z innymi osobami, np. z członkami rodziny, którzy również mogą mieć konta w mediach społecznościowych), 2 – być niezwykle ostrożnym przy wyciąganiu jakichkolwiek konsekwencji wyłącznie na podstawie treści odnalezionych online.

Bariery językowe i kulturowe

Istotny problem przy gromadzeniu i analizie danych publikowanych online przez służby migracyjne mogą stanowić bariery językowe i kulturowe. Z oczywistych względów użytkownicy mediów społecznościowych znajdujący się w kręgu zainteresowań pracowników i funkcjonariuszy takich służb będą się na ogół posługiwali obcymi językami narodowymi, niekoniecznie znanymi osobie, która ich weryfikuje. Ten problem można rozwiązać na poziomie organizacyjnym jedynie częściowo – przez zatrudnianie osób o wysokich kwalifikacjach językowych. Narzędziem stosowanym pomocniczo może być także tłumaczenie maszynowe (automatyczne), zwłaszcza przy uwzględnieniu stale rosnącej jakości tego typu usług. Może ono pozwolić na zredukowanie wymaganych umiejętności lingwistycznych wywiadowcy[37].

Różnice kulturowe i brak wiedzy mogą przeszkodzić służbom migracyjnym w zrozumieniu wielu informacji także ze względu na brak znajomości odpowiednich kontekstów czy znaczeń. Bez odpowiedniej wiedzy na temat chociażby bieżących trendów w światowej czy regionalnej propagandzie terrorystycznej wyłonienie treści, które się do niej odwołują, może być znacznie utrudnione. Jako przykład takiego problemu może posłużyć wykorzystywanie przez Państwo Islamskie w 2014 r. oznaczenia #Brazil2014 nawiązującego do trwających wówczas mistrzostw świata w piłce nożnej w celu propagowania materiałów ekstremistycznych[38]. Każda osoba publikująca treści

[36] Przykładowo, przeszukanie wspomnianego portalu społecznościowego pod kątem użytkowników o takim samym imieniu i nazwisku, jak autora niniejszego artykułu, ujawni kilka kont, z których żadne nie jest przez niego prowadzone. Tak prosty „eksperyment" może być powtórzony z wykorzystaniem dowolnych danych osobowych. Z przyczyn etycznych autor artykułu postanowił przedstawić problem na własnym przykładzie.

[37] K. Cohen i in., *Detecting linguistic markers*…, s. 251.

[38] C. Milmo, *Iraq crisis exclusive: Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter*¸ http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promo-

z tym oznaczeniem mogła więc być albo rzeczywistym fanem piłki nożnej, albo ekstremistą wspierającym terroryzm. Rozróżnienie takich osób wymagało odpowiedniej wiedzy. Podobne problemy można rozwiązać jedynie częściowo – przez prowadzenie szkoleń wewnętrznych i właściwą politykę kadrową.

Problemy prawne i etyczne

Gromadzenie informacji ze źródeł otwartych na podstawie dostarczonych formularzy wizowych może wywoływać wiele pytań o zgodność takiego działania z przepisami prawa i zasadami etyki. Dane z mediów społecznościowych na ogół będą stanowiły „dane osobowe", których gromadzenie i przetwarzanie podlega ścisłym regułom – zwłaszcza prawo obecnie obowiązujące na terenie Unii Europejskiej czyni pozyskiwanie takich informacji problematycznym[39]. Nie przekreśla to szerokiego wykorzystania opisywanych działań, ale może wymusić zmiany w obowiązującym prawie lub szczegółową analizę wymogów, które dotyczą ich legalności.

Częściowym rozwiązaniem może być pozyskanie od samych zainteresowanych zgody na przetwarzanie ich danych, w treści obejmującej zgodę na weryfikację informacji na ich temat opartą na technikach SOCMINT. Pozwoliłoby to na przesunięcie całego procesu poza prawno-etyczną „szarą strefę", ale jednocześnie niesie za sobą zagrożenie zaalarmowania sprawdzanych osób, które w związku z tym mogą starać się usunąć lub ukryć część dostępnych treści. Aby tego uniknąć, należy rozważyć, w jaki sposób można zredagować formularz zgody stanowiący część dokumentów w sprawie aplikacji wizowej i w ten sposób zmniejszyć to ryzyko bez ujawniania zbyt wielu informacji o procesie weryfikacyjnym. Podobnego typu zgody były już stosowane zarówno w sektorze publicznym, jak i prywatnym[40]. Jednak zbyt ogólnikowy formularz zgody może być niewystarczający do spełnienia wymogów prawnych, szczególnie w odniesieniu do gromadzenia danych wrażliwych. Te kwestie muszą być skrupulatnie rozważone przy wdrażaniu jakiejkolwiek polityki.

Podejmowanie decyzji

Po odnalezieniu podejrzanych treści w mediach społecznościowych niezwykle istotne jest uwzględnianie przy ocenie wszystkich ograniczeń, aby wykluczyć możliwość wystąpienia nieporozumień. Treści zamieszczane w Internecie często można źle zrozumieć, fałszywie przypisać ich autorstwo określonej osobie, błędnie uznać za prawdziwe,

te-9555167.html [dostęp: 15 IV 2018].

[39] Zob. zwłaszcza *Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych osobowych)*.

[40] Zob. m.in. wzór formularza ankiety bezpieczeństwa dla kandydatów do służby cywilnej w Kanadzie, http://www.fja-cmf.gc.ca/appointments-nominations/forms-formulaires/bc-va/bc-va.pdf [dostęp: 15 IV 2018].

podczas gdy są one kłamliwe lub żartobliwe. Przykładowo, publikacja, która miała mieć charakter żartobliwy, spowodowała problemy w sprawie L. van Bryana i E. Bunting – pary podróżującej z Wielkiej Brytanii do Stanów Zjednoczonych, która przed podróżą zamieściła na Twitterze informację o tym, że jedzie „zniszczyć Amerykę". Pomimo tego, że ich zamiarem wyrażonym w ten sposób było spędzanie czasu na imprezach w klubach i barach, kontekst tej informacji nie został rzeczywiście wzięty pod uwagę przez amerykańskie służby. Parze odmówiono prawa wjazdu do Stanów Zjednoczonych i zawrócono ją z granicy USA[41]. Inny przykład dotyczy osoby, która ubiegała się o tygodniową wizę turystyczną i która bezpośrednio przed wyjazdem opublikowała długą wiadomość pożegnalną skierowaną do znajomych. Wynikało z niej, że planuje wielomiesięczną nieobecność w kraju ojczystym. Takie zachowanie mogło wskazywać na chęć przekroczenia terminu dozwolonego pobytu, ale również – na ewentualny wyjazd po jego upływie do innych państw lub nawet zmianę rodzaju wizy z turystycznej na pobytową wkrótce po przyjeździe (np. w związku z zawarciem planowanego małżeństwa)[42].

Co do zasady prawdziwe jest stwierdzenie, że skuteczne wykorzystanie informacji wywiadowczych nie polega li tylko na samym ich gromadzeniu, ale że sukces jest uzależniony od wartości, jaką takie informacje wniosą przy podejmowaniu określonych decyzji[43]. Tym samym najistotniejszą częścią całego procesu jest ocena zgromadzonych danych i odniesienie się do tej oceny przy podejmowaniu decyzji w sprawach wizowych (przy założeniu, że celem jest przestrzeganie rzetelnej i spójnej procedury migracyjnej). Przy czym jest niezbędne ustalenie odpowiedniej i sformalizowanej polityki wewnętrznej w tym zakresie. Dzięki temu osoby odpowiedzialne za przebieg procesów migracyjnych i podejmowanie wiążących decyzji nie powinny być zdane na opieranie się w tej sprawie wyłącznie na własnym przeczuciu co do tego, w jaki sposób należy reagować w konkretnych sytuacjach. Konieczne jest więc zdefiniowanie zasad stosowania technik SOCMINT obejmujących szczegółowe wytyczne i wskazówki dotyczące nie tylko technik i możliwości gromadzenia danych ze źródeł otwartych, lecz także tego, w jaki sposób należy reagować w określonych sytuacjach, jakie treści powinny być uznane za „interesujące" i kwalifikujące się do dalszego sprawdzenia, kiedy i jakie informacje należy weryfikować w innych źródłach, kiedy prosić o dodatkowe dokumenty czy też w jakim momencie i na jakich warunkach osobiście konfrontować daną osobę z pozyskanymi informacjami jeszcze przed podjęciem decyzji ostatecznej.

[41] R. Hartley-Parkinson, *I'm going to destroy America and dig up Marilyn Monroe': British pair arrested in the US on terror charges over Twitter jokes*, http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes, html [dostęp: 15 IV 2018].

[42] Sprawa została zrelacjonowana podczas wywiadu badawczego z przedstawicielem australijskiej agencji rządowej (szczegółowe dane nie zostały ujawnione ze względu na konieczność zachowania poufności).

[43] D. Omand, J. Bartlett, C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 1, s. 7.

Wnioski i rekomendacje

Wykorzystanie technik SOCMINT bez wątpienia stwarza wiele możliwości wszelkim podmiotom państwowym i prywatnym, w tym zwłaszcza dbającym o utrzymanie bezpieczeństwa wewnętrznego. Zastosowanie tych technik w procesie migracyjnym, przy weryfikacji osób starających się o prawo wjazdu do danego kraju czy pobytu na jego terenie, może pozwolić na uzyskanie dodatkowej warstwy ochronnej w kontekście zagrożeń terrorystycznych, jak również może służyć weryfikacji danych prawnie relewantnych (tj. wpływających na prawo do wjazdu), podawanych przez takie osoby. Służby wizowe i migracyjne dysponują kompletnymi zestawami danych osobowych, które mogą służyć za „filtr danych wejściowych" w celu przeprowadzenia sprofilowanych przeszukań źródeł otwartych. Jednocześnie przy wykorzystywaniu tego rodzaju informacji należy pamiętać o uwzględnianiu obowiązujących norm prawnych.

Dzięki ocenie treści zamieszczonych na profilu społecznościowym jest możliwe ujawnienie zagrożeń bezpieczeństwa lub informacji stanowiących podstawę do odmowy wydania decyzji dotyczącej prawa wjazdu. Skutki odmowy wjazdu lub pobytu na terytorium danego kraju mogą być dla zainteresowanego bardzo poważne na gruncie prywatnym. Z tego powodu należy ze szczególną ostrożnością uwzględniać potencjalne problemy z tym związane, a cała procedura musi być prowadzona z przestrzeganiem zasady domniemania niewinności (stosowanej tu odpowiednio i w specyficznym rozumieniu). Biorąc pod uwagę wielość możliwości i zagrożeń wynikających z wykorzystania technik SOCMINT w procesie migracyjnym, należy opowiedzieć się za każdorazowym tworzeniem wewnątrzinstytucjonalnej polityki ich stosowania. W celu ograniczenia kosztów i zminimalizowania różnych rodzajów ryzyka polityka wewnętrzna powinna odnosić się do takich spraw, jak to, kiedy przeprowadzać weryfikację (czy wszyscy kandydaci powinni być sprawdzani, czy tylko niektóre ich grupy, np. odwiedzający kraj po raz pierwszy?), jakie narzędzia powinny być wykorzystywane przy weryfikacji (czy ewentualnie planuje się wdrożenie specjalistycznego oprogramowania?), gdzie poszukiwać informacji, jak je weryfikować (czy kandydat powinien być konfrontowany z pozyskanymi informacjami?) i czym się należy kierować na ostatecznym etapie procesu decyzyjnego. Stworzenie tego rodzaju wewnętrznego regulaminu działania powinno być wsparte również przez prowadzenie adekwatnych szkoleń merytorycznych. Można założyć, że wykorzystywanie danych ze źródeł jawnych w różnych obszarach życia publicznego i procedurach bezpieczeństwa będzie się pogłębiać. Już dziś trzeba poszukiwać najefektywniejszych sposobów wykorzystania SOCMINT w celu zapewnienia bezpieczeństwa.

Bibliografia:

Arslan C., Yanuk M., *A New Discipline of Intelligence: Social Media*, Istanbul 2015, ICMSS.

Benson D.C., *Why the Internet is not increasing terrorism*, „Security Studies" 2014, nr 23/2, s. 6.

Cohen K. i in., *Detecting linguistic markers for radical violence in social media*, „Terrorism and Political Violence" 2014, nr 26/1, s. 246–256.

Dabhi M.D., *Geofencing: a generic approach to Real time location based tracking system*, „International Journal of Computer Networks and Wireless Communications" 2016, t. 6.

Hamm M., Spaaij R., *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies*, Washington 2015, US Department of Justice.

Kaplan A., Haenlein M., *Users of the world, Unite!*, „Business Horizons" 2010, nr 53/1.

Klausen J., *Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq*, „Studies in Conflict and Terrorism" 2015, nr 38.

Liaropoulos N., *The challenge of social media for the Intelligence community*, „Journal of Mediterranean and Balkan Intelligence" 2013, nr 1.

Omand D., Bartlett J., Miller C., *Introducing Social Media Intelligence (SOCMINT)*, „Intelligence and National Security" 2012, nr 1.

Paullet K., Pinchot J., *Cybercrime: the unintentional effects of oversharing information on Facebook*, Proceedings of the Conference on Information Systems Applied Research, New Orleans 2012, EDSIG-AITP.

Raynes-Goldie K., *Aliases, creeping and wall clearing: understanding privacy in the age of Facebook*, „First Monday" 2010, nr 1–4.

Taleb N.N., *Black Swan. The impact of the highly improbable*, New York 2007, Random House.

Apuzzo M., Schmidt M.S., Preston J., *U.S. Visa Process Missed San Bernardino Wife's Online Zealotry*, http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html?_r=0 [dostęp: 15 IV 2018].

Cooke K., *US Police used Facebook, Twitter data to track protesters*, http://www.reuters.com/article/social-media-data-idUSL4N1CH4J1 [dostęp: 15 IV 2018].

Facebook community standards, https://www.facebook.com/communitystandards [dostęp: 15 IV 2018].

Facebook, *Information for law Enforcement Authorities*, https://scontentfra31.xx.fbcdn.net/hphotosxfp1/t39.23656/12532957_530107840495531_2074830868_n.pdf [dostęp: 15 IV 2018].

Facebook law enforcement guidelines, 2010, https://info.publicintelligence.net/Facebook2010-2.pdf [dostęp: 15 IV 2018].

Full text of Gym Killer's blog, http://nypost.com/2009/08/05/full-text-of-gym-killers-blog/ [dostęp: 15 IV 2018].

Google Transparency Report, https://www.google.com/transparencyreport/userdatarequests/#! [dostęp: 15 IV 2018].

Hartley-Parkinson R., *'I'm going to destroy America and dig up Marilyn Monroe': British pair arrested in the US on terror charges over Twitter jokes*, http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html [dostęp: 15 IV 2018].

http://www.fp7-prime.eu/home_page [dostęp: 15 IV 2018].

Ingram D., *Facebook says data leak hits 87 million sers, widening privacy skandal*, https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM [dostęp: 15 IV 2018].

Milmo C., *Iraq crisis exclusive: Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter*, http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promote-9555167.html [dostęp: 15 IV 2018].

Ministerstwo Spraw Zagranicznych RP, *System eKonsulat*, https://secure.ekonsulat.gov.pl/Uslugi/RejestracjaTerminu.aspx?IDUSLUGI=1&IDPlacowki=157 [dostęp: 15 IV 2018].

O'Brien B., *U.S. visa applicants to be asked for social media history: State Department*, https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P [dostęp: 15 IV 2018].

Reid Meloy J., *Identifying warning behaviors of the individual terrorist*, http://drreidmeloy.com/wp-content/uploads/2016/05/2016_IndividualTerrorist.pdf [dostęp: 15 IV 2018].

Ross B. i in., *Secret US Policy blocks agents from looping at social media of visa applicants, former official says*, http://abcnews.go.com/US/secret-us-policy-blocks-agents-social-media-visa/story?id=35749325 [dostęp: 15 IV 2018].

Schengen Information System, http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm [dostęp: 15 IV 2018].

Serrano R.A., *FBI chief: San Bernardino shooters did not publicly promote jihad on social media*, http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html [dostęp: 15 IV 2018].

Shontell A., *7 People who were arrested because of something they wrote on Facebook*, http://www.businessinsider.com/people-arrested-for-facebook-posts-2013-7?IR=T [dostęp: 15 IV 2018].

Social media use in law enforcement: crime prevention and investigative activities continua to driver usage, https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf [dostęp: 15 IV 2018].

Terrorist Screening Center, https://www.fbi.gov/about-us/nsb/tsc/tsc [dostęp: 15 IV 2018].

Twitter appeals ruling in bat tle over occupy Wall Street protester's information, https://www.aclu.org/blog/twitter-appeals-ruling-battle-over-occupy-wall-street-protesters-information?redirect=blog/technology-and-liberty-national-security-free-speech/twitter-appeals-ruling-battle-over-occupy [dostęp: 15 IV 2018].

Twitter, *Guidelines for law enforcement*, https://support.twitter.com/articles/41949# [dostęp: 15 IV 2018].

Abstrakt

Monitoring Internetu i analiza danych ze źródeł otwartych stanowią istotną część działań antyterrorystycznych o charakterze prewencyjnym. Bogactwo informacji i danych osobowych możliwych do odnalezienia w mediach społecznościowych jest wykorzystywane nie tylko do zwalczania zagrożeń terrorystycznych, lecz także do walki z przestępczością kryminalną. Artykuł opisuje możliwości i zagrożenia związane z potencjalnym wykorzystywaniem tzw. *Social Media Intelligence* (SOCMINT) w procedurach migracyjnych w celu zagwarantowania bezpieczeństwa wewnętrznego.

Słowa kluczowe: terroryzm, migracja, OSINT, SOCMINT, media społecznościowe.

Marek Świerczek

„System matrioszek”[1], czyli dezinformacja doskonała. Wstęp do zagadnienia

Wstęp

Aby zrozumieć, na jakich zasadach opiera się rosyjski system dezinformacji, trzeba wyjść od precyzyjnego zdefiniowania tego zjawiska. Ostatnimi czasy pojęcie dezinformacja nabrało niezwykle szerokiego znaczenia. Rozmywa ono jednak granice definicyjne tego zjawiska, a nade wszystko ma skutki praktyczne w postaci wychwytywania przez domorosłych tropicieli rosyjskich spisków coraz to nowych przejawów „dezinformacji”, pojmowanej najczęściej jako każde działanie informacyjne ukierunkowane na wywieranie wpływu na postawy obywateli państw – ofiar. W ten sposób pod pojęciem dezinformacja rozumie się zarówno propagandę (we wszystkich jej odmianach, włącznie z propagandą uprawianą jawnie przez rosyjskie media państwowe), jak i tzw. *fake news*, które często są z upodobaniem pozyskiwane i analizowane jako niezwykle poważne zagrożenie bezpieczeństwa państwa, choć jak dotąd nie ma wiarygodnych wyników badań, wskazujących na długofalową skuteczność posługiwania się nimi.

Zasadniczym rezultatem rozszerzania zakresu znaczeniowego pojęcia dezinformacja jest przeniesienie uwagi ze zjawiska niezwykle groźnego na zjawiska o znaczeniu marginalnym. Mówiąc obrazowo: prawdziwa dezinformacja tonie w kakofonii medialnych doniesień na temat fałszywych wiadomości i przejawów nachalnej propagandy Kremla, co sprawia, że rzeczywista dezinformacja, pozbawiona działań osłonowych ze strony kontrwywiadu, staje się jeszcze bardziej szkodliwa. Przede wszystkim więc jest konieczne bardziej precyzyjne zdefiniowanie pojęcia dezinformacja. W ocenie autora reprezentatywne dla większości prac poświęconych temu zagadnieniu są niżej przytoczone definicje tego zjawiska:

1. (…) wyjątkowo złożona metoda pracy operacyjnej, będąca sposobem oddziaływania na aktualnego czy potencjalnego przeciwnika, wrogą służbę specjalną bądź określone grupy czy warstwy społeczne w innym, ale niekiedy też i własnym kraju. Termin wymyślony przez niemieckie służby specjalne w czasie I wojny światowej; przy sztabie armii niemieckiej do końca działań wojennych istniała komórka dezinformacyjna sterowana przez wojskową służbę wywiadowczą. Później służby specjalne innych państw wpro-

[1] Matrioszka (ros. матрёшка, zdrobnienie od imienia Matriona) – rosyjska zabawka złożona z drewnianych, wydrążonych w środku lalek, włożonych jedna w drugą.

wadziły tę formę działania jako metodologiczny sposób oddziaływania na przeciwnika, podejmowany z zamiarem wykreowania celowego, ukierunkowanego wpływu na kształtowanie opinii i bieg możliwych do przewidzenia zdarzeń. Dezinformacja to zaplanowane według jednolitej koncepcji tajne działanie polegające na przygotowaniu, opracowaniu i w konsekwencji podsunięciu/podrzuceniu/przekazaniu przeciwnikowi (jego służbie specjalnej) lub jawnym rozpowszechnianiu, ale z ukrytymi celami, w społeczeństwie kraju przeciwnika częściowo lub całkowicie fałszywych informacji, dokumentów (pism, listów, publikacji, rękopisów itp.), zdjęć lub w innej formie spreparowanych danych, mających wytworzyć pozornie prawdziwy obraz lub pogląd i kształtować opinię o osobie, zdarzeniu czy zjawisku zgodnie z operacyjnymi interesami służby specjalnej podejmującej działania dezinformacyjne lub/i politycznymi państwa, w interesie którego dana służba je realizuje, na ogół dla spowodowania bezpośredniej lub pośredniej szkody dla bieżących lub przyszłych interesów przeciwnika. Efektem takich działań jest wpływanie na procesy decyzyjne rozważane przez gremia innego państwa (rząd, parlament, organy gospodarcze), które mogą wykorzystywać takie informacje dla podejmowania decyzji szkodzących żywotnym interesom tego kraju[2].

2. Celowo fałszywa informacja, która ma wpłynąć na określoną grupę ludzi lub całą populację. Jest to jedna z podstawowych metod pracy operacyjnej wywiadu, służąca wpłynięciu na postępowanie przeciwnika, by zachował się korzystnie dla służby wywiadowczej. (Przeciwnikiem może być wrogi wywiad lub inna organizacja lub osoba, przeciwko której skierowane są działania służby). Dezinformacje dzieli się na strategiczne, o długoterminowych planach i zamierzeniach, oraz dezinformacje operatywne, które tworzy się w zależności od chwilowej sytuacji. Dezinformacja pod względem formy może być językowa, obrazowa lub demonstracyjna (prezentacja obiektów fizycznych)[3].
3. Tworzenie i rozprzestrzenianie mylącej lub fałszywej informacji w celu zniekształcenia obrazu przeciwnika[4].
4. Dezinformacja (…) jest celowym przekazywaniem przeciwnikowi, za pomocą środków i metod pracy operacyjnej, nieprawdziwych informacji w celu wprowadzenia go w błąd i uzyskania zaplanowanych rezultatów[5].
5. (…) istotą dezinformacji jest prowokacja, a nie kłamstwo (…) państwa używają swych wywiadów do malowania obrazu prowokującego przeciwnika do podejmowania błędnych ocen[6].
6. (…) dezinformacja stawia sobie za cel realizację konsekwentnego programu zmierzającego do zastąpienia w świadomości, a przede wszystkim podświadomości, mas będących przedmiotem tych działań poglądów uznanych za niekorzystne dla dezinformatora takimi, które uważa on za korzystne dla siebie[7].

---

[2] J. Larecki, *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warszawa 2007, s. 159–160.

[3] *Encyklopedia szpiegostwa*, K. Wojciechowski (tłum.), Warszawa 1995, s. 72–73.

[4] N. Polmar, T.B. Allen, *Księga szpiegów. Encyklopedia*, Warszawa 2000, s. 151.

[5] H. Lewandowski, *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, Warszawa 2000, s. 81–82.

[6] E.J. Epstein, *Podstęp. Niewidzialna wojna między KGB a CIA*, Krosno 1993, s. 31.

[7] *Dezinformacja – oręż wojny*, V. Volkoff (oprac.), Warszawa 1991, s. 8.

7. Termin ten oznacza systematyczne wysiłki zmierzające do rozprzestrzenienia nieprawdziwych informacji i do zafałszowania lub zablokowania informacji dotyczących rzeczywistej sytuacji i polityki świata komunistycznego. W konsekwencji praktyki dezinformacyjne miały doprowadzić do zmylenia, wprowadzenia w błąd i wpływania tendencyjnie na świat niekomunistyczny, do podważania jego polityki oraz do skłonienia przeciwnika z Zachodu do nieświadomego przyczyniania się do realizacji celów komunizmu[8].
8. *Disinformation actually is a special type of „black" propaganda which hinges on absolute secrecy and which is usually supported by false documents*[9] (Dezinformacja jest właściwie specjalnym rodzajem „czarnej propagandy" opartej na całkowitej tajności zwykle wspartej przez sfałszowane dokumenty – tłum. aut.).

Jak łatwo zauważyć, wyżej przytoczone definicje pojęcia dezinformacja mają kilka elementów wspólnych. Należy do nich m.in. stwierdzenie, że dezinformacja jest domeną służb specjalnych i że polega na wytworzeniu u przeciwnika fałszywego obrazu rzeczywistości, który ma go skłaniać do podejmowania błędnych decyzji. To zaś wymaga utrzymania w tajemnicy przede wszystkim źródła pochodzenia informacji oraz pozbawienia ofiary możliwości ich zweryfikowania (gdyż wtedy nie tylko można je sfalsyfikować, lecz także – na zasadzie *cui bono* – wytypować prawdopodobnego dezinformatora). W związku z tym wyżej wymienione elementy dezinformacji dyskwalifikują zarówno propagandę, jak i tzw. *fake news* (a także pozostałe formy wojny informacyjnej prowadzonej za pomocą mass mediów oraz Internetu) z bycia dezinformacją sensu stricto, gdyż o ile w ich przypadku da się utrudnić identyfikację rzeczywistego źródła informacji, o tyle jest wykluczone pozbawienie ofiary możliwości zweryfikowania danych. Ponadto teza, że prowadzenie szeroko rozumianej wojny informacyjnej jest domeną służb specjalnych, jest dyskusyjna, gdyż służby zwykle nie mają środków na działania propagandowe.

W celu uniknięcia problemów logicznych pojawiających się przy zbyt szerokim definiowaniu pojęcia dezinformacja, należy wyjść od prostej konstatacji polegającej na zrozumieniu, jak – w ogólnych zarysach – przebiegają procesy decyzyjne w ośrodkach władzy państwowej. Najprostszą ilustracją takiego procesu jest tzw. cykl wywiadowczy (przedstawiony na schemacie), pokazujący ścisły związek decyzji polityczno-wojskowych z informacjami dostarczanymi przez wyspecjalizowane agendy państwowe, w tym wywiad i kontrwywiad.

[8] A. Golicyn, *Nowe kłamstwa w miejsce starych*, Warszawa 2007, s. 6.
[9] V. Marchetti, J.D. Marks, *The CIA and the Cult of Intelligence*, New York 1974, s. 173.

Schemat. Cykl wywiadowczy pokazujący ścisły związek decyzji polityczno-wojskowych z informacjami dostarczanymi przez wyspecjalizowane agendy państwowe, w tym wywiad i kontrwywiad.

Źródło: J. Hughes-Wilson, *Największe błędy wywiadów świata*, Warszawa 2002, s. 13.

Upraszczając nieco powyższy schemat, należy powiedzieć (choć graniczy to z truizmem), że zdecydowana większość rządów podejmuje decyzje polityczno-wojskowe na podstawie zweryfikowanych i przeanalizowanych informacji przekazanych przez instytucje państwowe utworzone w celu ich zbierania i przetwarzania, a nie na podstawie propagandy przeciwnika, informacji medialnych, *fake news* itp.

Oczywiście, wpływanie na opinię publiczną przez prowadzenie działań informacyjnych w rodzaju fałszywych doniesień medialnych może w dłuższej perspektywie oddziaływać na funkcjonowanie państwa, np. przez napędzanie wyborców konkretnym ugrupowaniom politycznym lub uaktywnianie dynamiki dużych grup społecznych (prowokowanie zamieszek itp.), na co rządy muszą w jakiś sposób reagować. Jednak generalnie trzeba przyjąć, że w większości przypadków państwowe ośrodki decyzyjne dojrzałych demokracji działają na podstawie informacji uznawanych za wiarygodne, tj. pochodzących ze źródeł pewnych, takich jak służby państwowe, zwykle wyspecjalizowane w działalności rozpoznawczo-analitycznej. Przyjmując ten punkt widzenia, można zatem – na potrzeby niniejszego artykułu – przyjąć następującą definicję dezinformacji: **dezinformacja to proces wpływania na zachowanie podmiotu dezinformowanego przez zniekształcanie postrzegania przez niego rzeczywistości, prowadzące ofiarę dezinformacji do podejmowania działań zgodnych z obrazem zdeformowanym,**

a zarazem odpowiadających interesom podmiotu dezinformującego. Jest to proces planowany i przeprowadzany przez wyspecjalizowane instytucje państwowe, które dysponują odpowiednimi do tego zasobami i starają się zapanować nad różnymi kanałami uzyskiwania informacji przez podmiot dezinformowany[10].

Rzeczą najważniejszą dla powyższego ujęcia omawianego zagadnienia jest zrozumienie, że **do prowadzenia działań dezinformacyjnych jest niezbędne zapanowanie nad kanałami pozyskiwania informacji przez ofiarę tych działań**, czyli – krótko mówiąc – przeprowadzanie przez ofiarę działań dezinformacyjnych wywiadu dotyczącego wiarygodności kanałów informacji. Nie da się prowadzić skutecznej dezinformacji, gdy ofiara może zweryfikować zdobyte dane u innych, wiarygodnych źródeł. Dlatego ani *fake news*, ani z gruntu fałszywe bądź tylko zmanipulowane treści, względnie enuncjacje propagandowe, umieszczane w przestrzeni medialnej przez agentów wpływu i „pudła rezonansowe" nie mogą mieć realnego wpływu na procesy decyzyjne dojrzałych państw. Mogą jednak prowadzić do problemów społecznych, niepewności decyzyjnej bądź szumu informacyjnego, ale w ostateczności muszą skłonić ośrodki władzy do weryfikacji i korekty pierwotnie błędnych ocen. Co więcej, podanie przez media wiarygodnej informacji o takich praktykach podmiotu odpowiedzialnego za rozpowszechnianie nieprawdy osłabia jego wiarygodność także w sprawach, w których jest on źródłem informacji prawdziwych[11].

W związku z tym, jeśli operacje dezinformacyjne mają być skuteczne, muszą w możliwie kompletny sposób odciąć ofiarę od alternatywnych źródeł informacji. Jeżeli się to uda, obiekt ataku dezinformacyjnego – zgodnie z podstawowymi zasadami sylogizmu – mając fałszywe przesłanki, **musi** dochodzić do fałszywych wniosków, nawet jeśli zastosuje najbardziej rygorystyczne procedury logiczne.

Najlepszą ilustracją tak pojmowanej dezinformacji były działania brytyjskiego The XX Committee (kontrwywiadu), który podczas operacji znanej jako *Double Cross System*, w celu oszukania niemieckiej Abwehry, zdołał przechwycić praktycznie wszystkich niemieckich szpiegów, postawić ich przed alternatywą: współpraca z MI5 lub powieszenie (co, nawiasem mówiąc, dało praktycznie stuprocentową skuteczność werbunku) oraz kontrolować przy tym rezultat swoich działań dezinformacyjnych dzięki skutecznemu dekryptażowi Enigmy[12]. Brytyjski kontrwywiad miał jednak zadanie ułatwione dzięki wyspiarskiemu położeniu Zjednoczonego Królestwa – agenci Abwehry byli sprawnie wyłapywani niemal natychmiast po wylądowaniu na terytorium Anglii[13].

---

[10] Wszystkie wyróżnienia w tekście pochodzą od autora – przyp. red.

[11] W taką pułapkę wpadła Federacja Rosyjska – która po wielu kampaniach medialnych rozpoznanych jako szerzenie zmanipulowanych lub kłamliwych informacji w żaden sposób nie potrafiła przeciwstawić się narracji zachodniej także w sprawach, w których oskarżenia wysuwane wobec Rosjan nie miały znaczących podstaw dowodowych. Wcześniejsze, udowodnione, kłamstwa rosyjskich mediów zdyskredytowały ich wiarygodność, co w ostatecznym rozrachunku doprowadziło do poważnych strat w prowadzonej przez ten kraj wojnie informacyjnej.

[12] Cała operacja została opisana przez jej współtwórcę w: J. Masterman, *Brytyjski system podwójnych agentów 1939–1945*, Warszawa 1973.

[13] Do podobnej sytuacji doszło w przypadku prowadzenia przez służby kubańskie pod

Służby kontynentalne, zwłaszcza dużych państw, niezdolnych do skutecznego kontrolowania nie tylko granic, lecz także całości własnego terytorium, zwykle nie są w stanie realizować tego typu działań, gdyż nie potrafią zapobiec uzyskiwaniu przez przeciwnika informacji od niekontrolowanych przez siebie źródeł. Ten problem został rozwiązany przez służby sowieckie (obecnie rosyjskie) już na początku lat 20. XX w., kiedy to Sowieci przyjęli zasadę prowadzenia kontrwywiadu ofensywnego, polegającego na **aktywnym** podstawianiu obcym szpiegom własnej agentury w charakterze obiektów werbunkowych i za jej pośrednictwem – dezinformowaniu przeciwników (tzw. *opieratiwnaja nastupatielnost'*). Sama aktywizacja kontrwywiadu jednak nie wystarczała (gdyż wywiad wprowadzany w błąd, poszukując alternatywnej weryfikacji, mógł nawiązać kontakt z innymi źródłami), w związku z czym Rosjanie (a właściwie, tzw. internacjonałowie, gdyż WCzK/GPU były tworzone głównie przez Polaków, Żydów i Bałtów) wpadli na genialny pomysł: proponowali ofiarom **pozorną weryfikację informacji.** Jądrem tej idei było założenie, że jeśli przedstawi się ofierze różne możliwości pozornego wyboru, to nawet gdyby nie zaufała jednemu źródłu, będzie prawdopodobne, że zaufa drugiemu, trzeciemu itd. Jest to zasada niezwykle podobna do zasady stosowanej przez telewizje komercyjne, które pozornie oferują wiele kanałów dopasowanych do konkretnych grup odbiorców, ale w rzeczywistości służą jedynie jako źródło prezentacji reklam, a więc zarabianiu na reklamodawcach.

Sowiecka wersja prowadzenia dezinformacji może być obrazowo nazwana „systemem matrioszek", gdyż każda próba zweryfikowania informacji przez ofiarę i dotarcia do wiarygodnych źródeł zawsze doprowadzała do pojawienia się na scenie kolejnej „matrioszki", tj. źródła zupełnie innego niż poprzednie, ale przekazującego te same treści, dopasowanego do potrzeb odbiorcy.

Znakomitą ilustracją takiego modelu działań sowieckich służb była aktywność kontrwywiadu OGPU wobec emigracji rosyjskiej po zdekonspirowaniu w kwietniu 1927 r. rzekomej monarchistycznej organizacji MOCR-Trust (w rzeczywistości była to instytucja przykrycia OGPU, która od 1921 r. skutecznie wprowadzała w błąd kierownictwo „białoemigrantów" i zachodnie wywiady).

Poniżej zostanie przedstawiona sekwencja działań OGPU, która posłuży jako ilustracja powyżej nakreślonego „systemu matrioszek".

Case study „systemu matrioszek"

W dniu 12 kwietnia 1927 r. agent OGPU będący jednocześnie członkiem zarządu organizacji MOCR-Trust, Eduard Opperput, wraz z wysłanniczką gen. Aleksandra Kutiepowa Marią Zacharczenko-Szulc przekroczyli granicę z ZSRR do Finlandii. Niemal natychmiast po przejęciu uciekinierów przez fińską straż graniczną i przekazaniu

kierownictwem KGB gry dezinformacyjnej przeciwko CIA, w czasie której Amerykanie byli oszukiwani przez podwójną agenturę przez niemal 25 lat.

ich fińskiemu odpowiednikowi Oddziału II (wywiadowi – również noszącemu nazwę „Oddział II") E. Opperput złożył obszerne zeznania, z których wynikało, że podziemna organizacja MOCR-Trust, z którą współpracowały organizacje białogwardyjskie i większość zachodnich wywiadów, była legendą OGPU służącą do dezinformowania rządów i sztabów generalnych Zachodu. Teoretycznie rzecz biorąc, było to zakończenie operacji dezinformacyjnej realizowanej przez Sowietów od 1921 r., gdyż enuncjacje E. Opperputa zdyskredytowały Trust. Jednak pomijając to, że sama struktura tej organizacji za granicą pozostała niezmieniona, Sowieci sięgnęli po naszkicowany powyżej „system matrioszek" i podsuwali w miejsce Trustu nowe, łżealternatywne źródła informacji.

Już 16 kwietnia 1927 r. gen. Aleksandr Kutiepow, kierujący Russkim Obszczewoinskim Sojuzom[14], otrzymał list od agenta OGPU, rzekomego członka Zarządu Trustu, gen. Nikołaja Potapowa[15]. W liście gen. Potapow oskarżał E. Opperputa o to, że jest agentem OGPU (a wcześniej WCzK)[16] oraz o (…) *finansowe machinacje* (…) stojące za jego ucieczką. Podawał przy tym wiele informacji, które miały wywołać u odbiorcy zjawisko nazywane przez GPU *putanicą*, czyli powiększających chaos informacyjny u przeciwnika[17]. Jednak głównym przesłaniem gen. Potapowa była sugestia, że część organizacji MOCR-Trust przetrwała „wsypę" i jest gotowa działać dalej, a ucieczka E. Opperputa była li tylko skutkiem jego finansowych machinacji. Była to pierwsza konsekwentnie realizowana *nowaja linija* OGPU, które w miejsce Trustu podsuwało kolejne oferty dla złaknionej nadziei emigracji.

W dniu 20 kwietnia 1927 r. sowiecka agencja informacyjna TASS przekazała wiadomości opublikowaną dzień później w „Izwiestijach" i „Prawdie" o rozbiciu grupy monarchistycznej zajmującej się (…) *szpiegostwem wojskowym i finansowymi machinacjami*[18]. Przy czym, co ciekawe, zarówno paryskie „Wozrożdienije", jak i berlińska „Rul'" stały na stanowisku, że jest to informacja nieprawdziwa[19].

Wielość doniesień prasowych na temat ucieczki E. Opperputa (zainicjowanych publikacją z 24 kwietnia 1927 r. w helsingforskiej „Hufvudsadsbladet"[20]) nie zmieniła

[14] Rosyjski Związek Ogólnowojskowy (ROWS) – organizacja utworzona w 1924 r. na emigracji przez gen. Piotra Wrangla w celu udzielania pomocy w emigrowaniu z ZSRR i zachowania elementów organizacji białej armii, która ewakuowała się z Krymu w 1920 r., chroniąc się przed Armią Czerwoną. Szerzej zob. Рыбас С.Ю, *Генерал Кутепов,* Москва 2010.

[15] Tekst pisma w: Л. Флейшман,, *В тисках провокции. Операция Трест и русская, зарубежная печать*, Москва 2000, s. 140–142.

[16] Rzecz jasna, posłużyło to w późniejszym okresie E. Opperputowi do dezawuowania oskarżeń ze strony byłych sawinkowców jako sowieckiej dezinformacji – por. „Siegodnia" z 17 maja 1927 r.

[17] Jak zwykle w działaniach OGPU uzyskiwano to dzięki wpleceniu sugestii w prawdziwe informacje. N. Potapow m.in. (zgodnie z prawdą) oskarżył E. Opperputa o bycie agentem już CzeKi; opisał pijacką eskapadę G. Radkiewicza z 5 IV 1927 r., histeryczne reakcje jego żony, próbę szantażu ze strony E. Opperputa żądającego pieniędzy za milczenie itp.

[18] Ta informacja została błyskawicznie przedrukowana przez prasę emigracyjną m.in. w „Последних Новостях" i w „Возрождению".

[19] Л. Флейшман, *В тисках провокции*..., s. 144.

[20] Nawiasem mówiąc, nazwiska w tekście były pisane błędnie, co sugerowało, że redakcja mogła

nastawienia emigracji do kierowników jaczejek Trustu (w rzeczywistości – organizacji przykrycia dla agentury OGPU) działających w Europie Środkowej i Zachodniej. Przynajmniej tak można sądzić po poleceniu gen. A. Kutiepowa, aby kierownik warszawskiego ZJARMA, Jurij Artamonow, podtrzymał kontakt z Oddziałem II niejako w oderwaniu od centrali Trustu w Moskwie[21]. Było to zaskakujące, zważywszy że gen. A. Kutiepow w rozmowie z kierownikiem Referatu „Wschód" Oddziału II mjr. Michałem Talikowskim dał do zrozumienia, że ROWS stracił zaufanie do Oddziału, ponieważ sztab i rząd RP są infiltrowane przez OGPU, i że w związku z tym przenosi centrum działalności do Finlandii[22].

Dnia 18 maja 1927 r. Pawieł Arapow (agent OGPU) napisał do swojego wuja gen. Piotra Wrangla list[23], w którym dyskredytował Trust. Pisał, że E. Opperput, wbrew temu, co się mówi, (…) *nie był jedynym prowokatorem* (…), że operacja służyła uderzeniu w gen. Kutiepowa i że dekonspiracja Trustu może jedynie wzmocnić inną strukturę związaną z Trustem – Eurazję[24]. Należy domniemywać, że gdy OGPU zorientowało się, iż emigracja przestała wierzyć w wiarygodność Trustu, podsunęło jej w ten sposób kolejny *dwojnik* w postaci Eurazji. Ponieważ gen. P. Wrangel od początku odnosił się do Trustu nieufnie, a po enuncjacjach E. Opperputa publicznie mówił o prowokacji GPU i kompromitacji gen. A. Kutiepowa, to OGPU podsunęło mu krewnego, który potwierdzał jego pierwotne przekonanie o Truście jako o sowieckiej organizacji prowokacyjnej. P. Arapow, przedstawiciel Eurazji, był idealnie przygotowaną przynętą: na temat spisku Trustu przekazywał te same informacje, co generał, i reprezentował Eurazję, czyli nurt rzekomo nieskażony sowiecką infiltracją (w przeciwieństwie do organizacji MOCR-Trust, która – jak pamiętajmy – zgodnie z tezami N. Potapowa miała ciągle działać, choć osłabiona przez aresztowania).

W dniu 10 lipca 1927 r. Arapow przesłał kolejny list do gen. P. Wrangla, w którym otwarcie pisał, że bez względu na niepowodzenie Trustu konieczne jest podtrzymanie kontaktu z sowiecką Rosją[25]. W domyśle, rzecz jasna, przez struktury Eurazji.

---

otrzymać informację ustnie lub w formie czyjejś odręcznej notatki.

[21] С. Войцеховский, *Трест. Воспоминания*, Kanada 1974, s. 111.

[22] Л. Флейшман, *В тисках провокации*…, s. 149.

[23] Hoover Institution Archives (HIA), Vrangel Coll., Box 151, file nr 44, s. 366–367.

[24] Eurazja – kierunek filozoficzno-polityczny w Rosji akcentujący sukcesję i współdziałanie kultury rosyjskojęzycznej z nomadycznymi imperiami stepów euroazjatyckich (przede wszystkim z mongolskim imperium Chingizidów). Zrodził się w środowisku emigracyjnym w latach 20. XX w. Organizacja, po jej agenturalnym opanowaniu, stała się dla GPU kolejnym kanałem dezinformacyjnym (szerzej: Т.К Гладков, *Артур Артузов*, Москва 2008). Tuż przed samodekonspiracją Trustu GPU „wyodrębniło" bowiem z jego struktur organizację o nazwie Eurazja, by za jej pomocą dalej podtrzymywać kontakt z emigracją (zob. G. Bailey, *The Conspirators*, London 1961, s. 82). Nawet po dekonspiracji MOCR-Trust Oddział II nie miał świadomości, że Eurazja może być kolejną legendą GPU. Dowodzi tego m.in. pismo podpułkownika Sztabu Generalnego Wojska Polskiego T. Schaetlza do attaché wojskowych w Paryżu, Pradze, Belgradzie i Moskwie z prośbą o dyskretne wyjaśnienie, które z mocarstw subsydiuje ten ruch – patrz: AAN, sygn. A.II.23, MSWojsk, SG, Oddział II, Nr 15567/II.inf./Ros. z 7 XII 1927 r.

[25] „(...) Что бы то ни было, я по прежнему считаю, что опасно терять связь с противником";

Dnia 13 lipca 1927 r. w paryskim „Wozrożdieniju" opublikowano nekrolog Marii Zacharczenko-Szulc będący początkiem jej późniejszej gloryfikacji jako „męczenniczki białej sprawy". Publikacja była próbą zatrzymania pogłosek uporczywie krążących wśród emigracji, że **cała** „trojka" E. Opperputa, która rzekomo miała przeprowadzić w Moskwie zamach w rewanżu za wprowadzenie w błąd emigracji za pomocą Trustu, składała się z agentów OGPU[26], a sama Maria – razem ze swoim kochankiem E. Opperputem – przeżyła.

Z końcem lipca 1927 r. w emigracyjnej prasie zaczęły się pojawiać informacje o aktywnej działalności organizacji Bractwo Russkoj Prawdy – grupy poprzednio marginalnej i współpracującej z Trustem[27], wydającej niskonakładowe pisemko antysowieckie[28] pt. „Russkaja Prawda". Zdaniem liderów BRP w Rosji miało wybuchnąć antysowieckie powstanie, zwłaszcza na południowym zachodzie i dalekim wschodzie ZSRR[29]. Gen. P. Wrangel początkowo trzeźwo uznał tę organizację za kolejną legendę OGPU[30], ale po spotkaniu z liderem BRP S.A. Sokołowem (w listopadzie 1927 r.), pod wpływem okazanych mu przez Sokołowa dokumentów, nieoczekiwanie zmienił swoje nastawienie. Następnie opublikował memorandum, w którym stwierdził, że BRP nie jest legendą, a kierujący Bractwem „Brat nr 1" dobrze służy ojczyźnie[31]. Co więcej, utrzymywał, że członkowie BRP byli uczestnikami terrorystycznych *trojek* (w tym tej kierowanej przez E. Opperputa i M. Zacharczenko-Szulc) wysyłanych do ZSRR. Ta interpretacja została następnie podchwycona przez emigracyjną prasę, która najpierw utrzymywała, że członkiem BRP była M. Zacharczenko-Szulc[32], ale potem – pod

Hoover Institution Archives (HIA), Vrangel Coll., Box 151, file nr 44, k. 368.

[26] Por. Л. Флейшман, *В тисках провокации*…, s. 222.

[27] Nawiasem mówiąc, BRP działało w RP i z naszego terytorium pomagało w kolejnych operacjach Trustu – por.: „Когда в июле 1924 года возник «Русский Обще-Войсковой Союз» (РОВС), почти все члены пинской монархической организации и БРП вошли и в РОВС. Пинская полиция не могла тогда разграничить БРП и РОВС: «Деятельность «Братства Русской Правды» и «Русского Обще-Войскового Союза» так взаимно переплетена, что трудно отличить, где кончается деятельность одной организации и начинается – другой, и наоборот. Обе эти организации работают солидарно на территории советов, а разделение труда является таким, что БРП, главным образом, занимается сбором денег на нужды двух организаций, однако руководство принадлежит РОВС». Пинские монархисты (Семен Бродович, Дмитрий Копацинский, Станислав Мацкевич, Николай Котович и др.) были вовлечены в знаменитую чекистскую операцию «Трест»: поддерживали контакты с её активными участниками – евразийцами Юрием Мукаловым и П. Демидовым (Орсини)". Zob. *Петербургский и пинский архитектор Николай Котович*, http://brama.brestregion.com/nomer24/artic16.shtml# [dostęp: 20 XI 2015].

[28] А. Добкин, С.А. Соколов-Кречетов, *От «Золотого Руна» к «Русской Правде». In memoriam: Исторический сборник памяти А.И. Добкина*, S.-Petersburg–Paryż 2000, s. 91–99.

[29] Por. Атаман Кречет, *Там, где ещё бьются. Из записной книжки повстанческого атамана*, „Возрождение" z 31 lipca 1927 r.

[30] „Всё это, думается, такая же ловушка для доверчивых дураков, как в свое время пресловутая «монархическая организация: Фёдоров"; HIA, Vrangel Coll., Box 147, file nr 34, k. 390.

[31] Л. Флейшман, *В тисках провокции*..., s 279–281.

[32] Амфитеатров А., *Листки*, „Возрождение" z 8 listopada 1927 r.

wpływem listu wysłanego do redakcji czasopisma „Россия" przez jej męża Grigorija Radkiewicza przeczącego temu[33] – zaczęła twierdzić, że członkiem Bractwa był inny uczestnik zamachu, Jurij Wozniesienskij, który miał zginąć wraz z Marią w obławie zorganizowanej przez OGPU[34].

W dniu 30 lipca 1927 r. gen. P. Wrangel otrzymał list od kolejnego sowieckiego nieświadomego agenta (rezonatora), Aleksandra Guczkowa, w którym Guczkow wzywał do zaprzestania wszelkich działań aktywnych w Rosji (tj. prowadzenia działalności terrorystycznej, której obawiało się OGPU[35]). Należy się domyślać, że A. Guczkow działał pod wpływem swojej córki Wiery, zwerbowanej do współpracy z GPU przez jej kochanka Konstantina Radzewicza[36], który w 1926 r. przyjechał z Rygi do Paryża (Radzewicz mieszkał w tym samym domu, co inny sowiecki agent, znany pisarz Siergiej Efron).

Dnia 7 sierpnia 1927 r. gen. P. Wrangel poinformował w liście gen. Pawła Szatiłowa[37], że gen. Aleksandr Łukomskij (który nie odzywał się do niego przez ponad rok, po czym nagle zaczął pisać po kilka listów tygodniowo) sugerował m.in., że Trust działa dalej, gdyż tylko część organizacji została zdekonspirowana.

We wrześniu 1927 r. z kolei G. Radkiewicz wysłał list do oficera OGPU Wiktora Steckiewicza[38]. Proponował w nim współpracę z OGPU w zamian za przekazanie listów Marii Zacharczenko-Szulc[39], która miała przebywać w wewnętrznym więzieniu tej organizacji. Był to skutek natrętnych plotek szerzących się wśród emigracji i sugerujących, że Maria, podobnie jak E. Opperput, była sowiecką agentką i że wcale nie zginęła w lasach smoleńskich. Brakuje danych na temat reakcji OGPU, ale zważywszy na to, że G. Radkiewicz był wówczas kierownikiem bojowego oddziału gen. A. Kutiepowa w Finlandii, odpowiedzialnego za realizację kolejnych ataków terrorystycznych na terytorium ZSRR, należy przyjąć za pewnik, że list został przyjęty przez OGPU z dużym zainteresowaniem. Być może ta informacja pozostaje w ścisłym związku z tym, że dwie kolejne *trojki* wysłane do Rosji przez gen. A. Kutiepowa zostały natychmiast zlikwidowane (pierwsza – już podczas przekraczania granicy – wszy-

[33] „Россия" z 19 listopada 1927 r.

[34] List rzekomego członka BRP Wasiljewa do redakcji, opublikowany w „Возрождению" 9 XII 1927 r.

[35] „(...) после провала «Треста» (...) приходится, конечно, приостановить всякую активную работу в России (...)"; HIA, Vrangel Coll., Box 151, file nr 44, k. 265.

[36] O tym, jak duży musiał być odsetek agentury wśród paryskich Rosjan, może świadczyć to, że oboje agenci OGPU w latach 30. XX w. przestali ukrywać swoje polityczne sympatie. Wiera stała się działaczką francuskiej partii komunistycznej, a Radzewicz uczestniczył w wojnie w Hiszpanii jako oficer Brygad Międzynarodowych.

[37] Por. list Łukomskiego z 2 VIII 1927 r.: „(...) одна из линии связий (sic!) была открыта и предана. Но из этого далеко ещё до вывода, что провалились все". Zob. HIA, Vrangel Coll., Box 147, file nr 33, k. 346–349.

[38] Raz jeszcze należy podkreślić, że to oznacza zachowanie wciąż działających kanałów komunikacji z Trustem, choć brakuje informacji, jakimi kanałami ta korespondencja była przekazywana.

[39] Л. Флейшман, *В тисках провокции*..., s. 232–233.

scy członkowie zabici, druga – schwytana i wykorzystana do pokazowego procesu, w czasie którego jej członkowie pokajali się i złożyli zeznania wykorzystane później w nagonce prasowej na fiński rząd, a także w nocie skierowanej przez rząd ZSRR do rządu Finlandii)[40]. Wskutek tego *démarche* Finlandia wydaliła organizację bojową gen. A. Kutiepowa, w tym G. Radkiewicza, który przeniósł się do Polski[41].

W dniu 11 września 1927 r. berlińska „Rul'" zamieściła *Pis'mo iz Giel'singforsa*, w którym informowano, że zabity członek *trojki* E. Opperputa, J. Wozniesienskij, w rzeczywistości nazywał się Peters i pochodził z rodziny znanych komunistów.

Dnia 22 października 1927 r. w kolejnym emigracyjnym piśmie „Bor'ba za Rossiju" pojawił się anonimowy list pt. *Triest i GPU. Pokazanija nieposriedstwiennogo uczastnika*, w którym dokonano racjonalnej (i zgodnej z prawdą) oceny celów postawionych Trustowi przez OGPU. Nade wszystko jednak napisano, że nie cały Trust był agenturalny, a nawet – że część jego działaczy konspirowała wewnątrz organizacji, wskutek czego likwidacja tej organizacji nie oznaczała przerwania działalności jej niektórych ogniw, nieskażonych infiltracją[42]. Przypuszczalnie autorem tego pisma był G. Radkiewicz, który stał także za wysyłaniem kolejnych *trojek* do ZSRR. Warto zanotować, że analiza celów Trustu zaprezentowana w liście była na tyle logiczna i napisana tak jasnym językiem, że nie odpowiadała poziomowi pisemnych wypowiedzi G. Radkiewicza przechowywanych w materiałach Oddziału II. Należy z tego wnosić, że jeśli to on ukrywał się pod anonimowym pismem, to był jedynie przekaźnikiem myśli kogoś innego. Ten list został następnie przedrukowany przez większość tytułów emigracyjnych[43].

W 1928 r. w ZSRR została opublikowana praca Nikołaja Kiczkasowa pt. *Biełogwardiejskij tierror protiw SSSR*, w której zamieszczono zniekształconą informację o likwidacji *trojki* E. Opperputa. Wiadomość zilustrowano fotografią mającą przedstawiać M. Zacharczenko-Szulc jako śliczną dziewczynę. Z całą pewnością jednak nie była to wyżej wymieniona Maria. Osoba na zdjęciu nie wykazywała żadnego podobieństwa do niej. Jak się wydaje, miało to utwierdzić emigrację w przekonaniu, że białogwardzistka zabita pod Smoleńskiem nie była Marią Zacharczenko-Szulc[44].

Niedługo potem G. Radkiewicz dokonał ataku bombowego na biuro przepustek OGPU. Jego cel do dnia dzisiejszego pozostaje niejasny (nie wiadomo, czy Radkiewicz chciał pomścić żonę, czy też była to kolejna prowokacja OGPU).

Powyższy, pobieżny przegląd działań wobec rosyjskiej emigracji jest oczywiście jedynie zarysem działań OGPU, które szybko przejdzie od dezinformacji i manipulacji do porwań i fizycznej likwidacji liderów emigracyjnych. Jak wynika z przed-

[40] Por. W. Ulrich, *Необходимо разрушить гнездо террористов в Финляндии*, „Izwiestija" z 4 października 1927 r.

[41] Л. Флейшман, *В тисках провокации*..., s. 272.

[42] Dowodem na skuteczność tej dezinformacji może być choćby najbardziej ośmieszona ofiara Trustu – Wasilij Szulgin, który do końca życia wierzył, że działacze organizacji MOCR-Trust, z którymi się spotkał, byli prawdziwymi spiskowcami, być może związanymi z Lwem Trockim.

[43] Л. Флейшман, *В тисках провокации*..., s. 273.

[44] Tamże, s. 303.

stawionego opisu zdarzeń, OGPU, kończąc jedną legendę, **jednocześnie** podsuwało ofiarom kolejną, nową, i mamiło emigrantów nadzieją, że tym razem będą mieli do czynienia z prawdziwymi patriotami zwalczającymi komunizm. Łatwo też zauważyć, że w tej grze planiści z Łubianki byli na tyle bezczelni, że nie tworzyli nawet nowych organizacji i nie kreowali nowych postaci, tylko w dużym stopniu sięgali do już istniejących zasobów (wynikało to zapewne z czystej pragmatyki i lenistwa oficerów nadzorujących operację). Likwidując organizację MOCR-Trust, podsunęli emigracji Eurazję i Bractwo Russkoj Prawdy (obie organizacje współpracowały z Trustem, były znane OGPU i – w najlepszym wypadku – były zinfiltrowane przez sowiecką agenturę, o ile nie były po prostu kolejnym *dwojnikiem* Trustu[45]). A rosyjscy emigranci, rozczarowani i ośmieszeni, dawali się łapać w kolejne sowieckie łowuszki grające na najbardziej ludzkich uczuciach: nadziei, tęsknocie za ojczyzną i obawie o rodzinę.

Ponieważ każda służba działa na podstawie obowiązujących instrukcji operacyjnych, można założyć, że zarysowany powyżej mechanizm kontynuowania prowokacji mógł mieć miejsce i w odniesieniu do innych organizacji współpracujących z Trustem, w tym do Oddziału II. Dwaj główni działacze warszawskiej jaczejki Trustu, Jurij Artamonow i Siergiej Wojciechowski, pozostali w bliskim kontakcie z oficerami Referatu „Wschód" także po dekonspiracji Trustu w 1927 r. Zażądano od nich jedynie pisemnych wyjaśnień na temat kontaktów z tą organizacją, które przyjęto bez dalszych dyskusji. Choć np. S. Wojciechowski, zapewne obawiając się, że jego korespondencja była czytana przez Oddział II, otwarcie pisał o swoich *obzorach* (szpiegowskich analizach dotyczących sytuacji politycznej), które były wysyłane do Moskwy.

Bractwo Russkoj Prawdy działało w RP zapewne podobnie jak wiele innych prowokacyjnych lub infiltrowanych struktur rosyjskiej emigracji. Oddział II SG WP nie przeprowadził jednak poważnego śledztwa, aby zweryfikować podejrzenia wobec własnych oficerów, choć – jak wynika z przedstawionych powyżej analiz – metodą GPU było oskarżanie autentycznych agentów, aby ich uwiarygodnić. Można więc uznać, że choć Trust jako organizacja się skończył, wywołując międzynarodowy skandal i kompromitując współpracujące z nim zachodnie oraz emigracyjne ośrodki wywiadowcze, to samą operację, której był częścią, kontynuowano. Sowieci pozwolili swoim ofiarom na otwarcie tylko pierwszej warstwy matrioszki, pod którą, niestety, znajdowały się kolejne.

[45] Problem rzeczywistego charakteru organizacji – mimo wysiłków rosyjskich historyków o przekonaniach prawicowych, którzy usiłują wykazać jej antysowiecki charakter – do dnia dzisiejszego pozostaje niewyjaśniony. Natomiast jest pewne, że informacje przekazywane przez Bractwo na Zachód (np. o rzekomym powszechnym powstaniu antysowieckim) były nieprawdziwe oraz że stosowana przez nie taktyka kontaktów z emigracją była dokładnym powtórzeniem metod wykorzystywanych przez Trust.

Zakończenie

Wyżej zarysowany przebieg zdarzeń w ocenie autora artykułu znakomicie ilustruje metodę sowieckich manipulatorów scharakteryzowaną na wstępie, którzy gdy tylko jedno źródło dezinformacji traciło w oczach ofiar na wiarygodności, natychmiast podsuwali im kolejne, przy czym często o odmiennej proweniencji politycznej. Ta metoda dzięki swej prostocie była skuteczna. Pozorna wielość źródeł informacji dawała złudzenie możliwości weryfikacyjnych i fałszywy komfort podejmowania decyzji na podstawie rzekomo wielośródłowych danych. Analitycy państw – ofiar splatali te dane w konstrukcje analityczne, których wyniki **musiały być** zbieżne z interesami manipulatora podsuwającego strzępy informacji przez wiele łże-źródeł.

Federacja Rosyjska, która powstała na gruzach ZSRR, przejęła najważniejsze elementy systemu sowieckiej państwowości, w tym całość instrumentarium służb specjalnych z wypracowanymi i doskonalonymi przez lata metodami dezinformacji. Nie jest więc zaskoczeniem, że „system matrioszek", czyli mnożenie fikcyjnych źródeł informacji lub pozornie różnych aktorów procesów społecznych, którzy jednak – przynajmniej na poziomie strategicznym – preferują te same rozwiązania, korzystne dla określonego podmiotu politycznego, jest stosowany po dziś dzień. Problem metodologiczny polega jedynie na tym, że w przeciwieństwie do źródeł historycznych współczesne przykłady wykorzystywania tego systemu nie są w pełni udokumentowane i w związku z tym są trudne do zaakceptowania w dyskursie naukowym. Dobrym przykładem tej tezy jest nigdy niepowtórzona informacja stacji telewizyjnej RTR Płanieta z pierwszych dni wojny rosyjsko-gruzińskiej, z której wynikało, że kontrwywiad Federacji Rosyjskiej aresztował kilkudziesięciu szeregowych żołnierzy i oficerów armii rosyjskiej pochodzenia gruzińskiego, którzy pracując dla gruzińskiego wywiadu wojskowego, wpadli rzekomo dzięki głupocie ich oficerów prowadzących. Ci ostatni mieli dzwonić do swojej agentury pod numery telefonów komórkowych, aby szybko zdobyć informacje na temat ruchów rosyjskich kolumn pancernych. W późniejszym okresie ta informacja nigdy nie została powtórzona, nie pojawiły się też dane o masowych procesach rzekomych zdrajców, co może sugerować, że gruziński wywiad mógł paść ofiarą prowokacji z wykorzystaniem licznych i wzajemnie wzmacniających swój przekaz podwójnych agentów.

Mówiąc o wykorzystaniu „systemu matrioszek", można postawić hipotezę, że zgodnie z metodyką stosowaną przez Rosjan agentura była zróżnicowana i obejmowała zarówno agentów podsuniętych gruzińskiemu wywiadowi do werbunku, jak i klasycznych oferentów otwarcie proponujących temu wywiadowi swoje usługi, przy czym o różnej proweniencji politycznej i motywacji. Przyjęcie perspektywy dezinformacji wielośródłowej, przy zastosowaniu tricku z pozorną możliwością zweryfikowania danych, tłumaczyłoby zarówno niezrozumiałą z militarnego i propagandowego punktu widzenia decyzję prezydenta Micheila Saakaszwilego o zaatakowaniu Osetii Południowej i Abchazji, które zakończyło się utratą przez Gruzję zbuntowanych terenów (i gdyby nie interwencja dyplomacji Zachodu doprowadziłoby do zdobycia Tbilisi

oraz ulokowania tam władz w pełni uległych wobec Federacji Rosyjskiej), jak i niepojętą zwłokę prezydenta Dmitrija Miedwiediewa z natychmiastowym udzieleniem pomocy rozjemczym wojskom rosyjskim atakowanym przez Gruzinów.

Warto przy tym zauważyć, że przed rozpoczęciem wojny rosyjskie satelitarne kanały telewizyjne przez niemal rok emitowały serię reportaży ukazujących rozkład rosyjskiej armii, rdzewiejące na redach rosyjskie okręty wojenne, pilotów, którzy nie byli w stanie wykonywać lotów ćwiczebnych z powodu braku paliwa, żebrzących żołnierzy itp. Agresywne w swej wymowie programy emitowano aż do wybuchu konfliktu, pomimo tego, że ich ostrze uderzało bezpośrednio w tandem rządzący Rosją – w premiera Władimira Putina i prezydenta Dmitrija Miedwiediewa. Natomiast w trakcie walk i po ich zakończeniu ton relacji nagle się zmienił – przybrały one charakter triumfalistyczny. W kontekście przebiegu całego konfliktu, który w ocenie większości analityków nosił cechy prowokacji, te działania mogły wskazywać na stosowanie przez Rosjan wieloźródłowej, wzajemnie wzmacniającej się dezinformacji, która miała przekonać Gruzinów o niezdolności rosyjskiej armii do zdecydowanej interwencji.

Trzeba także – bez pełnej bazy dokumentarnej – zwrócić uwagę na zastosowanie „systemu matrioszek" przy ochronie geopolitycznych interesów Federacji Rosyjskiej po rozpadzie Związku Sowieckiego. To, że większość posowieckich republik prowadziła (i nadal prowadzi) politykę zgodną z interesami postkolonialnego centrum w Moskwie, bez względu na proweniencję polityczną liderów, może świadczyć o tym, że rosyjska agentura mogła być rozmieszczana równomiernie na całości sceny politycznej danego państwa, aby zabezpieczyć interesy Kremla bez ryzyka zmiany kursu wahadła politycznego.

Podobne zjawisko można zaobserwować także w Europie Środkowo-Wschodniej, w której rosyjski wywiad chętnie sięga zarówno do ugrupowań lewackich, względnie nostalgicznie nastawionych do komunistycznej przeszłości, i jednocześnie fryzuje się na obrońcę wartości tradycyjno-chrześcijańskich, prawicowo-nacjonalistycznych, czasem wręcz o zabarwieniu faszystowskim. Z punktu widzenia logiki ideologicznej zasilanie pieniędzmi ugrupowań skrajnych po obu stronach sceny politycznej wydaje się absurdalne. Jednak przy zaakceptowaniu założeń „systemu matrioszek" płynącego z postimperialnej *Realpolitik* staje się skutecznym sposobem realizacji interesów FR, odpornym na wahania politycznej koniunktury.

„System matrioszek", mimo swej prostoty, jest skuteczny. Życie współczesnego człowieka jest oparte na wierze w znacznie większym stopniu niż życie naszych przodków, którzy przynajmniej swoje otoczenie znali zwykle z pierwszej ręki. Współczesność poznaje rzeczywistość przez pośredników: za pośrednictwem mediów, autorytetów, rzekomych bądź autentycznych prawd naukowych, tzw. autorytetu rozproszonego, słowem – niemal zawsze z drugiej ręki. Taka konstrukcja rzeczywistości zakłada wiarę w tych, którzy są dostarczycielami informacji. Umysł ludzki, by móc funkcjonować, potrzebuje oparcia. Ludzka myśl bez wiary w prawdę jest bezradna, gdyż już sama natura rozumowania wymaga przyjęcia prawdziwości przesłanek. Twórcy „metody matrioszek" to rozumieli, dlatego dawali (i dają) ofiarom pozorną

wielość możliwości wyboru, aby ujawniając jedno oszustwo, nie mogły się one nawet domyślać, że często pomagają im w tym kolejni oszuści, zyskujący na zaufaniu dzięki zdemaskowaniu poprzedniego kłamstwa tylko po to, żeby stworzyć nowe.

Bibliografia:

Bailey G., *The Conspirators*, London 1961, Viktor Gollancz.

Dezinformacja – oręż wojny, V. Volkoff (oprac.), Warszawa 1991, Helikon.

Encyklopedia szpiegostwa, K. Wojciechowski (tłum.), Warszawa 1995, SPAR.

Epstein E.J., *Podstęp. Niewidzialna wojna między KGB a CIA*, Krosno 1993, Scripta Manent.

Golicyn A., *Nowe kłamstwa w miejsce starych*, Warszawa 2007, Służba Kontrwywiadu Wojskowego.

Hughes-Wilson J., *Największe błędy wywiadów świata*, Warszawa 2002, Bellona.

Larecki J., *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warszawa 2007, KiW.

Lewandowski H., *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, Warszawa 2000, UOP.

Marchetti V., Marks J.D., *The CIA and the Cult of Intelligence*, New York 1974, Alfred A. Knopf.

Masterman J., *Brytyjski system podwójnych agentów 1939–1945*, Warszawa 1973, Ministerstwo Obrony Narodowej.

Polmar N., Allen T.B., *Księga szpiegów. Encyklopedia*, Warszawa 2000, Magnum.

Literatura rosyjska:

Амфитеатров А., *Листки*, „Возрождение” z 8 listopada 1927 r.

Атаман Кречет, *Там, где ещё бьются. Из записной книжки повстанческого атамана*, „Возрождение” z 31 lipca 1927 r.

Войцеховский С., *Трест. Воспоминания*, Канада 1974, Заря.

Гладков Т.К., *Артур Артузов*, Moskwa 2008, Молодая гвардия.

Добкин А., Соколов-Кречетов С.А.: *От «Золотого Руна» к «Русской Правде». In memoriam: Исторический сборник памяти А.И. Добкина*, Sankt-Petersburg–Paryż 2000, Феникс.

Петербургский и пинский архитектор Николай Котович, http://brama.brestregion.com/nomer24/artic16.shtml# [dostęp: 20 XI 2015].

Рыбас С.Ю., *Генерал Кутепов*, Moskwa 2010, Олма-пресс.

Ульрих В., *Необходимо разрушить гнездо террористов в Финляндии*, „Izwiestija" z 4 października 1927 r.

Флейшман Л., *В тисках провокции*. *Операция „Трест" и русская, зарубежная печать*, Moskwa 2000, Новое литературное обозрение.

Abstrakt

Autor analizuje w artykule jedną z metod manipulowania ofiarami operacji dezinformacyjnych realizowanych przez sowieckie (rosyjskie) służby specjalne. Polega ona na włączaniu w trakcie operacji agentury, która pozornie daje możliwość weryfikowania informacji uzyskiwanych przez ofiary od wcześniej podsuniętych agentów dezinformacyjnych i która może – w celu zdobycia zaufania ofiar – uczestniczyć w demaskowaniu i podważaniu wiarygodności agentury wykorzystanej wcześniej. Tę metodę autor określa obrazowo jako „system matrioszek".

W artykule opisano zastosowanie wyżej wspomnianego systemu na przykładzie działań sowieckiego kontrwywiadu wobec białej emigracji w 1927 r. i postawiono hipotezy oparte na założeniach opisanej metody, odniesione także do wydarzeń współczesnych (wojny w Gruzji oraz infiltracji przez służby rosyjskie ugrupowań uplasowanych na przeciwstawnych krańcach spektrum politycznego).

Słowa kluczowe: dezinformacja, manipulacja, ekstremizmy polityczne, wywiad rosyjski, emigracja rosyjska, polityka Federacji Rosyjskiej.

II
RECENZJE

Marek Świerczek

T.K. Gładkow, *Artur Artuzow*[1]

Pojęcie geniuszu zwykle kojarzy się z nauką i sztuką. To na tych polach – zgodnie ze stereotypem – intelekt ludzki może osiągać szczyty swoich możliwości. Czasem jednak to pojęcie przenosi się na obszary niezwiązane z twórczością, jak wojna, a nawet przestępczość, stąd zbitki pojęciowe, takie jak: „geniusz wojskowy" czy „geniusz zbrodni", pomimo swojego języka gazetowego, są przyjęte i nie obrażają purystów.

Książka T.K. Gładkowa wpisuje się w powyższe rozważania semantyczne, traktuje bowiem o człowieku obdarzonym autentycznym geniuszem, oddanym służbie zbrodniczego systemu, system zaś – wykorzystawszy jego dorobek i jego samego – ostatecznie go zabił. Mowa o Arturze Artuzowie, który na początku lat 20. XX w. stworzył podwaliny tego, co do dzisiaj stanowi wyzwanie dla wolnego świata – maszynerię strategicznej dezinformacji realizowanej przez rosyjskie służby specjalne.

Artuzow nie był nawet Rosjaninem, a obywatelem Szwajcarii, noszącym po ojcu, rzetelnym serowarze, nazwisko Frautschi, a po dziadku imię Christian. W Rosji znalazł się dzięki ojcu, który chciał, jak wielu mieszkańców ówczesnej Europy Zachodniej, zarobić fortunę w rozwijającym się szybko imperium Romanowów. Młody Christian studiował na politechnice, ale jego zainteresowania wybiegały daleko poza tajniki mechaniki i chemii. Zajmował się literaturą (pisał wiersze, co w przyszłości zbliżyło go do szefa OGPU Wiaczesława Mielżyńskiego, który nawet publikował swoje utwory), muzyką, językami obcymi, a nade wszystko teatrem. Znajomość tej ostatniej dziedziny sztuki zaowocowała w późniejszym okresie jego życia włączeniem zasad inscenizacji teatralnych do działalności sowieckiego kontrwywiadu.

Młody Frautschi, jak cała ówczesna inteligencja rosyjska, był zafascynowany ideami, które wstrząsały podstawami imperium. Po 1905 r. rosyjska inteligencja, jak pisał Stanisław Cat-Mackiewicz, zaczęła nienawidzić własne państwo. Z Zachodu napływały nowe myśli. Rozwijał się spirytyzm, a miejsce dawnego przywiązania do cerkwi prawosławnej zajmowały ruchy mistyczne i masoneria, która – w naturalnym sojuszu z burżuazją i generalicją – zmierzała do przebudowy państwa rządzonego przez Mikołaja II. Ten władca w typowy dla Rosji sposób łączył depresyjną nieudolność ze świętym przekonaniem, że władza nad dziesiątkami milionów ludzi była mu dana od Boga, a zatem nie może jej z nikim dzielić.

Wspomniany „koktajl" idei oszałamiał rosyjską inteligencję łączącą słowiański idealizm z niemal azjatycką mentalnością władyków euroazjatyckiego imperium. Rezultatem tego był bujny rozwój ruchów rewolucyjnych. W sposób niepojęty dla europejskiej logiki te ruchy, głosząc konieczność likwidacji klas pasożytniczych, były jednocześnie wspierane przez (przynajmniej część) tychże klas, hojnie łożących na

[1] T.K. Gładkow, *Artur Artuzow,* Moskwa 2008, Mołodaja Gwardia, 477 s.

działalność terrorystyczną, mającą doprowadzić do upadku znienawidzonej monarchii, a więc i systemu, z którego korzystali. Zaślepiony i bezmyślny car odpowiadał represjami i rozbudową aparatu policyjnego, co z kolei powodowało wzajemne przenikanie się organizacji odpowiedzialnych za bezpieczeństwo i ruchów rewolucyjnych, infiltrujących się za pomocą podwójnej agentury.

Żadne z aktywnych politycznie środowisk nie dostrzegało reform Piotra Stołypina i niebywałego tempa rozwoju gospodarczego, które w ostatecznym rozrachunku musiały doprowadzić do zmian w strukturze społecznej, a zarazem i w systemie politycznym Rosji. Można założyć, że ten niemal operetkowy układ sił kształtowany przez dwór carski, skorumpowany i rządzony przez Grigorija Rasputina, burżuazję walczącą o pozycję w państwie i zapatrzoną we wzorce zachodnie, inteligencję zawzięcie dyskutującą w kółkach masońskich oraz agresywne organizacje rewolucyjne mógłby trwać, wzajemnie się szachując.

Tyle że na przeszkodzie stanęła głupota cara, który – podjudzony przez ambitnych generałów – wplątał kompletnie nieprzygotowaną Rosję w wojnę z państwami centralnymi. Klęski armii imperialnej nałożyły się na charakterystyczną dla rosyjskiego ludu pogardę dla słabości rządzących oraz aktywną działalność propagandową kanapowej do tej pory opozycji, złożonej z rewolucjonistów zapiekłych w swojej wierze w utopię, prowincjonalnych masonów i przedstawicieli burżuazji marzących o wprowadzeniu na wzór zachodni plutokracji, skrywanej demokratycznymi hasłami. Mimo że armia rosyjska cofała się bez popłochu, gospodarka zdołała w końcu zaopatrzyć wojsko w sprzęt i żywność, a Rosja była jedynym wśród walczących państw krajem nieznającym kartek na żywność – wybuchła rewolucja lutowa. Kierujący dziesięciomilionową armią Mikołaj II w obawie przed buntem w jednym tylko mieście w stu kilkudziesięciomilionowym imperium zrzekł się tronu.

Zaczął się festiwal politycznej wolności, który doprowadził do rozprzężenia całej machiny państwowej i został zakończony puczem wojskowym, szumnie nazwanym rewolucją październikową. Przejęcie władzy przez bolszewików nie było jednak końcem historii: Rosja pogrążyła się w chaosie gospodarczym, wojnie domowej, masowym terrorze i pogłębiającym się upadku wszystkich instytucji państwowych.

Ten krótki rys historyczny jest niezbędny do tego, aby zrozumieć, o czym właściwie pisze T.K. Gładkow. Rosyjski autor w sposób klasyczny dla pisarzy i badaczy powiązanych z Łubianką buduje w swej pracy pomnik Artuzowowi, wzięty żywcem z propagandowych historyjek o Feliksie Dzierżyńskim. Artuzow – w wizji Gładkowa – jest postacią spiżową. Skromny, oddany sprawie rewolucji, rezygnujący z przysługujących mu nomenklaturowych przywilejów, niemający nic wspólnego ze zbrodniami CzeKi *gienij kontrrazwiedki*[2].

To oczywista bzdura. Artuzow, który został wprowadzony do służby w kontrwywiadzie przez rewolucjonistę Michaiła Kierowa, znanego mu z czasów przedwojennych, był mordercą – pozbawionym ludzkich uczuć dokładnie w takim samym stopniu

[2] Geniusz kontrwywiadu.

jak Kiedrow. Rosyjski historyk przemilcza lub przeinacza fakty. Opisując rozbijanie kolejnych organizacji kontrrewolucyjnych przez nasyłanych przez Artuzowa prowokatorów, nie wspomina o losie ich uczestników, bitych i rozstrzeliwanych setkami po wyciągnięciu ich z czekistowskich katowni. Nie pisze o wymuszaniu torturami zeznań, o psychopatycznych metodach przesłuchań, np. zamykaniu więźnia w piwnicy pełnej rozkładających się trupów czy podtapianiu. Ani słowa o „zdejmowaniu rękawiczek", czyli o zdzieraniu skóry z dłoni jeńców po uprzednim sparzeniu jej wrzątkiem. Nie zająknął się o aresztowaniach członków rodziny i grożeniu przesłuchiwanemu ich śmiercią w razie braku kooperacji z jego strony, o miażdżeniu goleni między szynami kolejowymi, ściskaniu głów w przemysłowych imadłach, o wrzucaniu skazanych do pieców hutniczych. Po prostu – radziecki geniusz kontrwywiadu, który w myśl zasady Żelaznego Feliksa, musi mieć chłodną głowę, gorące serce i czyste ręce.

Po usunięciu propagandowego zadęcia i zwykłej dezinformacji książka Gładkowa pozwala zrozumieć fenomen Artuzowa. Trzeba sobie bowiem uświadomić, że Rosja Sowiecka oprócz masowych grobów, państwowego terroru, systemu obozów koncentracyjnych i kłamstwa jako metody uprawiania polityki miała jedno, niezaprzeczalne osiągnięcie – przekształciła zwykłe, ludzkie łgarstwo i dwulicowość w strategiczną metodę funkcjonowania organów państwowych. Krótko mówiąc, dzięki Artuzowowi sowieckie tajne służby odkryły, że niekoniecznie trzeba wykończyć przeciwnika, gdy można go oszukać. Pojęły również dzięki niemu, że masowa prowokacja oraz strategiczna dezinformacja mogą być podstawowym narzędziem ich pracy.

Artuzow, choć jak reszta jego kolegów, posyłał setki ludzi na brutalną śmierć, różnił się od nich inteligencją. Miał przy tym niebywałe szczęście, że jego pracę nadzorowali dwaj inni psychopaci obdarzeni wybitnym intelektem i polskim pochodzeniem[3], tj. Feliks Dzierżyński i Wiaczesław Mienżyński. Zasługą Artuzowa było włączenie w repertuar metod sowieckich służb systematycznej i masowej prowokacji, równie powszechne użycie podwójnej agentury, tworzenie rzekomych organizacji podziemnych lub też przejmowanie kontroli nad już istniejącymi, a także realizacja długotrwałych i starannie przygotowanych gier kontrwywiadowczych z przeciwnikami, stosowanych nie w celu jednorazowego wykorzystania naiwności tych przeciwników, ale w celu systematycznego i możliwie kompletnego oszukiwania ich przez jak najdłuższy czas. Artuzow, a później jego następcy, doskonalili tę metodę. O ile pierwsze tego typu operacje, np. ściągnięcie do Rosji Sowieckiej wrogiego Sowietom Borysa Sawinkowa, były krótkie i trwały od kilku do kilkunastu miesięcy, to już późniejsze operacje rozwijały się kilka lat, np. operacja „Trust" była prowadzona od 1921 r. do 1927 r., ostatnia zaś znana tego typu operacja przeciwko CIA była rozgrywana na Kubie w ciągu… ćwierćwiecza!

To Artuzow stał za przejęciem podstawowych założeń pracy agenturalnej przygotowanych przez najlepszego carskiego kryminologa płk. Arkadija Koszko, w myśl których infiltracji wrogich organizacji i środowisk należało dokonywać za pośrednictwem ludzi z nich się wywodzących, pod każdym względem podobnych do swoich

[3] W wypadku Mienżyńskiego nie do końca potwierdzonym.

ofiar, a co za tym idzie, zdolnych do zdobycia ich zaufania. On też wykorzystał wnioski carskiej Ochrany wyciągnięte po sprawie Jewno Azefa, z których wynikało, że podwójni agenci są niezwykle skuteczną bronią, o ile można ich w pełni kontrolować. CzeKa, a potem GPU, dały Artuzowowi narzędzia kontroli niedostępne służbom cywilizowanych krajów. Mógł wypuszczać swoich prowokatorów, podsuwając ich obcym wywiadom i organizacjom podziemnym, gdyż dzięki systemowi *krugowoj poruki*[4], byli oni zawsze oddani sowieckiej władzy, która dawała sobie prawo do ukarania za nielojalność nie tylko ich samych, lecz także ich rodziny i przyjaciół.

Artuzow, stosując bestialskie metody, pozostawał wybitnie inteligentnym i bezkompromisowo wierzącym w komunizm człowiekiem, który – gdy zawodziły tortury i strach – potrafił sięgnąć do metod zbliżonych do prania mózgu stosowanego przez współczesne nam sekty. Ofiarami takich „miękkich" metod oddziaływania padli m.in. polscy peowiacy. Schwytani przez CzeKę na szpiegowskiej misji w Rosji Sowieckiej, dzięki ideologicznej indoktrynacji zastosowanej przez Artuzowa stali się komunistycznymi fanatykami zwalczającymi własne państwo. Cała plejada polskich renegatów przeszła pod skrzydła Artuzowa: Wiktor Steckiewicz, Ignacy Dobrzyński, Wiktor Marczewski, Juna Przepilińska, Irena Zatorska, Karol Czyllok, Maria Nawrocka-Niedźwiałowska. Wszyscy oni niczym zombie szli ślepo za głosem Artuzowa. Nie dość, że zdradzali Polskę, to wciąż nakłaniali innych do zdrady. Byli jak zakażona rakiem tkanka, która stale dokonuje przerzutów, albo jak ofiary wampira, które same pokąsane kąsają kolejnych ludzi.

Gładkow, pomijając w swojej książce masowe egzekucje stosowane przez Artuzowa, z lubością skupia się na tej drugiej, jaśniejszej stronie *gienija kontrrazwiedki*. Opisuje kolejne operacje realizowane przez Artuzowa na wzór teatralnych inscenizacji. Prowokacyjne organizacje mające za zadanie przyciągnąć obce służby i rosyjską opozycję: „Pieski", „Liberalni Demokraci", „Monarchiczna Organizacja Centralnej Rosji" zwana Trustem… i ich ofiary – zwykle inteligentni, doświadczeni ludzie, oszukiwani jak dzieci dzięki niebywale rozbudowanym legendom Artuzowa. Można tu przytoczyć kilka przykładów – były terrorysta i wróg bolszewików Borys Sawinkow, którego oszukano po mistrzowsku, skłoniono do publicznego pokajania się przed władzą sowiecką, aby w końcu wyrzucić go z okna Łubianki. Równie gładko jak Sawinkowa wyprowadzono w pole Jurko Tiutiunnyka, walczącego z Sowietami atamana, którego także nakłoniono do kolaboracji z bolszewikami i ostatecznie rozstrzelano. Szpieg brytyjski Sidney Reilly, zabity strzałem w potylicę, został wcześniej ogłupiony przez Artuzowa do tego stopnia, że do końca nie rozumiał, co właściwie się z nim dzieje. Zachodnie służby wywiadowcze były systematycznie okłamywane. Skala oszustw była tak duża, że Artuzow mógł się pochwalić przed Politbiurem tym, że 95 proc. informacji zbieranych przez obcych szpiegów było produktami utworzonego przez niego Biura Dezinformacyjnego.

[4] Odpowiedzialności zbiorowej, w myśl której karani byli wszyscy ludzie powiązani z osobą represjonowaną.

T.K. Gładkow z lubością ciągnie ten spis wyczynów swojego bohatera, aby w końcu – wyjątkowo skąpo i niechętnie – opisać nieunikniony koniec wiernego sługi bolszewików. Artuzow zginął tak jak jego ofiary. Nie rozumiał, co się dzieje i dlaczego właściwie morduje go system, któremu oddał duszę. Oskarżony o zdradę i skatowany, został zabity strzałem w potylicę. Nie poszedł jednak na śmierć sam. Wraz z nim zostali zamordowani jego współpracownicy, nakłonieni przez niego do zdrady polscy renegaci, którym władza sowiecka „dziękowała" za wierną służbę, bijąc kablami, miażdżąc genitalia i wysyłając ich rodziny do łagrów. Artuzow, jak dziesiątki, setki tysięcy innych internacjonałów, oddał życie Golemowi, który go zniszczył. Nie mógł zrozumieć, że nowy system musiał się ich pozbyć, gdyż stworzona przez nich mieszanka okrucieństwa i inteligentnego polotu była dla tego systemu nie do przyjęcia. Dla nowych pokoleń enkawudzistów zdegenerowanych życiem w sowieckim raju burżuazyjna inteligencja i światowość *leninskoj gwardii* była zdradą proletariackiej *rodiny*. A ich usunięcie stwarzało wyrwanym z sowieckich wsi karierowiczom – niezdolnym do konkurowania z pierwszymi pokoleniami czekistów, którzy znali wiele języków oraz Europę – warunki do wspinania się po szczeblach kariery.

Na szczęście – dla Europy, a może i całego świata – zakończenie życia Christiana Frautschi przez strzał w potylicę był też podzwonnym dla współtworzonych przez niego służb specjalnych. Moloch sowieckich służb przetrwał i rozwijał się, ale po wytępieniu swoich najzdolniejszych pracowników nigdy nie odzyskał rozmachu i fantazji z początkowego stadium. Już nikt nie był w stanie oczarować ofiar bystrością sądów i ideologią. Z diady stosowanej przez Artuzowa, czyli okrucieństwa i inteligencji, zostało już tylko okrucieństwo.

Krzysztof Izak

Nabeel Qureshi, *W odpowiedzi na dżihad. Lepsza droga ku przyszłości*[1]

Recenzowana książka jest poświęcona nie bezpośrednio problematyce bezpieczeństwa i terroryzmu, lecz islamowi. Co prawda została ona opublikowana już dwa lata temu, ale z dwóch powodów jest warta omówienia. Po pierwsze została napisana przez byłego muzułmanina, który porzucił islam w wyniku własnych przemyśleń i przeszedł na chrześcijaństwo. Po drugie odkłamuje głoszone przez większość muzułmanów, wielu niemuzułmanów, polityków, zwolenników imigracji do Europy oraz islamofilów tezy o islamie jako religii tolerancji i pokoju oraz o terroryzmie jako zjawisku sprzecznym z islamem. Nie jest to pierwsza tego typu praca. Należy w tym miejscu wymienić chociażby książkę szwajcarskiego dziennikarza Sylvaina Bessona zatytułowaną *Islamizacja Zachodu?*[2], została ona jednak oparta przede wszystkim na aktach sądowych, analizach i odtajnionych materiałach służb specjalnych po zamachach z 11 września 2001 r. Cztery lata później Thilo Sarrazin, były senator i członek zarządu Bundesbanku, opublikował książkę *Niemcy likwidują się same: jak wystawiamy nasz kraj na ryzyko*[3]. Chociaż przytoczył w niej ogólnie znane fakty świadczące o braku integracji imigrantów ze społecznością kraju przyjmującego, to niemieccy politycy i media zaatakowały go, uznając jego argumenty za herezję. W atmosferze skandalu Sarrazin był zmuszony zrezygnować ze stanowiska w zarządzie Bundesbanku. Odcięły się od niego nie tylko CDU Angeli Merkel, ale również jego własna partia (SPD), chociaż wywodził się z politycznej lewicy. Kilka organizacji muzułmańskich w Niemczech pozwało go do sądu, a największe szkody przyniosły mu bezpodstawne oskarżenia o antysemityzm. Podobny ostracyzm spotkałby zapewne i Qureshiego, gdyby był mieszkańcem Europy Zachodniej, a nie USA. Chociaż niemieccy politycy uczynili wszystko, aby wyciszyć debatę o imigracji i islamie, popularność książki Sarrazina była rekordowa – 2 mln sprzedanych egzemplarzy. Na szczęście taka seria nienawistnych ataków nie spotkała francuskiego pisarza Michela Houellebecqa za powieść *Uległość*[4], w której snuje wizję dojścia do władzy we Francji muzułmanów podczas wyborów w 2022 r., ale prawdopodobnie dlatego, że premiera książki zbiegła się w czasie z zamachami na redakcję satyrycznego tygodnika „Charlie Hebdo" 7 stycznia 2015 r. Zbliżoną problematykę podejmują również polscy publicyści, chociażby Bogdan Dobosz[5],

[1] N. Qureshi, *W odpowiedzi na dżihad. Lepsza droga ku przyszłości*, Ustroń 2016, Szaron, 211 s.

[2] S. Besson, *Islamizacja Zachodu? Historia pewnego spisku*, Warszawa 2006.

[3] Książka nie została przetłumaczona na język polski. Tytuł oryginału: *Deutschland schafft sich ab: Wie wir unser Land aufs Spiel setzen*, Monachium 2010.

[4] M. Houellebeck, *Uległość*, Warszawa 2015.

[5] B. Dobosz, *Emiraty francuskie*, Warszawa 2016.

Paweł Lisicki[6] czy Marek Orzechowski[7]. Jednak najbliższe książce Qureshiego jest opracowanie ks. Krzysztofa Kościelniaka[8] oraz – ostatnio wydana – analiza islamu i jego systemu prawnego autorstwa Mirosława Sadowskiego[9].

Qureshi zgłębia problematykę islamu i wyjaśnia sprawy dotyczące dżihadu, islamskiego terroryzmu i powstania ISIS/IS. Inspiracją do napisania książki w *Odpowiedzi na dżihad* były dla amerykańskiego autora zamachy w Paryżu z 13 listopada 2015 r. (zginęło w nich 137 osób, a ponad 300 zostało rannych) oraz strzelanina 2 grudnia 2015 r. w San Bernardino w Kalifornii, podczas której muzułmańskie małżeństwo Sjed Rizwan Faruk i Tashfeen Malik zabili 14 podopiecznych ośrodka pomocy społecznej i ranili 21 kolejnych, a następnie zbiegli z miejsca zdarzenia. Zostali oni zastrzeleni w policyjnej obławie. Qureshi jest także autorem bestselleru „New York Timesa" *Szukając Allaha, znalazłem Jezusa*. Opisał w niej swoją duchową przemianę, która doprowadziła go do konwersji z islamu na chrześcijaństwo w wieku dwudziestu dwóch lat. Co ciekawe, Qureshi był wyznawcą ahmadijji, islamskiego nurtu oskarżanego o herezję ze względu na założyciela ruchu Mirzę Ghulama Ahmeda, który uważał się za proroka. W związku z tym, że islam uznaje Muhammada za ostatniego proroka, nazywając go „pieczęcią proroków" (*al-chatam an-nabijjin*), większość muzułmanów uważa achmadytów za heretyków[10].

Qureshi podzielił swoje opracowanie na trzy rozdziały: *Pochodzenie dżihadu*, *Dżihad dzisiaj* i *Dżihad w kontekście judeochrześcijańskim*, w których łącznie zostało zawartych 18 pytań zadawanych najczęściej autorowi na temat dżihadu i obszernych na nie odpowiedzi. Autor wyjaśnia w nich pochodzenie tego fenomenu i pokazuje jego dzisiejsze oblicze. Każdą odpowiedź kończy krótkie podsumowanie. Qureshi nie sugeruje, że jedynie jego wykładnia islamu i dżihadu jest słuszna. Pragnie odsłonić przemoc leżącą u podłoża islamu, której fundamentem jest *Koran* i tradycja (sunna) związana z życiem proroka Muhammada. Powrót do niej (*salafijja*) skutkuje obecnie nową falą przemocy. A więc jak długo islam jest praktykowany w sposób, który wzywa muzułmanów do powrotu do jego korzeni, tak długo skutkiem tych działań będzie przemoc. Z pewnością istnieją dodatkowe czynniki skłaniające muzułmanów do radykalnego islamu, niezależnie od tego, czy są to czynniki osobiste, jak poszukiwanie własnej tożsamości, czy polityczne, jak odpowiedź na rządowe opresje. Jednak

[6] P. Lisicki, *Dżihad i samozagłada Zachodu*, Lublin 2015.

[7] M. Orzechowski, *Mój sąsiad islamista. Kalifat u drzwi Europy*, Warszawa 2015; tenże, *Mój sąsiad islamista. Tunis–Paryż–Bruksela*, wyd. drugie zaktualizowane, Warszawa 2016.

[8] K. Kościelniak. *Dżihad, święta wojna w islamie*, Kraków 2001.

[9] M. Sadowski, *Islam. Religia i prawo*, Warszawa 2017.

[10] Muzułmańskie Stowarzyszenie Ahmadijja zostało założone w 1889 r. Jego członkowie wierzą, że Chrystus nie zmarł na krzyżu, lecz uciekł do Indii, gdzie zmarł w Srinagarze na terytorium Kaszmiru w wieku 120 lat. Ahmadijja łączy wiele cech fundamentalistycznego i konserwatywnego islamu z modernizmem. Jako cel stawia sobie rozpowszechnianie metodami pokojowymi odrodzonych wartości wczesnego islamu, skierowanych do muzułmanów, chrześcijan, wyznawców judaizmu i hinduizmu. Ta zasada jest dla wyznawców „szóstym filarem" islamu. Chociaż ahmadyci ze względu na oficjalny status założyciela ruchu znacznie odbiegają od głównej tradycji sunnizmu, to wypełniają główne zalecenia islamu.

bez względu na to, z jakimi czynnikami dodatkowymi ma się do czynienia, podstawy islamu i jego historia nie tylko zezwalają na użycie przemocy w celu osiągnięcia muzułmańskiej dominacji – one wręcz ją nakazują. Qureshi zaakcentował we wstępie, że jest chrześcijaninem, który porzucił islam po zgłębieniu fundamentów obu tych religii. Stara się być obiektywny w prezentowaniu informacji o dżihadzie. Stara się też nie wprowadzać do dyskusji wyraźnych chrześcijańskich poglądów, choć takie wkradły się do 18. pytania i wniosków. W ostatnich zdaniach wstępu autor pisze, że chrześcijańskie nauczanie miłości skierowane do nieprzyjaciół, nawet w obliczu śmierci, może być najpotężniejszą odpowiedzią na dżihad, którą ludzie mają dzisiaj do dyspozycji. Pozwala ona nie tylko przeciwdziałać dżihadowi, ale umożliwia traktowanie muzułmanów z największą godnością: jako ludzi stworzonych na obraz i podobieństwo Boga (wyznawcy islamu zaprzeczają tej tezie).

Brak miejsca nie pozwala, niestety, na skomentowanie odpowiedzi na każde pytanie postawione przez autora w poszczególnych rozdziałach (po sześć pytań w każdym rozdziale). Warto jednak wymienić wszystkie pytania i szerzej omówić najistotniejsze zagadnienia zawarte w odpowiedziach, w których autor często cytuje wybrane wersety *Kranu* i hadisy[11] dla poparcia swoich argumentów. Należy przy tym zwrócić uwagę na błąd (być może popełniony przez autora, a może przez tłumacza lub wydawcę) polegający na identycznym brzmieniu 17. i 18. pytania w treści książki – *Jak ma się dżihad do wypraw krzyżowych?* Korekta tego błędu została w pewien sposób naprawiona przez umieszczenie w spisie treści następującego zapisu: przy pytaniu 17. – *Pytanie siedemnaste*, a przy pytaniu 18. – treść pytania (podanego jak wyżej).

Rozdział pierwszy:

1. *Czym jest islam?*
2. *Czy islam jest „religią pokoju”?*
3. *Czym jest dżihad?*
4. *Czy dżihad jest obecny w Koranie i życiu Mahometa?*
5. *Czym jest szariat?*
6. *Czy islam szerzony był mieczem?*

Rozdział drugi:

1. *Czym jest radykalny islam?*
2. *Czy islam potrzebuje reformacji?*
3. *Czym są Al-Kaida, ISIS i Boko Haram?*
4. *Kim są prawdziwi muzułmanie?*
5. *Dlaczego muzułmanie poddają się radykalizacji?*
6. *Czy muzułmanie dążą do przejęcia Zachodu szariatem?*

[11] Hadisy są przekazami o wypowiedziach i czynach proroka Muhammada. Dzielą się na hadisy: mocne, czyli w pełni wiarygodne i autorytatywne (*sahih*), dobre, co do których istnieją niewielkie wątpliwości (*hasana*), słabe, często kwestionowane pod względem autentyczności (*daif*) i zmyślone, czyli fałszywe (*mawdu*). Hadisy stanowią obok *Koranu* główne źródło prawa (szariatu). Są często publikowane w wielotomowych opracowaniach pod wspólnym tytułem *Kitab as-sitta* („Sześcioksiąg”).

Rozdział trzeci:

1. *Czy muzułmanie i chrześcijanie wielbią tego samego Boga?*
2. *Dlaczego niektórzy chrześcijanie nazywają Boga „Allahem”?*
3. *Jak się ma dżihad do starotestamentowych działań wojennych?*
4. *Czego naucza Jezus o przemocy?*
5. *Pytanie siedemnaste.*
6. *Jak ma się dżihad do wypraw krzyżowych?*

Omawiając koncepcję dżihadu, Qureshi zgodnie z tradycją dzieli go na dżihad większy (*dżihad akbar*) i dżihad mniejszy (*dżihad asghar*). W odróżnieniu od innych autorów starających się dowieść, że ten pierwszy rodzaj dżihadu jest walką z własnymi przywarami, żądzami czy egoizmem oraz pogłębianiem swojej wiary na ścieżce Allaha, a drugi oznacza walkę zbrojną w obronie islamu, Qureshi odwraca tę kolejność. Według niego główne użycie słowa „dżihad” zawsze sugerowało walkę fizyczną. Przedstawianie dżihadu głównie w aspekcie duchowych starań jest niespójne z *Koranem*, hadisami, historią islamu i klasyczną islamską hermeneutyką. Mało tego, dżihad będący walką zbrojną zajmował tak ważne miejsce w genezie islamu, że przez niektórych autorów został nazwany „szóstym filarem islamu” (obok wyznania wiary – *szahada*, modlitwy – *salat*, postu w miesiącu ramadan – *saum*, jałmużny – *zakat* i pielgrzymki do Mekki – *hadżdż*). Skłonność do przemocy i walka zbrojna we wczesnych społecznościach muzułmańskich nasilały się od momentu *hidżry*, czyli ucieczki proroka z Mekki do Medyny w 622 r. Za życia Muhammada zorganizowano 38 wypraw bojowych (według innych źródeł było ich ponad 60), a w 25 z nich prorok uczestniczył osobiście. Były to tzw. błogosławione ataki (*maghazi al-mabruka*) i napady rabunki (*razzia*). Ich celem było zdobycie łupów i kobiet, a dopiero potem kontrola podbitego terytorium. Po śmierci proroka Muhammada w 632 r. muzułmanie bardzo dynamicznie podbijali militarnie Bliski Wschód i Afrykę Północną.

Potrzeba prowadzenia działań wojennych przez pierwszych muzułmanów ma swoje odzwierciedlenie w *Koranie*. Jest wiele wersetów wzywających do przemocy, które powstały w okresie medyńskim życia proroka (622–632). Qureshi skoncentrował swoją uwagę na surze dziewiątej *Koranu*, zatytułowanej *Tawba*, która według niego jest ostatnim chronologicznie, głównym rozdziałem świętej księgi islamu. Autor tłumaczy jej tytuł jako *Ultimatum*, podczas gdy w polskim wydaniu *Koranu* w przekładzie Józefa Bielawskiego z języka arabskiego tytuł tej sury brzmi *Skrucha*[12].

[12] Sura dziewiąta rzadko nazywana jest *Al-Bara'a*, czyli *Ultimatum*, ale pod taką nazwą występuje w hadisah. Józef Bielawski pisze w komentarzu do polskiego wydania *Koranu*, że tytuł *Skrucha* wziął się od słowa „*tawba*” powtarzającego się wiele razy. Oprócz tego powszechnie przyjętego tytułu przyjmuje się niekiedy jeszcze inny tytuł pochodzący od słowa z wersetu pierwszego, a mianowicie „*al-bara'a*”, ale słowo to jest tłumaczone przez Bielawskiego jako „zwolnienie się” (z obowiązku) lub „uniewinnienie”. Jak wynika z treści sury, chodzi tu o zwolnienie z zobowiązania zaciągniętego w zawartym traktacie z mieszkańcami Mekki będącymi politeistami. Mowa o „zwolnieniu się z zobowiązania” ujętego w traktacie, jaki prorok zawarł pod Hudajbijją z Mekkańczykami w 628 r. Muhammad wypowiedział ten układ po zdobyciu Mekki w 630 r. *Skrucha* jest jedną z ostatnich sur, a większa jej część dotyczy wielkiej wyprawy wojennej proroka na północ,

Podobnie do polskiej interpretacji tytuł tej sury jest objaśniony w znanym tłumaczeniu angielskim (*Repentance*) i innych przekładach na ten język[13]. Natomiast dwujęzyczne arabsko-polskie wydanie Muzułmańskiego Stowarzyszenia Ahmadijja jest pozbawione tłumaczenia na język polski poszczególnych tytułów rozdziałów *Koranu*[14]. Słowo „*tawba*" może być przetłumaczone również jako „pokuta". Niezależnie jednak od nazwy ten rozdział najbardziej odwołuje się do przemocy. Ze względu na swoje zdecydowane nakazy i bezkompromisowość jego treść jest odczytywana jako ostateczne nakazy Allaha dla jego wysłannika, unieważniające wcześniejsze pokojowe fragmenty *Koranu* z mekkańskiego okresu życia Muhammada (do 622 r.), gdy niewielka grupa wyznawców islamu żyjących w niechętnym im środowisku musiała liczyć się ze zdaniem wrogiej im większości. Po wkroczeniu do Mekki w 630 r. wszystkie wcześniejsze traktaty zawarte przez Muhammada z politeistami zostały zerwane i narzucono im ultimatum: przyjmą islam lub zostaną zabici. Sura dziewiąta nakazuje porzucenie wszelkich umów z politeistami oraz podporządkowanie żydów i chrześcijan. Muzułmanie muszą walczyć zgodnie z tą surą, a jeśli tego nie czynią, to ich wiara jest kwestionowana i są zaliczani do grona hipokrytów (*munafikun* – w świecie muzułmańskim określenie kogoś słowem „*munafik*" stanowi największą obelgę). Jeśli muzułmanie walczą, są im obiecane dwie nagrody: łupy wojenne albo raj osiągnięty przez męczeństwo (najlepszym tego przykładem jest działalność członków Państwa Islamskiego i innych organizacji). Allah zawarł układ z mudżahedinami (bojownikami dżihadu): zabić albo być zabitym podczas walki dla chwały Allaha i islamu. W tym miejscu należy zacytować słowa autora książki: *Mimo że Koran prawdopodobnie nie przewiduje czegoś podobnego do terroryzmu XXI wieku*[15]*, nakazuje muzułmanom używać terroru i siać strach: „Przygotujcie przeciwko nim, ile możecie sił i oddziałów konnicy, którymi moglibyście przerazić wroga Boga i wroga waszego". To nauczanie Koranu potwierdza się poprzez hadisy. Jak mówi Mahomet: „Odniosłem zwycięstwo przez terror" (Sahih al-Buchari 4.52.220). Szerzenie strachu w sercach wrogów Allaha jest zatem nakazane przez Koran i ma odzwierciedlenie w życiu Mahometa*.

Wersety w surze dziewiątej potwierdzają tezę autora o dżihadzie jako walce ofensywnej, podczas gdy wielu muzułmanów świadomych udziału Muhammada w wielu bitwach wierzy i twierdzi, że bitwy te miały charakter defensywny, mimo że już pierwsza konfrontacja pod Badr (624 r.) była najzwyklejszą zbrojną napaścią na kupiecką karawanę z Mekki. Sura *Skrucha* daje również muzułmanom nakaz walki z żydami i chrześcijanami ze względu na ich religię, a nie ze względu na jakąkolwiek agresję z ich strony. To rozumowanie jest potwierdzone wysłaniem przez Muhammada

która zatrzymała się pod Tabukiem, gdzie stoczono bitwę z wojskami bizantyjskimi. Por. *Koran*, J. Bielawski (przekł.), Warszawa 1986, s. 875–876.

[13] Tekst bilingwiczny arabsko-angielski: M. Pickthall, *The Maeaning of The Gloriopus Qur'an*, Kuala Lumpur 2002.

[14] *Święty Koran. Tekst arabski i tłumaczenie polskie*, Surrey 1996.

[15] Autor nieprzypadkowo użył takiego sformułowania, ponieważ *Koran* istniejący od zawsze obok Allaha według islamskich teologów zawiera treści wciąż aktualne i zakazana jest jego reinterpretacja mimo zmieniającej się rzeczywistości.

wojowników przeciwko Bizantyjczykom, którzy stoczyli bitwę pod Tabukiem (630 r.), mimo że bizantyjscy chrześcijanie nigdy nie zagrażali muzułmanom. Innym świadectwem ofensywnego dżihadu okresu pierwszych muzułmanów jest *Kronika Jana z Nikiu*. Z tego miasta, położonego w Egipcie, zbiegli bizantyjscy żołnierze na wieść o zbliżających się wojskach arabskich dowodzonych przez Amra ibn al-Asa, natomiast cała ludność cywilna z dziećmi włącznie została wymordowana. Podobny los spotkał mieszkańców innych miast chrześcijańskiego Egiptu. Współcześni muzułmanie wierzą, że posłuszeństwo pierwszych generacji wyznawców islamu pozwoliło rozszerzyć muzułmańskie imperium ponad wszelkie przypuszczenia. Dało też podstawy Złotemu Wiekowi Islamu, który muzułmanie zachowują w sercu jako czas, kiedy ludzie byli posłuszni Allahowi. Wyznawcy islamu byli wtedy u szczytu potęgi, dlatego też muzułmanie są dumni z własnej przeszłości, wychwalają dawne wartości i wspominają pokolenie szlachetnych przodków (*as-salaf as-salih*) za ich poświęcenie. Jeśli będą brać z nich przykład posłuszeństwa wobec Allaha i podążać za prorokiem w jedności, Allah znowu ich pobłogosławi i przywróci ich potęgę. To oczekiwanie na hegemonię islamu i nostalgiczne pojęcie Złotego Wieku stało się źródłem radykalizacji wiary.

W drugim rozdziale książki autor porusza temat narodzin radykalnego islamu i współczesnego dżihadu. Jest dla niego rzeczą oczywistą, że rewolucja przemysłowa i europejska kolonizacja położyły kres dominacji islamu w wielu zakątkach świata. Uczeni muzułmańscy zaczęli szukać odpowiedzi na pytanie: jak to się stało, że świat islamu popadł w zależność ekonomiczną i kulturową od „niewiernych"? Reformiści podjęli próbę oczyszczenia religii z naleciałości wypaczających islam i w przeciwieństwie do modernistów szukali odrodzenia potęgi islamu w powrocie do źródeł religii i ścisłego przestrzegania jej zasad. Qureshi przybliża też sylwetki trzech znanych przedstawicieli radykalnego nurtu islamu. Abu al-Ala al-Mawdudi (1903–1979), jeden z największych egzegetów *Koranu*, w pracy zatytułowanej *Dżihad w Islamie* pisał – wbrew tezom wczesnych muzułmańskich uczonych – że dżihad nie był staraniem się o podbicie obcych islamowi ziem, ale raczej szczerym pragnieniem muzułmanów szerzenia religii, którą kochali. To przez dżihad niemuzułmanie mogli zetknąć się z islamem. Z jego wywodów wynika, że islamscy wojownicy nie podbijali wciąż nowych terenów, nie mordowali, nie zamieniali „niewiernych" w niewolników, nie byli kolonialistami, lecz wyzwolicielami i bojownikami o wolność. Pisał, że islam jest rewolucyjną religią, która istnieje po to, aby zniszczyć każdą formę państwa stworzonego przez ludzi. W tych rewolucyjnych zapędach islam nie będzie się ograniczał do jednego kraju czy grupy państw. Jego celem jest rewolucja na skalę światową. Rozumowanie i apologetyka Al-Mawdudiego są bardzo wpływowe do dziś w świecie islamu. Już w latach 40. XX w. Ruhollah Chomeini, późniejszy przywódca rewolucji islamskiej w Iranie, sygnalizował, że jest gotów posunąć się do metod terrorystycznych (zapewnić im odpowiednie teologiczne zaplecze, a także materialne wsparcie), żeby upokorzyć tych, których uważał za wrogów islamu. *Islam mówi tak: „Wszelkie dobro istnieje tylko dzięki mieczowi i w cieniu miecza! Ludzi nie da się zmusić do posłuszeństwa inaczej niż mieczem! Miecz jest kluczem do raju, który otworzy się tylko*

przed świątobliwymi bojownikami"[16]. Dla Sajjida Kutba (1906–1966), który dwa lata spędził w Stanach Zjednoczonych (1948–1950), Zachód był przerażającą kulturą ze źle wychowanym zbiorowiskiem brutalnych i nieokrzesanych ludzi, pozbawionych jakichkolwiek duchowych wartości. Po powrocie do Egiptu został ideologiem Braci Muzułmanów (Al-Ichwan al-Muslimin)[17] i wzywał do obalenia rządów prezydenta Gamala Abdel Nasera, który był pierwszym celem egipskich radykałów. W świetle nauk dżihadu należało przede wszystkim poskromić „bliskiego wroga" (*adu karib*), czyli oczyścić społeczność muzułmańską. „Daleki wróg" (*adu baid*), czyli Zachód, musiał zaczekać, aż islam sam się zreformuje. Dzihad powinien rozpocząć się od pokojowego proklamowania islamu jako religii światowej, następnie zaangażować w ograniczone działania wojenne, wyegzekwować kary za opresję rządzących wobec islamskiego społeczeństwa, aby w końcu rozpocząć niekończące się działania wojenne przeciw niemuzułmańskiemu światu. Pozostając pod wpływem Al-Mawdudiego, Kutb postrzegał dżihad jako wyzwolenie niemuzułmańskiej części ludzkości, przy zapewnieniu, że niemuzułmaninowi dane jest usłyszeć i rozważyć przesłanie islamu, co może się nie zdarzyć, dopóki dżihad nie zostanie przeprowadzony[18]. Z kolei Muhammad Abd as-Salam Faradż (1952–1982), autor pracy zatytułowanej *Dżihad zapomnianą powinnością*, odwoływał się do założeń Kutba i twierdził, że muzułmańscy przywódcy stali się apostatami, a muzułmanie muszą powrócić do czystej formy islamu. Opowiadał się za dżihadem jako walką z niemuzułmanami, którą Allah pobłogosławi, dając muzułmanom nowe terytoria, gdzie będę w stanie zakładać państwo islamskie i wprowadzić kalifat. Tam islam mógłby być praktykowany w swojej czystej postaci. Faradż wzmocnił deklarację Kutba dotyczącą apostazji przywódców. W ten sposób powstał grunt pod założenia *takfiru*, czyli oskarżenia o bezbożność lub o brak wiary, idei głoszonej przez ekstremistyczne organizacje islamskie na czele z Al-Kaidą i Państwem Islamskim. Te kryteria to: otwarta manifestacja niewiary, ignorowanie szariatu oraz odmowa zaangażowania w dżihad w celach obrony *ummy*. Państwo Islamskie podzieliło wszystkich muzułmanów na „ludzi raju", czyli samych siebie i „ludzi piekła" – wszystkich pozostałych. Każdego wiernego, którego interpretacja *Koranu* i szariatu nie odpowiada modelowi głoszonemu przez ISIS/IS, uznaje się za członka tej drugiej grupy – apostatę i bezbożnika, którego należy wyeliminować ze świętej społeczności.

Autor wysuwa tezę, że radykalny islam narodził się z frustracji pozostawania w politycznej niższości współczesnych narodów muzułmańskich względem Zachodu. Opierając się na koranicznej obietnicy, że Allah zagwarantuje zwycięstwo tym, którzy dla niego walczą, radykalni muzułmanie wierzą, że tych, którzy są oddani prawdziwej

[16] L. Wright, *Wyniosłe wieże. Al-Kaida i atak na Amerykę*, Wołowiec 2018, s. 67–68.

[17] Motto Braci Muzułmanów brzmi: „Allah jest naszym celem, Prorok jest naszym przywódcą, Koran jest naszą konstytucją, dżihad jest naszą drogą, a śmierć w imię Allaha naszym pragnieniem".

[18] W latach 90 XX w. Stowarzyszenie Studentów Muzułmańskich w RP publikowało w Białymstoku, gdzie znajdowała się główna siedziba tej organizacji, polskie tłumaczenia prac Al-Mawdudiego i Kutba. Dziś publikacja niektórych z nich byłaby zakazana ze względu na treści zachęcające do przemocy.

nauce islamu i są gorliwi w jej wypełnianiu, czeka kolejny Złoty Wiek. To oni ujrzą przywróconą chwałę islamu. Radykalny islam wywodzi się z rozumowania, że przeciętne praktykowanie islamu w dzisiejszych czasach jest zbyt oddalone od nauczania Muhammada i *Koranu*. Radykałowie często uważają tzw. umiarkowanych muzułmanów[19] za apostatów ze względu na ich brak gorliwości w przestrzeganiu nauk islamu, a *Koran* daje podstawę do podjęcia dżihadu przeciwko takim właśnie muzułmańskim hipokrytom (*munafikun al-muslimin*). Radykalizm islamski wykorzystuje ponadto egzystencjalny kryzys panujący wśród młodych muzułmanów, tworzy związek między nauczaniem wartości radykalnych w meczetach i cyberprzestrzeni a uznaniem ekstremistycznej ideologii, aktywnością rewolucyjną i przyjęciem wiary w męczeństwo nagrodzone wiecznym szczęściem w raju. Jednocześnie wbrew temu, co mówi wielu zachodnich muzułmanów, że terroryści nie są prawdziwymi wyznawcami islamu, dla Qureshiego właśnie takimi są. Wielbią bowiem Allaha, starają się podążać drogą wyznaczoną przez proroka, przestrzegają islamskich obowiązków i wyrażają troskę o *ummę*. Kładą większy nacisk na realizowanie założeń islamu, niż każdy przeciętny muzułmanin, który twierdzi, że islam jest religią pokoju. Ci ostatni nie wypełniają jednego z poleceń *Koranu*, który nakazuje im walczyć ze swoimi wrogami, w tym i członkami rodziny, oraz tymi, którzy nie walczą z muzułmanami nawet w obliczu męczeńskiej śmierci, ponieważ ta prowadzi do zbawienia. Nieustanna walka ma na celu ustanowienie islamu jako jedynej religii na ziemi. Wielu pokojowo nastawionych muzułmanów nie czyni tego, ignoruje niektóre tradycje, jak gdyby nie istniały. W tym przypadku, mimo że mogą uważać się za „dobrych muzułmanów", to jednak w ich myśleniu brakuje spójności z nakazami ich wiary, ponieważ sposób wyrażania islamu, który jest pełen przemocy, jest zawarty w *Koranie* i hadisach. Pokojowa wersja islamu musiałaby zredefiniować tradycję proroka, aby być wewnętrznie spójną, lub ją ignorować. Niezależnie od tego, którą opcję wybiorą nastawieni pokojowo muzułmanie, określanie przez nich islamskich terrorystów jako niemuzułmanów jest z gruntu fałszywe. Należy też dostrzec jeszcze jeden ważny argument – wspólnym mianownikiem wszystkich zradykalizowanych muzułmanów jest ich ostateczny wybór wierności surowszym i dosłownie odczytywanym fundamentom islamu, niż jest to w przypadku większości pozostałych muzułmanów.

[19] Jest to pojęcie zbyt ogólne i nie wiadomo, co się pod nim kryje. Muzułmanie niepraktykujący, zlaicyzowani, zintegrowani lub też zasymilowani ze społecznościami krajów ich przyjmujących zgodnie z doktryną islamu nie są już wyznawcami tej religii. Powodem, dla którego muzułmanie mogą być zarówno pobożni, jak i pokojowo nastawieni, pomimo pełnego przemocy nauczania *Koranu* i hadisów, jest interpretacja islamu przez osoby z dużym autorytetem, często zgodnie z różnymi szkołami myśli i latami tradycji. Kiedy muzułmanie pragną obejść to, co nakazują owe autorytety i powrócić do korzeni swojej wiary, niezależnie, czy wynika to z rozczarowania obecnym sposobem wyrażania islamu, czy chęci zadowolenia Allaha i zdobycia jego przychylności lub błogosławieństwa, często ich postępowanie w wyrażaniu wiary jest pełne przemocy. Próby zmodernizowania tej religii i dostosowania jej do realiów XXI wieku są właśnie tym radykalnym islamem. Przedstawiciele postępowej myśli muzułmańskiej, mimo że nieliczni i z ograniczonymi wpływami, są obecni i działają, ryzykując często życie.

O ile skłonność do przemocy przejawia mniejsza liczba muzułmanów, to, według Qureshiego, wprowadzenia szariatu w Europie chciałaby już prawie połowa z nich, a w USA jedna trzecia. Autor zacytował słowa Muammara Kaddafiego, byłego przywódcy Libii, wypowiedziane w kwietniu 2006 r. dla telewizji Al-Dżazira: *Mamy 50 mln muzułmanów w Europie. Oni są znakiem, że Allah zapewni islamowi zwycięstwo w Europie – bez miecza, bez broni, bez podbojów* […]. *Oni zmienią ją w muzułmański kontynent w ciągu kilku dekad. Europa jest w kłopotliwym położeniu. Podobnie Ameryka. Powinni zgodzić się na islam z upływem czasu, w przeciwnym wypadku będą zmuszeni wypowiedzieć wojnę muzułmanom*. To oświadczenie potwierdziło obawę wielu konserwatystów na Zachodzie, że muzułmanie rozpoczęli wojnę demograficzną i ideologiczną i usiłują obalić zachodnie systemy prawne i kulturę. Oświadczenie Kaddafiego wywołało dyskusję, która pogłębia się od tamtego czasu i skupia głównie na dwóch kwestiach: szariatu i muzułmańskiej demografii. Na rzecz dominacji islamu w Europie aktywnie pracuje też Organizacja Współpracy Islamskiej (OIC), druga co do wielkości po ONZ organizacja międzynarodowa, skupiająca 57 państw z siedzibą w Arabii Saudyjskiej. Publikuje ona coroczny raport na temat islamofobii na Zachodzie. Qureshi zwraca uwagę, że „islamofobia" jest słabo opisaną koncepcją, rzekomo stosowaną do określenia uprzedzeń w stosunku do muzułmanów, ale wielokrotnie używaną po prostu jako ogólny termin określający jakąkolwiek krytykę islamu czy muzułmanów, prawdziwą lub wyimaginowaną. Przez wspomniane publikacje i naciski polityczne OIC subiektywnie lobbuje przeciwko wolności słowa, licząc na uciszenie krytyki islamu, co często jest skuteczne, jeśli patrzy się na sytuację w wielu krajach UE. Według OIC wolność słowa chroni ludzi, którzy (…) *raz po raz stają się powodem nieuzasadnionych napięć, podejrzeń i niepokojów społecznych, szkalując islamską wiarę poprzez ogromne zniekształcenia i błędną interpretację, wkraczając na grząski grunt i obrażając uczucia religijne muzułmanów*. Innymi słowy ludzie, którzy krytykują islam, są winni niepokojów w środowiskach muzułmańskich. Orzeczenie OIC jest bezpośrednio sprzeczne z wolnością słowa, ale całkowicie zgodne z szariatem. W USA podobne wysiłki czyni Rada Stosunków Amerykańsko-Islamskich (CAIR), znajdująca się pod silnym wpływem międzynarodowego ruchu Braci Muzułmanów. CAIR oskarża o islamofobię innych muzułmanów, którzy nie zgadzają się z jej decyzjami. Autor recenzowanej publikacji przytacza badania Raheel Razy, Kanadyjki przewodniczącej północnoamerykańskiej organizacji Muslims Facing Tomorrow, według której w świecie muzułmańskim przeważa radykalizm, zależy tylko, jak się go rozumie. Jeśli za radykalnych muzułmanów uważa się tylko mudżahedinów, wtedy ich liczba będzie znikoma, ale jeśli za radykalnych muzułmanów uzna się również tych, którzy pragną, aby *umma* była zarządzana zgodnie z szariatem, wówczas będą oni dominować liczbowo w świecie muzułmańskim. Większość muzułmanów odrzuca też zachodni model świeckiego demokratycznego państwa nieprzystajacy do uniwersalnych rządów opartych na islamie, którego jedną naturą jest uległość, ale tylko wobec Allaha, natomiast drugą – dominacja, narzucanie swoich praw wszystkim narodom i stopniowe obejmowanie swoją władzą całej ziemi.

W trzecim rozdziale Qureshi podejmuje bardzo interesujące rozważania dotyczące zasadniczych różnic w pojmowaniu Boga przez muzułmanów i chrześcijan oraz istoty przemocy w obu religiach. Jako były muzułmanin, a obecnie praktykujący chrześcijanin znający *Koran* i *Biblię*, wyjaśnia sprzeczności w rozumieniu obu religii, obalając przy tym wiele stereotypów w sposobie myślenia wyznawców chrześcijaństwa i islamu.

Zdaniem autora muzułmanie i chrześcijanie wbrew obiegowym poglądom nie wierzą w tego samego Boga. Dzieje się tak, mimo że *Koran* zapewnia, że *Tora* i *Ewangelia* są natchnionymi pismami i że żydzi i chrześcijanie są Ludem Księgi oraz, że *Koran* zwraca się do muzułmanów, aby mówili żydom i chrześcijanom, że mają jednego Boga. Tożsamość Boga muzułmanów jest inna od tożsamości Boga chrześcijan. Jezus (Isa) jest określany w *Koranie* nie jako Syn Boży, lecz jako jeden z wielu proroków. Muzułmanie odrzucają też wiarę w jego śmierć na krzyżu, zmartwychwstanie i kult Matki Bożej (doketyzm). Islam też stanowczo potępia doktrynę Trójcy Świętej, zestawiając z nią dla kontrastu własny fundamentalny dogmat *tawhidu*, czyli jedyności Boga. *Tawhid* w tak zdecydowany sposób zaprzecza istnieniu Trójcy Świętej, że zmusza do stwierdzenia, że pojęcie Boga w islamie jest całkowicie inne od doktryny Boga w chrześcijaństwie. Są one wręcz przeciwstawne. Ponadto dla muzułmanów Bóg nie jest ojcem ludzkości, ponieważ ludzie są tylko istotami, które Bóg stworzył. Te dogmatyczne różnice w postrzeganiu Boga znalazły swoje odbicie w postanowieniu malezyjskiego Sądu Najwyższego, który w czerwcu 2016 r. wydał orzeczenie potwierdzające nielegalność używania przez miejscowych chrześcijan nazwy „Allah" w odniesieniu do chrześcijańskiego Boga. Wcześniej Kościół katolicki kwestionował ten zakaz na podstawie tego, że malezyjskie tłumaczenie *Biblii* od wieków używa słowa „Allah". Początkowo Kościołowi udało się przekonać rząd malezyjski do zniesienia zakazu, ale w odpowiedzi muzułmanie zaczęli atakować chrześcijańskie świątynie, co ostatecznie doprowadziło do ponownego wprowadzenia zakazu w październiku 2013 r. Trzy miesiące później skonfiskowano chrześcijanom egzemplarze *Biblii*, czego podstawą było nazywanie w tej księdze Boga Allahem, a w czerwcu 2014 r. sędziowie potwierdzili to bezkompromisowe stanowisko wobec chrześcijan.

Kolejnym istotnym tematem rozważań Qureshiego jest koncepcja dżihadu jako islamskiej doktryny wojennej i żydowskich zdarzeń wojennych ze Starego Testamentu. Muzułmańscy teolodzy zarzucają żydom i chrześcijanom, że ich *Biblia* też jest pełna przemocy. Tymczasem święte księgi muzułmanów i chrześcijan to dwie różne kategorie. *Koran* to słowa Allaha przekazane prorokowi Muhammadowi za pośrednictwem archanioła Gabriela, podczas gdy *Stary Testament* to napisane przez ludzi teksty o różnym charakterze, w których odnotowano wiele zdarzeń rzeczywistych lub mitycznych, niekoniecznie pochwalanych przez Boga. Takie wydarzenia nie powinny stanowić tej samej kategorii, co bitwy i wojny, które nakazał sam Allah. Przemoc w *Starym Testamencie* nakazana przez Boga nastąpiła po 400 latach oczekiwania. Bóg przypomniał żydom, że wygnanie innych ludów miało miejsce nie ze względu na to, że żydzi byli najlepszymi z ludzi, co w *Koranie* przekazano muzułmanom, ale dlatego,

że grzeszyli przeciw Bogu. Działania wojenne w *Starym Testamencie* nie są przykładem, na którym chrześcijanie wzorują dzisiaj swoje życie. Dzieje chrześcijaństwa nie kształtowały się od pokojowych do pełnych przemocy, lecz zupełnie na odwrót. Tymczasem życie proroka Muhammada z pokojowego zamieniło się w pełne nasilającej się coraz bardziej przemocy. *Koran* nakazuje muzułmanom walczyć z żydami i chrześcijanami, tak aby Allah mógł uczynić islam religią panującą nad wszystkimi innymi religiami.

Nakazem dla chrześcijan jest miłość i miłosierdzie, dla muzułmanów zaś – dżihad. Rozwijając ten wątek, autor porównuje koncepcję dżihadu w islamie do świętej wojny w chrześcijaństwie. Chrześcijanie dopiero tysiąc lat po Jezusie rozwinęli ideę świętej wojny, podczas gdy sam Muhammad i *Koran* nauczali, że walka jest zbawienna. Święta wojna leży u podstaw islamskiej wiary. Qureshi polemizuje z poglądami wielu polityków i autorów na temat wypraw krzyżowych, m.in. Johna Esposito, profesora studiów islamskich w Georgetown University, który w książce *Islam: prosta ścieżka* napisał: *Pięć wieków pokojowej koegzystencji legło w gruzach poprzez polityczne wydarzenia i imperialno-papieskie rozgrywki sił, które doprowadziły do trwającej wieki serii tak zwanych świętych wojen, kierujących chrześcijaństwo przeciwko islamowi i pozostawiających trwającą do dziś spuściznę niezrozumienia i braku zaufania*. Jednak te słowa są oparte na fikcji, która przeważa w powszechnym rozumieniu krucjat, także po stronie wielu autorów zachodnich. Zapominają oni o tym, że to Muhammad pierwszy wystąpił przeciwko bizantyjskim chrześcijanom. Następnie muzułmanie podporządkowywali sobie chrześcijańskie ziemie (i nie tylko), tak jak nakazywał im *Koran,* i to muzułmanie podbili dwie trzecie świata chrześcijańskiego przed pierwszą wyprawą krzyżową. W opinii Qureshiego, kiedy potępia się wyprawy krzyżowe, powinno się mieć na względzie ich przyczyny i okoliczności – były to wysiłki podjęte w obronie jako następstwo podboju chrześcijańskiego świata przez muzułmanów. Autor potępia krucjaty, w ramach których przeprowadzono rzeź niewinnych żydów w Europie i muzułmanów w Jerozolimie. To pozbawione sensu okrucieństwo było prowadzone w imię Chrystusa. Przyznaje też, że czułby się dużo lepiej, gdyby wysiłki krzyżowców wynikały z nakazu przywódców poszczególnych państw Europy, a nie Kościoła. Jednak jako chrześcijanin jest wdzięczny, że tysiąc lat zajęło chrześcijanom zniekształcanie nauczania Jezusa do tego stopnia, że krucjaty stały się nakazem religijnym jako święta wojna. Chrystus nie pozostawił żadnego tego rodzaju nakazu. Narodziła się ona dopiero w XI wieku. Dla kontrastu – pełen przemocy, ofensywny dżihad prowadzony dzisiaj przez muzułmańskie organizacje ekstremistyczne jest koranicznym nakazem. Islam wzywa swoich wyznawców do angażowania się w świętą wojnę, oferując im zbawienie, jeśli zginą w bitwie. Muzułmanom tysiąc trzysta lat zajęło odejście od radykalnych fundamentów ich religii, aby mogli upierać się przy tezie głoszącej islam jako religię pokoju.

We wnioskach autor pisze: […] *niemalże wszyscy muzułmanie, nieważne, czy nastawieni pokojowo, czy nie, wierzą, że wyznają pierwotną formę islamu. Muzułmanie, którzy uważnie studiują koraniczne teksty, zostaną ostatecznie postawieni przed*

wnioskami, których nie da się uniknąć, a które mówią, że fundamenty ich wiary są pełne przemocy. Tak było w moim przypadku. Wypierałem te wnioski przez lata, ale kiedy rzeczywistość stała się nieunikniona, stanąłem na rozdrożu i musiałem wybrać pomiędzy apostazją, apatią a radykalizacją. Jak wiadomo Qureshi wybrał to pierwsze, ponieważ stanął przeciwko tradycji islamu, która jest pełna przemocy. Miał bowiem przyjaciela chrześcijanina, który mu zasugerował, że islam nie jest jego jedynym wyborem oraz że istnieją szczególne powody, aby przyjąć ewangelię. Według przyjaciela Qureshiego laicyzm i ateizm nie stanowią dobrej alternatywy dla islamu, ponieważ nie są duchowo rozbudowane, do czego jest przywiązana większość muzułmanów. Obecnie lawinowo narasta liczba sfrustrowanych wyznawców islamu. Przyczyną tego są treści przekazywane w cyberprzestrzeni przez media społecznościowe będące źródłem propagandy, indoktrynacji i rekrutacji. Autor sugeruje, aby aktywnie wzbudzać wśród muzułmanów emocje miłości i przyjaźni, uznając jednocześnie prawdę o islamie. Prawdopodobnie jest to niemożliwe, ponieważ prawda o islamie przedstawiona przez Qureshiego pozbawia niemuzułmanów optymistycznej wizji przyszłości, zwłaszcza w kontekście dynamicznie wzrastającej liczby muzułmanów w Europie i postępującej ich radykalizacji.

Publikacja zawiera cztery dodatki: A – kalendarium dżihadu w Islamie od narodzin proroka Muhammada do ataku terrorystycznego w San Bernardino w grudniu 2015 r.; B – wypowiedzi proroka na temat dżihadu zebrane w zbiorze hadisów Muhammada ibn al-Buchariego; C – odpowiedź na pytanie, czym jest kalifat; D – informacja na temat sekty ahmadijja. Na końcu znajduje się słownik pojęć. Publikacja Nabeela Qureshiego to bardzo interesująca pozycja. Ukazuje islam od strony mało znanej przeciętnemu mieszkańcowi Zachodu. Przedstawia religijne źródło ataków terrorystycznych w wykonaniu islamskich ekstremistów. Czyta się ją łatwo, dobrze i daje dużo do myślenia. Szczerze ją polecam wszystkim osobom zainteresowanym islamem oraz zawodowo zajmującym się rozpoznawaniem i zwalczaniem terroryzmu.

III
SPRAWOZDANIA

Witold Ostant

Sprawozdanie z ogólnopolskiej konferencji naukowej pt. „Oblicza współczesnego terroryzmu”

W dniach 23–24 kwietnia 2018 r. na terenie Akademii Sztuki Wojennej w Warszawie odbyła się pierwsza ogólnopolska konferencja naukowa pt.: „Oblicza współczesnego terroryzmu”. Organizatorami i współorganizatorami tego przedsięwzięcia były następujące podmioty: Wydział Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza w Poznaniu, Wydział Politologii Uniwersytetu Mikołaja Kopernika, Wydział Nauk Społecznych Uniwersytetu Gdańskiego, Wydział Bezpieczeństwa Narodowego Akademii Sztuki Wojennej, Wydział Cybernetyki Wojskowej Akademii Technicznej, Wydział Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej, Wydział Nauk o Bezpieczeństwie Akademii Wojsk Lądowych, Wydział Bezpieczeństwa Narodowego i Logistyki Wyższej Szkoły Oficerskiej Sił Powietrznych, Wydział Bezpieczeństwa Wewnętrznego Wyższej Szkoły Policji w Szczytnie, Wydział Nauk o Bezpieczeństwie Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, Wydział Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego, Instytut Stosunków Międzynarodowych Uniwersytetu Wrocławskiego, Instytut Politologii i Europeistyki Uniwersytetu Szczecińskiego, Instytut Zachodni w Poznaniu, Instytut Naukowy Bezpieczeństwa Wyższej Szkoły Bankowej w Chorzowie, Ośrodek Analiz Politologicznych UW, Zakład Nauk o Bezpieczeństwie Politechniki Rzeszowskiej, Ruch Wspólnot Obronnych oraz Naukowa Fundacja Prowadzenia Badań. Opiekę patronacką nad konferencją objęły renomowane czasopisma naukowe: „Przegląd Zachodni”, „Przegląd Strategiczny”, „Przegląd Bezpieczeństwa Wewnętrznego”, „Przegląd Politologiczny”, a także Polskie Towarzystwo Geopolityczne, Fundacja AT-System Group, Difin S.A. Wydawnictwo i Polskie Towarzystwo Nauk Politycznych. Natomiast patronat honorowy sprawowali: gen. bryg. dr Ryszard Parafianowicz – Rektor-Komendant Akademii Sztuki Wojennej, insp. dr Marek Fałdowski – Komendant-Rektor Wyższej Szkoły Policji w Szczytnie, płk dr hab. Bogdan Grenda – Dziekan Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej, prof. dr hab. Ryszard Zięba – Instytut Stosunków Międzynarodowych Uniwersytetu Warszawskiego, prof. dr hab. Zdzisław Winnicki – Dyrektor Instytutu Studiów Międzynarodowych Uniwersytetu Wrocławskiego, prof. dr hab. Janusz Ruszkowski – Dyrektor Instytutu Politologii i Europeistyki Uniwersytetu Szczecińskiego, prof. dr hab. Sławomir M. Mazur – Dziekan Wydziału Nauk o Bezpieczeństwie Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, dr hab. Urszula Chęcińska – Dziekan Wydziału Humanistycznego Uniwersytetu Szczecińskiego, dr hab. Andrzej Stelmach – Dziekan Wydziału Nauk Politycznych i Dziennikarstwa Uniwersytetu im. Adama Mickiewicza, dr hab. Stanisław Sulowski – Dziekan Wydziału Nauk Politycznych i Studiów Międzynarodowych Uniwersytetu Warszawskiego, dr hab. Stanisław Gędek – Dziekan Wydziału Zarządzania Politechniki Rzeszowskiej,

dr hab. Zbigniew Karpus – Dziekan Wydziału Politologii i Studiów Międzynarodowych Uniwersytetu Mikołaja Kopernika, dr hab. Tadeusz Dmochowski – Dziekan Wydziału Nauk Społecznych Uniwersytetu Gdańskiego, płk dr hab. Adam Radomyski – Dziekan Wydziału Bezpieczeństwa Narodowego i Logistyki Wyższej Szkoły Oficerskiej Sił Powietrznych, płk dr hab. Witalis Pellowski – Dziekan Wydziału Nauk o Bezpieczeństwie Akademii Wojsk Lądowych, kmdr dr hab. Jarosław Teska – Dziekan Wydziału Dowodzenia i Operacji Morskich Akademii Marynarki Wojennej, dr Krzysztof Koj – Dziekan Wydziału Zamiejscowego w Chorzowie Wyższej Szkoły Bankowej w Poznaniu oraz dr Justyna Schulz – Dyrektor Instytutu Zachodniego w Poznaniu.

Zasadniczym celem konferencji była pogłębiona refleksja nad terroryzmem, który w pierwszych dekadach XXI wieku stał się jednym z czołowych wyzwań i zagrożeń szeroko rozumianego bezpieczeństwa. Główne osie dyskursu były zogniskowane wokół następujących problemów: globalna wojna z terroryzmem (GWOT) – uwarunkowania, wymiary i perspektywy; terroryzm a problem państw upadłych i upadających; terroryzm a problem migracji we współczesnym świecie; terroryzm a państwo demokratyczne – wyzwania i zagrożenia; terroryzm a broń masowego rażenia.

Dzięki starannemu doborowi uczestników wydarzenie miało charakter unikatowy. Jego multidyscyplinarny charakter gwarantował wysoki poziom debaty oparty na uwarunkowaniach metodologicznych. W ramach prowadzonych rozważań w dyskursie uczestniczyli zarówno praktycy, jak i teoretycy – reprezentanci różnych dyscyplin naukowych z największych ośrodków naukowych i analitycznych w Polsce.

Oprócz walorów naukowych konferencji należy podkreślić także jej wymiar praktyczny, ponieważ zdiagnozowanie poziomu najważniejszych zagrożeń wynikających z nasilania się zjawisk o charakterze terrorystycznym pozostaje cenną wartością, która może być wykorzystana przez instytucje państwowe oraz służby dbające o bezpieczeństwo i zachowanie ładu publicznego.

Na konferencję składało się: sześć paneli naukowych, w ramach których wygłoszono trzydzieści referatów, oraz debata reporterska z udziałem m.in.: Witolda Repetowicza, Wiktora Batera, Rafała Stańczyka, Jana Wójcika i Dawida Wildsteina.

W pierwszym dniu spotkań zaprezentowano ćwiczenie taktyczno-operacyjne z wykorzystaniem śmigłowca, zorganizowane przez Biuro Operacji Antyterrorystycznych Komendy Głównej Policji. W drugim dniu przedstawiciele Służby Ochrony Państwa zorganizowali pokaz sprzętu wykorzystywanego w ramach realizowanych przez siebie zadań.

Konferencję w imieniu swoim i współorganizatorów uroczyście otworzył płk dr hab. Bogdan Grenda – Dziekan Wydziału Bezpieczeństwa Narodowego Akademii Sztuki Wojennej, a następnie wykład inauguracyjny wygłosił prof. zw. dr hab. Ryszard Zięba z Uniwersytetu Warszawskiego. Wystąpienie prof. R. Zięby było pogłębionym studium pozycjonującym terroryzm na tle innych wyzwań i zagrożeń bezpieczeństwa w drugiej dekadzie XXI wieku.

W panelu pierwszym na szczególną uwagę zasługiwały dwie prezentacje. Pierwsza z nich nosiła tytuł: *Cele społeczne terrorystów w państwach Unii Europejskiej*.

Jej autorem był prof. dr hab. Jarosław Gryz z Akademii Sztuki Wojennej. Druga – *Anty-Terror System* – była dynamiczną demonstracją działań w sytuacji zagrożenia ze strony tzw. samotnego strzelca. Tę prezentację opracowali dr Aleksandra Gasztold z Uniwersytetu Warszawskiego oraz Maciej Górski – współzałożyciele Fundacji AT-System Group. Profesor J. Gryz przedstawił cele operacyjne, taktyczne i strategiczne ugrupowań terrorystycznych działających w państwach Unii Europejskiej, których zadaniem jest podważanie fundamentalnych mechanizmów współpracy i organizacji współczesnych społeczeństw demokratyczno-liberalnych. Zespół Fundacji AT-System Group natomiast zobrazował optymalny model zachowania w sytuacji zagrożenia ze strony „samotnego strzelca" (najczęściej stosowana metoda dokonywania zamachów terrorystycznych w państwach Europy Zachodniej i w USA).

W panelu drugim – ze względu na szczególną aktualność – zwłaszcza dwa zagadnienia były wyjątkowo istotne. Pierwsze – to zapewnianie bezpieczeństwa w ruchu lotniczym, co w niezwykle trafny i kompleksowy sposób przedstawił płk rez. dr hab. Adam Radomyski z Wyższej Szkoły Oficerskiej Sił Powietrznych w Dęblinie (referat pt. *Współczesne aspekty przeciwdziałania terroryzmowi powietrznemu*), drugie natomiast – to problem uchodźstwa i jego potencjalnych skutków w kontekście zagrożenia terrorystycznego. W ramach drugiego zagadnienia na podkreślenie zasługiwały dwa referaty: *Polityka antyterrorystyczna i uchodźcza jako wyzwanie Unii Europejskiej w XXI w*. – dr hab. Izabeli Oleksiewicz z Politechniki Rzeszowskiej oraz *Czy migrant to terrorysta? Rewizja rozwiązań migracyjnych i uchodźczych*: *ONZ 2018* – dr Joanny Dobrowolskiej-Polak z Instytutu Zachodniego w Poznaniu.

Pierwszy dzień konferencji kończyła debata reporterska, która, podobnie jak wiele referatów wygłoszonych wcześniej, wzbudziła ożywioną dyskusję. Prowadzili ją doświadczeni dziennikarze – praktycy: prof. dr hab. Piotr Grochmalski – Dyrektor Instytutu Studiów Strategicznych Wydziału Bezpieczeństwa Narodowego ASzWoj oraz Witold Repetowicz.

Drugi dzień spotkań rozpoczął się dwoma panelami prowadzonymi równolegle. W ich trakcie wygłoszono kolejnych dziesięć referatów, spośród których, z uwagi na ciekawe i nowatorskie spojrzenia, na wyróżnienie zasługują: *Aktywność Państwa Islamskiego podczas konfliktu w Syrii* – dr. hab. Mariana Żubera z Akademii Wojsk Lądowych, *Wykorzystanie internetu przez terrorystów islamskich* – płk. dr. hab. Piotra Deli z Akademii Sztuki Wojennej oraz *Rozpoznanie osobowe w kontekście zagrożeń terrorystycznych*. *Grupy ryzyka* – podinsp. Przemysława Wrzoska i podinsp. Mariusza Kupniewskiego z Wyższej Szkoły Policji w Szczytnie. Uwzględniając trzy tak odległe od siebie zagadnienia dotyczące jednego problemu zasadniczego, należy podkreślić, że w ramach dyskusji zwrócono uwagę na zasadność tworzenia interdyscyplinarnych zespołów do zwalczania terroryzmu i potrzebę pogłębionej refleksji nad tym zjawiskiem w kontekście opracowywania strategicznych dokumentów dotyczących bezpieczeństwa.

Dwa kolejne panele poświęcono głównie problemom stojącym przed RP, jeśli chodzi o zwalczanie terroryzmu w ujęciu wewnętrznym i zewnętrznym oraz w aspekcie bilateralnym i multilateralnym. Analizując konteksty poszczególnych ujęć

tematów z uwzględnieniem najważniejszych zagadnień przedmiotowych, trzeba podkreślić wagę wystąpienia gen. dyw. (rez.) pil. dr. Anatola Czabana z Uniwersytetu im. Adama Mickiewicza pt. *Terroryzm w strategiach bezpieczeństwa państw i organizacji międzynarodowych*. *Współczesne wyzwania*, prezentacji dr. Macieja Magiery z Uniwersytetu im. Adama Mickiewicza pt. *Kultura bezpieczeństwa społeczeństwa polskiego z perspektywy współczesnych zamachów terrorystycznych w Europie* oraz referatu dr. Remigiusza Rosickiego z Uniwersytetu im. Adama Mickiewicza pt. *Bezpieczeństwo antyterrorystyczne na przykładzie szczególnych uprawnień polskich służb specjalnych w zakresie inwigilacji cudzoziemców*.

Kompleksowe zarysowanie problemów przez wyżej wymienionych naukowców uświadomiło uczestnikom konferencji, jak wiele jeszcze jest deficytów w zakresie zwalczania terroryzmu w Polsce oraz to, że trzeba włożyć dużo wysiłku w udoskonalenie polskiego systemu antyterrorystycznego, ukierunkowanego nie tylko na zwalczanie tego groźnego zjawiska, lecz także na szeroko rozumianą prewencję, której najskuteczniejszym i najbardziej efektywnym narzędziem jest edukacja dla bezpieczeństwa.

W podsumowaniu należy podkreślić, że pierwsza ogólnopolska konferencja naukowa pt. „Oblicza współczesnego terroryzmu" była pod względem merytorycznym i organizacyjnym dużym wydarzeniem w naszym kraju w 2018 r. Dzięki prezentacji wysoko specjalistycznej wiedzy ma ona szanse stać się elementem wpływającym na zwiększenie skuteczności działań administracji państwowej w zakresie zwalczania terroryzmu i przeciwdziałania temu zjawisku. Niewątpliwy sukces tego przedsięwzięcia nie byłby możliwy bez wsparcia i zaangażowania wielu osób, które pracowały na jego jak najlepszy wydźwięk w wymiarze zarówno merytorycznym, jak i organizacyjnym. W związku z tym w imieniu organizatorów i współorganizatorów konferencji szczególne podziękowania należy skierować do: dr. Cypriana Kozery – Akademia Sztuki Wojennej, dr. Piotra Lewandowskiego – Akademia Sztuki Wojennej, dr. Przemysława Gasztolda – Akademia Sztuki Wojennej, ppłk. dr. Grzegorza Motrycza – Akademia Sztuki Wojennej, dr Anny Mróz-Jagiełły – Akademia Sztuki Wojennej, Eweliny Czerwińskej – Akademia Sztuki Wojennej, Grzegorza Woźnego – Akademia Sztuki Wojennej, Pauliny Krawczyk – Akademia Sztuki Wojennej, Emilii Solarz – Akademia Sztuki Wojennej, Jowity Brudnickiej – Akademia Sztuki Wojennej, Jagody Gawliczek – Akademia Sztuki Wojennej, dr Moniki Lewińskiej – rzecznik prasowej Akademii Sztuki Wojennej, Moniki Dzięciołowskiej – Akademia Sztuki Wojennej, dr Natalii Jackowskiej – Instytut Zachodni („Przegląd Zachodni"), Anny Przyborowskiej – Agencja Bezpieczeństwa Wewnętrznego („Przegląd Bezpieczeństwa Wewnętrznego"), dr hab. Magdaleny Karg-Musiał – Uniwersytet Adama Mickiewicza („Przegląd Politologiczny") oraz prof. zw. dr. hab. Sebastiana Wojciechowskiego – Uniwersytet Adama Mickiewicza („Przegląd Strategiczny").

IV
ARTICLES AND DISSERTATIONS

Waldemar Walczak

Corruption as a net of influences, links and connections

Introduction

The topic of corruption practices fits into issues widely publicised and used by the media with the intensive discussions or disputes of political nature in public spaces. There are superficial and curt comments of emotional nature while it is clearly noticeable that there is lack of in-depth and substantial knowledge as well as an even-handed analysis of the phenomenon. In view of how complex and multifaceted problem it is nowadays, corruption becomes more and more a subject of numerous case studies. This need for wider inquiring and scientific exploration is rational and justified by its cognitive and utilitarian qualities, since the topic stays within the interests of special services. Their legal tasks are recognition, prevention as well as fighting corruption in public and economic life.

The aim of deliberations and analysis is to present the essence of corruption perceived in organizational and legal aspects of social and economic environment, which influence to the greatest possible extent the common management methods and decision making processes. As the preliminary remark it has been explained how the corruption notion should be understood and main corruption mechanisms have been characterised. Further on corruption as an element of management system has been described. Risks to the economic interests of a state have also been raised as well as violations of principles of the rule of law and social justice. An important argument for such broad approach to the problem is communiqué on the website of the Central Anti-Corruption Bureau, which clarifies in legible and clear way risks connected to the described phenomenon.

"Corruption threatens the rule of law, democracy and human rights, undermines good governance, fairness and social justice, distorts competition, hinders economic development and endangers the stability of democratic institutions and the moral foundations of society" (Criminal Law Convention on Corruption ratified by the Republic of Poland on 27 January 1998 in Strasbourg).[1]

Definitions

The starting point of further considerations shall be an explanation of the term corruption, which is essential and absolutely necessary because of diversity and ambiguity of definitions[2] as well as through perspectives of the phenomenon

[1] Public Information Bulletin of the CBA, http://bip.cba.gov.pl/bip/nabor-do-sluzby/profile-kandydatow/ekonomisci/14,Ekonomisci.html [access: 10 I 2018].

[2] A. Kubiak, *Działania antykorupcyjne – wybrane przykłady*, „Acta Universitatis Lodziensis

described.[3] It should be pointed out that the information showing the way corruption is understood is fundamental[4] because it determines interpretation of a certain notion and, in consequence, sets orientations for further analytical actions and scientific research. Having the above in mind, corruption will be perceived in broad terms as **an abuse of power, influences, professional position for one's individual interests and goals**.[5] It means that the phenomenon will cover both corruption criminal offences and also other forms of the so called legal corruption, which is not sanctioned in the penal code.

In the proposed definition one should pay attention that it uses the words "an abuse of power" intentionally. From the legal perspective it is fundamentally different from "misuse of power", which can be treated as misconduct in relation to a particular group of people, as provided for in Article 231 of the penal code. To present substantive arguments for the validity of assumptions, it is worth referring to one of the official governmental documents, i.e. The Anti-Corruption Governmental Program for the period 2014–2019 (Rządowy Program Przeciwdziałania Korupcji na lata 2014–2019) approved by the Council of Ministers. In the introductory part of the document there is the following passage:

> Legal definition of corruption is contained in Article 1 paragraph 3a of the Act of 9 June 2006 on the Central Anti-Corruption Bureau (Journal of Laws 2012, item 621, as amended), and the Program refers to such definition for the main part. Nevertheless, one should also not forget about other non-punishable forms of corruption like conflict of interest, nepotism and favouritism which are a problem also for public life. That is the reason why this document refers also to these kinds of corruption phenomenon understood in broad terms.[6]

Folia Oeconomica" 2013, no. 288, pp. 45–46; K. Nowakowski, *Korupcja a instytucje w gospodarce*, „Ekonomia i Prawo" 2006, no. 1, pp. 140–148; A. Stachowicz-Stanuch, A. Sworowska, *Definiowanie korupcji w kontekście różnic kulturowych*, „Organizacja i Zarządzanie" 2012, no. 1, pp. 97–116.

[3] K. Dzietczyk, *Zjawisko korupcji jako element życia społecznego*, „Seminare. Poszukiwania naukowe" 2016, no. 3, pp. 111–121; A.Z. Kamiński, *Korupcja jako symbol instytucjonalnej niewydolności państwa i zagrożenie dla rozwoju polityczno-gospodarczego Polski*, „Zeszyty Centrum im. Adama Smitha" 1997, no. 29, pp. 3–32; K. Nowakowski, *Korupcja jako problem teoretyczny i społeczno-ekonomiczny*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 1996, no. 2, pp. 77–94; J. Svensson, *Osiem pytań na temat korupcji*, „Gospodarka Narodowa" 2006, no. 9, pp. 77–106.

[4] R. Maćkowska, *Informacja w przestrzeni publicznej a zjawisko korupcji i jego postrzeganie*, in *Public relations w perspektywie naukowej*, A. Adamus-Muszyński (ed.), Katowice 2016, pp. 116–124.

[5] The parts written in a bold print come from the author.

[6] The Anti-Corruption Governmental Program for the period 2014–2019 (*Rządowy Program Przeciwdziałania Korupcji na lata 2014–2019)*, adopted by the resolution no. 37 of the Council of Ministers of 1 April 2014, Polish Monitor Polish official journal, item 299, Warszawa, 28 April 2014, source: https://cba.gov.pl/pl/publikacje/strategia-antykorpcyjna/3409,Rzadowy-Program-Przeciwdzialania-Korupcji.html [access: 10 I 2018].

A careful examination of the cited interpretation by the Council of Ministers regarding existing forms of corruption, shall unequivocally confirm the accuracy of the concept of the multifaceted approach to the described phenomenon adopted in this article. Furthermore, it gives legal bases for using adequate terminology while describing certain activities, decisions and patterns of behaviour of some concrete persons.

According to the Chief of CBA (...) *corruption is a multidimensional phenomenon analyzed and diagnosed in the aspects most important for a country, i.e. social, ethical, legal*.[7] However, one could argue with the opinion that (...) *corruption criminality violates basic rules of the country*[8]*,* because all categories of corruption patterns pose a threat to the economic interests of the country, sense of security among nationals, and blatantly devastate the rules of law and social justice. It seems that a direct reference to Article 2 of the Constitution of Poland would be justified here, which states that *The Republic of Poland is a democratic country based on the rule of law making rules of social justice real*.[9]

Agata Miętek, while analyzing this note, notices that the last part of that sentence pointing out the need of making rules of social justice real by the country is a subject of much smaller interest than the idea of a country based on the rule of law.[10] It is a very relevant opinion, that one should agree with.

Corruption fostering mechanisms

While describing main areas of threats from corruption from the perspective of the Supreme Audit Office (NIK), Alina Hussein points out the way services are commissioned by public entities to private ones and the area building investments are localized.[11] Using experts' services and consultancy services is described as follows:

(…) outsourcing takes place often without needs analysis (which means unnecessary services are ordered), without following the rules of public procurement/contracts and competition, without preserving required transparency of actions. Remuneration of outside bodies is overstated, contract conditions are unilaterally beneficial to private contractors and not to public institutions.[12]

[7] *Mapa korupcji. Zwalczanie przestępczości korupcyjnej w Polsce w 2016 r*., Central Anti-Corruption Bureau, Warszawa 2017, p. 5.

[8] Ibidem, p. 5.

[9] The Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended).

[10] A. Miętek, *Zasada demokratycznego państwa prawnego w orzecznictwie Trybunału Konstytucyjnego*, „Dialogi Polityczne III RP" 2009, no. 11, p. 76.

[11] A. Hussein, *Obszary zagrożenia korupcją – przegląd badań NIK opublikowanych w 2016 roku*, „Kontrola Państwowa" 2017, no. 5, p. 51.

[12] Ibidem, p. 51.

What is important in the above cited paper is that there are multi-million sums of money paid from contracts revealed in the course of checks (inter alia 15 million Polish zloty on contracts with employment agencies in 4 courts from the territory of the Warsaw Court of Appeal, consultancy and expert services contracts between 2012 and 2014 by the 4 PKP group companies for the amount of 171 million Polish zloty, and so on), and with regard to the described occurence the following term is used: (...) *irregularities having qualities of corruption mechanisms*.[13] It is particularly telling and symptomatic, especially in view of the lack of any mention of liability for decisions made, that resulted in appearance of large sums of money in the accounts of chosen beneficiaries.

For further considerations it is necessary to discuss chosen terms and to make an attempt to present the phenomenon of corruption in systemic frames. In the first place it is necessary to explain what corruption mechanisms are. In the nomenclature applied by the Supreme Audit Office corruption mechanisms mean *irregularities in functioning of public institutions, which cause or enhance the risk of corruption*.[14] In other words it can be said that these are factors and conditions which favour the occurrence of corruptive practices. NIK points out 4 most important premises: (...) *discretion of the proceeding, conflict of interests, lack of required transparency of the proceeding, lack or weaknesses of the control*.[15] It is worth mentioning that the conflict of interests has been mentioned in the Governmental Program of Counteracting Corruption for 2014–2019 in a **double sense**, i.e. as a non–punishable form of corruption (*one cannot forget about non-punishable forms of corruption, like conflict of interests*[16]), and as one of recognized corruption fostering mechanisms.[17] According to NIK conflict of interests *is a situation when public official is involved in conflicting private businesses*.[18] In this governmental document there is a much broader description:

> We can speak about this conflict when a public official resolves in a certain sphere of public matters or takes part in preparations for such resolve does have or may have personal interest in the way the case is resolved. The conflict occurs not only when a public official acts in his/her personal interests but also when there is even a hypothetical possibility that the interest would outweigh the concern over public interest.[19]

A comparative analysis of the cited interpretations tends to notice certain differences having a significant influence on the way the essence of the problem

[13] Ibidem, p. 52.

[14] A. Hussein, *Mechanizmy korupcjogenne – cztery grzechy główne władz publicznych*, „Przegląd Antykorupcyjny" 2011, no. 1, p. 43.

[15] Ibidem, p. 44.

[16] *The Governmental Program of Counteracting Corruption for 2014–2019*, p. 7.

[17] Ibidem, p. 19.

[18] A. Hussein, *Mechanizmy korupcjogenne* ..., p. 44.

[19] *The Governmental Program of Counteracting Corruption for 2014–2019*, www.antykorupcja.gov.pl/ak/prawo/polskie-przeoisy-1/11409/Rządowy-Program-Przeciwdziałania-Koruocji-na-lata-2014–2019.html, p. 19.

is understood. Well, in one of the opinions the term "entangled" has been used in the aspect of already existing circumstances, and the second one emphasises the likelihood itself, i.e. a theoretical possibility of such a situation in the process of decision-making. These remarks indicate how different the perception of certain things is, and also how ambiguous the term conflict of interests is. Unfortunately, in Polish legislation there is no legal definition of the term, which is crucial for these deliberations. In view of the above three questions arise:

- Was a situation of conflict of interests rightly mentioned explicitly in the governmental document as a non-punishable form of corruption and a particularly dangerous corruption-fostering mechanism at the same time?
- Is it logical and eligible to narrow a conflict of interests down only to situations when decision-making by public officials is involved?
- What are other factors and circumstances that foster corruptive practices?

The answer to the first question is yes, which means that conflict of interests situation is in fact one of the forms of the so called legal corruption.

As far as the second question is concerned one should admit that in each and every case of using power and decision-making competences connected to a particular position in a certain organization, a real conflict of interests can occur. And hence, the term should not be limited in any way or assigned to public officials activities only, because conflict of interests can take place not only in other public institutions (courts, prosecutor's offices, hospitals, high schools etc.) or in companies with capital engagement of state legal entities, but also – with no exceptions – in all the other categories of private entities. Rather common are events, processes and decisions when not only public interest, common good but parties' interests, personal benefits of a certain profession, benefits of private business, foundation, company, group of colleagues, mates, or acquaintances etc. are taken into consideration.

According to the assessment of the Polish government the other **corruption fostering mechanisms** are:

- Irregularities in law-making process: violating existing legal procedures, and omitting necessary procedure of commenting or interdepartmental arrangements in particular; amendments to already agreed projects; adopting implementing acts with a considerable delay, loopholes and ambiguity causing discretionary interpretation of provisions, inconsistent revision of laws, adopting more and more legal acts,
- Cumulating competence: too much decision-making authority and departure from the rule of action allocation regarding one case among different officials,
- Disregard for documentation and reporting: accepting insufficient documentation, without all evidences or attachments required by the procedure, resignation from required reporting, and decision-making without justification which makes control of decision-making procedures more difficult,
- Lack of personal responsibility for decisions already taken.[20]

[20] *The Governmental Program of Counteracting Corruption for 2014–2019* ..., pp. 19–20.

It should be added that from the perspective of management practice it is significant that the authority accumulation element as well as combining positions by one person is not dominant sufficiently. This is really a very important factor, whose role and significance cannot be depreciated.

Corruption as element of management system

For the correct understanding of **areas and forms of corruption** in the organizational reality, it is helpful to highlight some basic topics regarding management paradigms used in practice, which, unfortunately, differ from ideas popularised in scientific theories.

1. Corruption comes down to taking advantage of the opportunities which arise from the authority held and granted decision powers to ensure personal as well as material benefits. As a result it becomes an integral element of management processes. According to Article 115§ 4 of the penal code it is about (...) *material or personal benefit both for himself/herself and for someone else*.[21] In the opinion of the Central Anti-Corruption Bureau material benefits are different goods meeting certain needs, the worth of which can be expressed in money. Apart from cash it can be inter alia: *attractive objects, excursions, preferential loans, debt write-off or public procurement*.[22]In practice there are numerous situations that personal benefit improving situation of the person is directly linked to a material benefit, for example promotion in a work place or employment in a particular position, attractive training granted for free, apprenticeship, fellowship overseas and so on.
2. Management of organizations is to a large extent based on managing property and finances of the third party, which makes perception of such terms as thriftiness, economy, purposefulness and rationality of spending to be completely different than it is in the situation of spending one's own money. An example: people represented in institutions from public finance sector taking decisions concerning taxpayers' money and not their own personal funds. Co-op authorities run the community property of its members and not their own, and as far as the finances are concerned they dispose the residents' payments. Banks and other financial institutions, like Polish SKOKs manage the assets entrusted to them by citizens, CEOs of the state-owned companies run state-owned property, authorities of the municipal companies manage municipal property, the authorities of the private companies manage their property and their clients money, authorities of foundations spend money from donors, sponsors, from state subsidies, 1% of income tax, Norwegian funds, EU funds and from public fund-raisers, and it is not their private money.
3. **Personnel and financial decisions** (both taken collectively and one-man decisions) are of **arbitrary, discretionary and biased nature**. In most cases

[21] The Act of 6 June 1997, Penal Code (Journal of Laws 1997, no. 88, item 553 as amended).

[22] *Mapa korupcji. Zwalczanie przestępczości korupcyjnej w Polsce w 2016 r.*, Warszawa 2017, p. 23.

the only justification required is confirmation that the decision was taken by the competent authority, competent person within the powers attributed to them as well as on the basis of and in accordance with national law provisions such substantive explanation is absolutely sufficient. If the law imposes an obligation of specific procedures, for example the so called open and competitive procedure, it is always possible to fix and prepare proper action and members of the commission in such a way that „the choice made" will be in line with previous informal arrangements and planned scenarios accepted in a narrow circle of the most trusted confidants.

4. Corruption contributes significantly to the strengthening of power and expanding sphere of influence by creating and widening nets of personal links and dependencies. That is the reason why personnel politics plays such a crucial role from the perspective of efficient effective, right and secure performance of particular interests.
5. Corruption is a particularly precious value and the main factor integrating bonds and relations between people, who are extremely successful thanks to it, make careers, get above-average material benefits as well as personal benefits.
6. In each organization (from public finance sector or private sector) it is always possible to create and justify the need for employing particular persons, signing certain contracts, cooperation in other legal forms and spending some money on the established business venture in order to achieve a certain goal. Then, the scenarios of further activities would be submitted to this idea. They will *de facto* legitimise, from the legal perspective, legitimacy of the material benefits obtained by the favoured group of chosen and privileged beneficiaries.
7. Integrity, justice, compliance with the law, equal treatment, constitutional principle of equality before the law: *everyone is equal before the law. Everyone has the right to be equally treated by the public authorities* (article 32 § 1)[23], moral norms, ethical principles, decency and responsibility have no significance at all from the corruption point of view. These values are replaced by arrogance, being self-interested, bias, clientelism, discrimination, accessory, favouritism which are subordinated to one idea: striving for maximum private benefits and securing one's own interests.
8. From the management perspective taking power and control over assets and finances of a certain organization, i.e. placing the most trusted people on the highest positions with a wide range of decision-making competences are of crucial importance. While analyzing personnel politics one cannot narrow the whole picture only to profits because even more valuable fact is what kind of budget the entity is working with and what kind of **financial flows** to other entities, companies can be created. It is about a **real influence on**

[23] Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483, as amended).

material benefits gained by other institutions and people. The **contacts and ties** (political, business, professional, family) of the particular position holder as well as **the accumulation of posts**, previously taken positions, other areas of interest and activity are equally crucial. These topics are of significance for analytical activities, which enable proper understanding of the events and processes studied.[24]

Structuring some chosen questions of terminology shown in the picture 1 is important and necessary, because – as Łukasz Goczek points out: *corruption is one of the most controversial topics in public debate, although its mechanism is also one of the least understandable.*[25]

Basic factors creating plane for corrupt practices are **legal provisions**, **accumulation of power** and **a sense of impunity** for actions taken. Jerzy Matusiak takes the view that the source of corruption is law, adding at the same time that (...) *the fight with corruption sails under false colours.*[26] The author adds that (...)*the basis for criminal responsibility are legal acts and: nullum crimen sine lege*.[27] So, if a particular pattern of conduct, a particular act is not directly specified in a penal code, such behaviour cannot be treated as a criminal offence. From the management practice point of view accumulation of posts and performing many tasks by one person plays a very important role because it leads to accumulation of decision-making powers, and thus it allows direct influence on the course of actions, their assessment and control in a few organizations simultaneously. Maciej Gurtowski claims that (...) *corruption possibilities can be linked to a control over sources of uncertainty*.[28] It is very important, particularly in view of the real influence on settlements made. The more posts one combines, the more one broadens and strengthens the authority acquired, which in consequence creates multiple influences and possibilities to run errands, do some businesses, formalities, proceedings. Because the accumulation of positions involves several different institutions (organizations, companies) there comes a multidimensional and extensive network of contacts, links, dependencies, relationships of both formal and business nature (institutional, overt) and of informal, private nature (covert). This configuration of **ties, interdependencies** and the architecture of **accumulated power and influences** are the biggest driving force in terms of real possibilities to create corrupt practices. In this respect, it is important to

[24] W. Walczak, *Działania analityczno-informacyjne identyfikujące mechanizmy korupcyjne w procesach zarządzania***,** „Przegląd Bezpieczeństwa Wewnętrznego" 2017, no. 16**,** pp. 55–72.

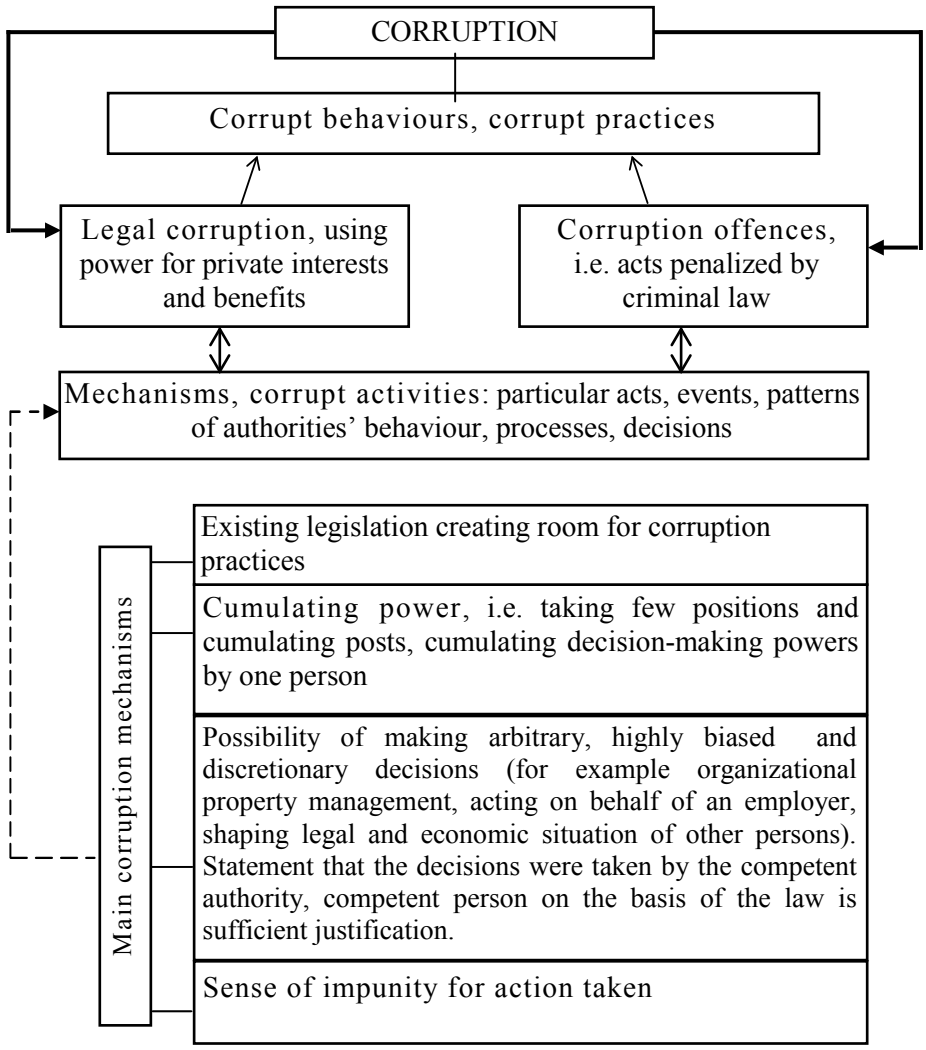
[25] Ł. Goczek, *Przyczyny korupcji i skuteczność strategii antykorupcyjnych*, „Gospodarka Narodowa" 2007, no. 4, p. 33.

[26] J. Matusiak, *Peryferyjny kapitalizm zależny*, e-book, 2006, pp. 123–124.

[27] Ibidem, p. 124.

[28] M. Gurtowski, *Niepewność, korupcja i granice podmiotowości w medykalizującym się świecie z perspektywy teorii władzy Michela Croziera i Erharda Friedberga*, „Pogranicze. Polish Borderlands Studies" 2016, no. 2, vol. 4, p. 200.

note that the sense of impunity and immunity[29] is a key element which determines the real effectiveness of ongoing projects.



Pic. 1. Broad understanding of corruption in practical organization management.

Source: private study.

Main corruption mechanisms mentioned in the picture 1 do not exhaust the list of factors that can lead to corruption, nor do they contest the significance of the elements mentioned earlier in the governmental anti-corruption program.

[29] P. Falenta, *Przestępstwo korupcji – uwarunkowania karnoprawne i społeczne*, „Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu" 2016, no. 1, p. 157.

Division of corruption practices into two separate categories: legal corruption and corruption offences, is clearly derived from applied criterion, i.e. punishability of specific conduct in accordance with the law in Poland. Unfortunately some common corruption practices are subject to differing interpretations because of their complexity and ambiguity. They can also be assessed depending on who expresses value judgements and what is the reference point. Momentous and sensitive problem concerns perception and legal categorisation of certain behaviours, concrete decisions, facts and processes in the context of possible irregularities, pathologies[30] and whether they can or should be described as criminal offences.[31]

Anna Pluskota gives some interesting thoughts on the topic: (...) *every time when there is something about corruption coming from transgressing one's powers, interpretation of such behaviour can differ depending on cultural background of the society. Mostly, it is citizens who with the help of legal provisions in force recognize a particular activity as corruption.*[32] It is very hard to agree with such a way of thinking that it is up to citizens to make a biding assessment of an activity if it is corruption coming from transgressing one's powers.

Waldemar Wojtasik is of the opinion that political corruption violates basic principles of democratic system, free market and civil society. The general perception is that it is a (...) *pathology of modern economic and political relations.*[33] Does it mean that each and every symptom of political corruption can be interpreted only in this way? Well, definitely not. Social perception of a particular phenomenon by services, prosecutors (i.e. law enforcement) can differ from legal and criminal approach as well as from the final and binding **interpretation by courts**. So, only the competences of judiciary of the Republic of Poland shall be decisive in terms of assigning criminal responsibility for any concrete corruption activities (proceeding, trials, decisions). It happens that such activities like extreme abuse of authority and unfair, highly harmful practices are recognized by society, however they are treated by law enforcement only as forms of unethical conduct authorized under law. Nevertheless, it does not change the fact that each form of corruption[34] (legal and punishable) is a fundamental **breach of social and economic justice** and poses

[30] K. Dendura, *Korupcja jako patologia kapitału społecznego*, in: *Zarządzanie bezpieczeństwem w sektorze publicznym i biznesie*, T. Białas, M. Grzybowski, J. Tomaszewski (ed.), Wyższa Szkoła Administracji i Biznesu, Gdynia 2009, pp. 31–38.

[31] K. Laskowska, *Rola korupcji w działalności zorganizowanych grup przestępczych*, in: *Oblicza współczesnej przestępczości zorganizowanej*, K. Laskowska (ed.), Temida 2, Białystok 2014, pp. 143–154.

[32] A. Pluskota, *Czy globalizacja wspiera korupcję?*, „Ekonomia Międzynarodowa" 2017, no. 17, p. 40.

[33] W. Wojtasik, *Społeczne postrzeganie korupcji politycznej w perspektywie oceny uczciwości władz politycznych*, „Political Preferences" 2017, no. 17, p. 120.

[34] A. Stachowicz-Stanuch, A. Sworowska, *Oblicza korupcji: formy i typy zachowań*, „Organizacja i Zarządzanie" 2012, no. 1, pp. 117–133.

serious threat to moral foundations of the Polish society.[35] Propensity to some acts[36] cannot invalidate or question this.

Boundaries between corruption criminality and legal corruption have become more and more blurry. Punishable forms of corruption in general understanding are associated with such activities as promising, proposing and giving an undue advantage. Marcin Brol states that (...) *the more difficult detection and proving the fact of giving or taking bribes the more frequently corruption exchange will take place*.[37] One of the reports of the Internal Security Agency (ABW) of 2004 rightly emphasises that modern types of corruption take the form of secret and veiled actions. The way and form of giving benefits changes – (...) *more frequently it is of non-cash nature.*[38] Bribery scheme is often attributed to non-material services (for example legal advisory, business consulting, expertise), value of which is hard to assess and measure unequivocally. According to ABW (...) *in many cases astronomical fees amounting to tens of thousands Polish zloty, paid for example for one-page legal opinions or expertise (often fictional or of poor value) are nothing else than hidden form of bribery.*[39] There is also additional problem in the fact that one cannot speak about undue compensations in the context of passing money, if there is a proper legal basis for it because of a signed contract or other assignments related to advertising, marketing, sponsoring, public relations and appointment to the supervisory board or board of directors, delegation of appointed agent or plenipotentiary of the board of directors function.

The real corruption on a big scale is that the transfer of benefits has its legal grounds in legal economic situations and financial operations. Then, it is impossible to charge somebody with undue profits. What is more, material benefits distribution can be postponed in time for appearances' sake and security reasons as well as it can be delivered to a designated trusted recipient, intermediary (intermediaries) so as not to arouse any suspicion. Subsequently, further businesses and capital transfers are created, frequently involving other people and entities (companies, foundations, associations). The more complex structure of those processes the more difficult it is to understand real intentions and goals of some established financial operations because they seem to be apparently normal events associated with pursuit of economic activities. Currently corruption becomes a synonym of well-thought-out long-term **investment strategy**, not only what is achievable right now that counts but also what can be achieved in the future thanks to certain activities.

---

[35] K. Kietliński, *Korupcja jako naruszenie sprawiedliwości społeczno-gospodarczej oraz zagrożenie dla moralnych podstaw społeczeństwa*, „Problemy Zarządzania" 2010, no. 2, pp. 139–147.

[36] P. Chodak, *Zgoda społeczeństwa na niewielkie przestępstwa korupcyjne*, „Journal of Modern Science" 2013, no. 3, pp. 193–209.

[37] M. Brol, *Ekonomiczne i instytucjonalne metody przeciwdziałania korupcji*, „Współczesne Problemy Ekonomiczne" 2017, no. 2, p. 59.

[38] *Korupcja w Polsce – próba analizy zjawiska*, *Raport Agencji Bezpieczeństwa Wewnętrznego*, Warszawa 2004, p. 13, also accessible on: http://www.antykorupcja.gov.pl/download/4/5356/RaportAgencjiBezpieczenstwaWewnetrznegoKorupcjawPolsce-probaanalizyzjawiska.pdf.

[39] Ibidem, p. 14.

All this happens within a narrow circle of trusted people who are aware of what they are taking part in and what their role in it is, but also how tangible benefits they get. There is no question of demanding or expecting some undue benefits because returning the favours is not forced and volitional. At the same time, one can legally support a particular political party, election campaign of a particular politician, friendly media, friendly scientific association, private high school, cultural institutions, chosen NGO, foundation or think tank because they meet social objectives and nobody should be surprised that someone wants to be a donor, backer or sponsor of a certain event.

Unfortunately, the notions about modern forms and the real scale of corruption in Poland cannot be pictured from the 31-page-long publication Map of Corruption or from the 33 page study Information on the CBA activities in 2016.[40] Naturally, some general remarks can be found there like (...) *there were analyses of contracts for consultancy services, legal services, insurance services and security services by chosen state-owned companies in the years 2015–2016. The actions are carried out within the frame of coordinated control and presentation of final findings and results will be possible upon completion.*[41] 2015 and 2016 have passed and the public got no information on the results of the control. The knowledge is secret and not accessible for potentially interested citizens.

Similar situation is with corruptive practices. Society gets only fragmented media information on disclosed repercussions and effects of certain actions but the essence of corruptive mechanisms is a sequence of processes and the course of actions which were of original character. In order to know exhaustively the case one should get answers to questions, who was the initiator, originator, who assisted, who was engaged, with whom, what kind of dependencies and interpersonal links there were, who had a direct impact on the course of actions and decisions taken, on whose authority, in whose name, for whom worked, who offered immunity and so on. This, however, is a matter of exclusive esoteric knowledge, its depositaries being a close circle of insiders.

Dorota Karpiel claims that corruption is linked to organized crime. *Common interest of all those involved makes this phenomenon difficult to discover and even more difficult to prove. This truth is so common and confirming impunity that has undoubtedly influence on broadening zones of direct danger from it.*[42] ABW takes the same view, the circumstance that makes corruptive offences difficult to detect is the fact that individuals involved in this practice are not interested in disclosing it at all. The most frequently detected cases of bribery, trading in influence and the abuse of functions, (...) *occur solo very rarely, in most cases they are disclosed in connection*

[40] *Informacja o wynikach działalności Centralnego Biura Antykorupcyjnego w 2016*, Warszawa 2017, pp. 4–5.

[41] Ibidem.

[42] D. Karpiel, *Przestępczość zorganizowana*, „Internetowy Przegląd Prawniczy TBSP UJ" 2017, no. 7, p. 12.

to other economic cases.[43] Corruption in the practice of management does not come down to isolated incidents but takes a complex form of **organised actions in a systemic dimension**. It is its main hallmark and its most important attribute. It is a deliberate and intended **use of legal power** and influences to create and extend **nets of closed systems** overlapping a plane of financial streams to the chosen beneficiaries' accounts. In other words, the point is to reserve prominent positions, good job, lucrative contracts, orders, serious businesses, career paths, possibilities of promotion and development **only to those from a deal, with right connections, links**, and thanks to them they take privileged positions.

Elżbieta Durys is of the opinion that deals, connections, hooks resemble (...) *conspiratorial paranoia in the modern Polish theatre.*[44] The author has every right to her independent views, opinions and value judgements as well as to announce results of scientific studies in any chosen subject. Freedom of doing science is a constitutionally guaranteed right.[45] Taking the above under consideration it is worth answering the question whether a "deal" is only an invented and abstract existence noticed by followers of conspiracy theories. According to E. Durys it is present in films as: *"They" create a group taking care of their mutual interests*. (...) *Impunity is guaranteed by connections and links* (...).[46]

Analysing a public statement of one of the representatives of judiciary we come across a passage on personnel changes: (...) *I just do not fit into* ***the new system*** *which is being created right now.*[47] Cognitively, it is a very valuable sentence for scientific goals connected to the topic of this article. Firstly, the cited statement is considered, measured, true and authentic. It is an important argument confirming the fact that **a "deal" in judiciary exists**, and moreover it shows the present transformation of its structure. In a logical way it can be understood in the following way: created "deal" is subject to some modification, and hence personal changes. This is rational and substantive argumentation as well as correct usage of the word deal to describe the way an organised group functions.

Secondly, this information has not been made public incidentally but it was deliberate and intentional. It is not from illegal tapping nor is it of private nature. One should admit, that it correctly maps described organisational reality. Thirdly,

[43] *Korupcja w Polsce – próba analizy zjawiska*, ... p. 13.

[44] E. Durys, *Układy, znajomości, „haki". Paranoja spiskowa w polskim kinie współczesnym*, in: *Studia Etnologiczne i Antropologiczne*, vol. 16, M. Rauszer, G. Studnicki (ed.), Katowice 2016, pp. 44–54.

[45] According to Article 73 such right is granted to each and every citizen. *The freedom of artistic creation and scientific research as well as dissemination of the fruits thereof, the freedom to teach and to enjoy the products of culture, shall be ensured to everyone.* According to Article 54 § 1 *The freedom to express opinions, to acquire and to disseminate information shall be ensured to everyone.* Source: the Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483 as amended).

[46] E. Durys, *Układy, znajomości*, *„haki"*..., p. 50.

[47] Source: https://www.tvn24.pl/lodz,69/odwolany-prezes-lodzkiego-sadu-nie-pasuje-do-nowego-ukladu,807449.html [access: 7 II 2018].

the analysis of the cited wording does not refer to assessment of the validity of personnel decisions in judiciary by any means but its goal is to verify a thesis about the deal which was the subject of the present considerations.

Areas of corruptive behaviours, its manifestations and forms

If we want to identify correctly modern types of corruption which has its real confirmation in a day to day organisational reality, we should bear in mind that they are tightly linked to the following elements: governance (gaining power, maintenance of power, strengthening of power, expanding of power), applied methods of management, style of management, taking decisions, possible personal and material benefits. Maciej Ciesielski quite rightly believes that (...) *in modern forms of corruption it is about realisation of scenarios based on complex personal interdependences, which are not the same as criminal activity described in articles 228, 229 and 230 of the Penal Code.*[48] The author adds that more and more common forms of corruption are nepotism and clientelism, as well as (...) *relationships (links), usually of informal nature, which centre on the influence, whose effect is the achievement of particular objectives (personal, business purposes).*[49] The observations cited are extremely accurate and by any measure correct, although with one tiny restriction of semantic nature. Namely, these relationships and connections are not built (...) *around the influence*, but around concrete persons having influence, power and decision making competences.

Jerzy Matusiak presents opinions that develop the issue. *Nepotism, clientelism and jobs for the boys take care of cushy jobs, and even ministerial seats. It is society that pays for all those sinecures. They secretly subordinate state interest to private interests. In Poland political capitalism is a sanctioned substance of governing.*[50] It is hard not to agree with these beliefs because in a synthetic formula they resemble a description of methods and processes of management commonly present in organisational reality. Bearing in mind the consequences of such patterns of behaviour it should be assumed that the statement (...) *corruption undermines trust in law and state authorities, plus it violates citizens' sense of security, devastates basic moral values, destroys honesty and responsibility*[51] is true and reasonable. What is more, it poses a serious threat from the perspective of protecting economic interests of the state, because (...) *loss caused by corruption in economic trade only exceeds many times loss caused by ordinary criminality.*[52]

[48] M. Cielsielski, *Zjawiska korupcyjne jako podstawowa kategoria zagrożeń bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP– perspektywa Służby Kontrwywiadu Wojskowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, no. 13, p. 214.

[49] Ibidem, p. 213.

[50] J. Matusiak, *Peryferyjny kapitalizm zależny*, e-book, 2006, p. 123.

[51] Ibidem, p. 117.

[52] Ibidem.

Dirk Tanzler points out that (...) *corruption does not happen in the void but at the interface between public sector administration and private companies, wherever there are public funds*.[53] The above beliefs require a few words of comment to direct thinking to a correct identification of possible areas where corruption practices appear. Firstly, one cannot narrow the field of vision only to a chosen category of institutions financed from taxpayers' money, known as *administration,* because public finances sector embraces also among others public control bodies and law enforcement courts, tribunals, executive agencies, budget institutions, Social Security Office (ZUS), Agricultural Social Insurance Fund (KRUS), National Health Service (NFZ), public autonomous health care management units, public high schools, Polish Academy of Science (PAN) and its organizational units, state and local institutions of culture (article 9 of the Act on public finances).[54] Secondly, there are also other entities in the ordinary course of trade, like state-owned companies and their subsidiaries, companies with a capital share of local government authorities, housing corporations, societies and credit unions, sports federations, foundations, associations, private financial institutions, media concerns, listed companies, law firms, and so on, that trade with public sector organizations as well as with private sector.

So, corruptive practices can occur in all categories of organizations functioning in the economy[55], although they are perceived and interpreted differently depending on whether they are present in institutions supervised by the state or in private entities.[56] Nevertheless, it cannot be said that corruption in a broader meaning occurs only in public sector[57], although undoubtedly the most frequently detected forms of corruption refer to the described situations.

---

[53] D. Tanzler, *Korupcja jako metafora*, „Roczniki Nauk Społecznych" 2012, no. 4, p. 78.

[54] The Act of 27 August 2009 on public funds (Journal of Law 2009, no. 157, item 1240 as amended).

[55] J. Burzyński, T. Burzyński, *Ryzyko zachowań korupcyjnych w instytucjach państwowych na przykładzie Służby Celnej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2013, no. 2, pp. 217–229; A.E. Chodorowska, J.M. Stopińska, *Korupcja w ochronie zdrowia*, „Journal of Modern Science" 2012, no. 4, pp. 163–181; K. Nowakowski, *Zagrożenia etyczne i korupcyjne w mediach*, „Studia Medioznawcze" 2017, no. 2, pp. 128–140; J. Potulski, *Penalizacja korupcji w sporcie – uwagi krytyczne*, „Prokuratura i Prawo" 2012, no. 3, pp. 67–78; P. Szwajdler, *The legal aspects of corruption in sport*, „Journal of Education, Health and sport" 2016, no. 5, pp. 445–451; A. Turska-Kawa, M. Czaja (ed.), *Postawy wobec korupcji w samorządzie terytorialnym. Raport z badań w województwie śląskim*, Katowice 2015; L. Wilk, *Korupcja w reklamie farmaceutycznej*, „Prokuratura i Prawo" 2011, no. 10, pp. 21–36.

[56] J. Burzyński, T. Burzyński, *Ryzyko zachowań korupcyjnych w instytucjach państwowych na przykładzie Służby Celnej*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2013, no. 2, pp. 217–229; A.E. Chodorowska, J.M. Stopińska, *Korupcja w ochronie zdrowia*, „Journal of Modern Science" 2012, no. 4, pp. 163–181; K. Nowakowski, *Zagrożenia etyczne i korupcyjne w mediach*, „Studia Medioznawcze" 2017, no. 2, pp. 128–140; J. Potulski, *Penalizacja korupcji w sporcie – uwagi krytyczne*, „Prokuratura i Prawo" 2012, no. 3, pp. 67–78; P. Szwajdler, *The legal aspects of corruption in sport*, „Journal of Education, Health and sport" 2016, no. 5, pp. 445–451; A. Turska-Kawa, M. Czaja (ed.), *Postawy wobec korupcji w samorządzie terytorialnym. Raport z badań w województwie śląskim*, Katowice 2015; L. Wilk, *Korupcja w reklamie farmaceutycznej*, „Prokuratura i Prawo" 2011, no. 10, pp. 21–36.

[57] J. Bojarski, *Korupcja gospodarcza. Studium z dziedziny polityki kryminalnej*, Toruń 2015.

Another important issue that should be mentioned here is that public money passed to a concrete private entity under a prior contract (for example winning a tender, signing a lucrative multimillion contract, lucrative assignment) is usually distributed further by authorities of this company, and, at the same time, it gets to other organizations, contractors, suppliers, subcontractors, co-workers, and so on. Referring to further financial flows one cannot absolutely acknowledge that these are processes and decisions connected to spending public money. Similarly, it is not true that a foundation established by state-owned companies shall become the authorising entity as far as public means are concerned and spends taxpayers' money concluding commercial agreements with third parties. That is why speaking about a particular case one should adopt a more complex perspective without reducing thinking perception to noticing only single isolated economic events because the sequence of processes and links between them, as well as their dependences or organisational and legal conditions are equally important. To supplement the considerations one can only add that state-owned companies do not belong to public finances sector and private companies (entities) are not obliged to comply with the public procurement law[58], they can freely part with their assets and their authorities do not have to justify their decisions in front of the public.

Piotr Borowiec, while analysing the chosen aspects of huge corruption in the 3rd Republic of Poland, refers to privatisation of state assets, legislation processes, media activity, public procurement and corruption by employing. He also adds that such practices are used in (...) *all procedures connected with getting jobs or changing positions and, what should be stressed, it does not refer only to jobs in the budgetary area and well-paid positions*.[59] He also pays attention to usurpation of public institutions commenting that (...) *access was strictly limited to "the chosen" – unnecessarily competent and honest people*.[60] Insightful analysis of concrete events and processes going on in the economy lets us confirm that it is a pragmatic and right reasoning. The same reasonable statement is that corruption (...) *undermines the principle of equality of citizens before the law and equal access to public institutions*[61], and notorious corruption is (...) *the biggest threat to the state*.[62] Equally rational seems the following statement: (...) *wherever huge money is involved, there is also a risk of corruption, and the bigger amount of money the higher the risk is*.[63] Piotr Solarz adds that (...) *corruption will occur when a monopolistic decision is discretionary, without any risk of personal responsibility for results of the choice. Corruption is a monopoly plus discretion minus responsibility*.[64]

---

[58] The Act on public contracts of 29 January 2004; Journal of Laws 2017, item 1579 as amended.

[59] P. Borowiec, *Korupcja w III RP – obszary szczególnego występowania*, „Środkowoeuropejskie Studia Polityczne" 2007, no. 1, p. 196.

[60] Ibidem, p. 201.

[61] Ibidem, p. 191.

[62] M. Romański, *Znaczenie zjawiska korupcji dla bezpieczeństwa państw upadłych*, „Roczniki Ekonomii i Zarządzania" 2017, no. 1, vol. 9, p. 25.

[63] M. Chruściel, *Wojsko jako podatny grunt dla korupcji*, in: *Realizacja działań antykorupcyjnych w resorcie obrony narodowej*, R. Wykurz (ed.), Warszawa 2017, p. 7.

[64] P. Solarz, *Korupcja, klientelizm i kapitalizm polityczny jako podstawowe pojęcia w dyskursie*

To following issues are included within the functional areas of organisation management, where corruption usually occurs:

- Employment processes, i.e. getting jobs in institutions of public finance sectors, positions in supervisory boards and boards of state-owned companies and executive positions in those entities. The same phenomena occur in other organizations of private sector but there they are not perceived as pathologies but rather as family and environmental entrepreneurship.
- Contracting with outer companies, lucrative orders, contracts.
- Awarding of grants from public money, awarding concessions and permissions.
- Tenders and public procurement.
- Reprivatisation.
- Issuing of fictional invoices to prove non-existing economic events, VAT extortion.

Personnel policy as a key component of corruption

As mentioned earlier corruptive practices exist in each area of social and economic life in different form and scale, in all institutions of public finances sector, state-owned companies and other companies and organisations of private sector. Law frames for certain categories of organisations basically create ground for some particular behavioural commitments, as well as for their different assessment not only from legal and penal perspective but also in the context of social approach. It is a widespread feeling that in private business such phenomena as nepotism, favouritism, job for the boys and accessory are considered positive – treated as desired expression of resourcefulness.

Personnel policy in institutions under state supervision is one of the topics that attracts media attention and arouses numerous controversies because of ambiguity of opinions and assessment of the phenomenon. Commonly accepted are beliefs that in many cases it is not outstanding and above-average competences and extensive knowledge that decide about nominations, promotions to lucrative positions, but such factors as agreements and connections, relationships with high-profile contacts, i.e. powerful people are decisive. What is more, the subject of **access to the so called lucrative and highly-paid positions** and functions for Polish citizens is also very important. In this matter legal provisions describing formal and legal procedures of employment in a particular category of organisation play the key role. For example, procedures of choosing members of management boards and supervisory boards in state-owned companies and companies that belong to regional and local authorities do not require an open and competitive competition procedure. At least, it would make an illusory impression that the interested people have proper knowledge, competences and qualifications to apply for the position. The same situation applies to management positions and other jobs in state

o jawności życia publicznego w Polsce, „Kontrola Państwowa" 2007, no. 3, p. 118.

companies, as well as many other positions in the public administration and the local administration who are appointed in the legal frame of appointment for the position. It is sufficient to give a legal ground for a personnel decision and statement that the decisions are taken by competent organ, person and according to the legal regulations.

Against this background there may appear different opinions and interpretations. If everything is going on in accordance with applicable law, under no circumstances one can question actions by competent authority in the area of personnel policy. It is not illegible to hunt corruption out in these processes, because it influences the reputation, undermines credibility, reliability and authority of government, as well as citizens' trust in the country's public bodies. Nevertheless, one can take slightly different, widened and multi-dimensional perspective of analytical thinking, which refers to the so called **principle of availability** in public service. It stems directly from the Constitution: *Polish citizens enjoying full public rights shall have a right of access to the public service based on the* ***principle of equality*** (Article 60).[65]

The act amending the law on the civil service[66] adopted in the end of 2015 has introduced some significant changes, for example discontinuation of the so called "open and competitive mode" by employment on higher management positions as well as the scope of qualifications, the candidates shall fulfill.[67] In the public debate back then there were logical and justified arguments that resignation from competitions for recruitment for higher positions in the civil service is appropriate, because all those notifications were anyway fictitious – and the winner was the person who was supposed to be chosen, and there was no need to pretend that it was honest and competitive. There were also other rational and right opinions that the modifications of provisions made a quick change of personnel possible. Naturally, official explanatory memorandum to the draft generally indicated that (...) *proposed changes with regard to the occupation of higher posts are a consequence of previous practice which disclosed how ineffective and long-winded the procedures were*[68]*,* and in the legal opinion of BAS (Bureau of Parliamentary Analyses) of 12 January 2016 on the changes made, there are neither remarks nor comments with reference to Article 60 of the Constitution of the Republic of Poland. It all proves how illusionary the provisions of the Constitution are, which theoretically are a set of rules of law – a foundation of a democratic country based on the rule of law.

---

[65] The Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483 as amended).

[66] Evolution of the legislative process, source: http://www.sejm.gov.pl/Sejm8.nsf/PrzebiegProc.xsp?nr=119 [access: 7 II 2018].

[67] The Act of 30 December 2015 amending the act on civil service and some other acts (Journal of Laws 2016, item 34).

[68] M. Gintowt-Jankowicz, *Opinia prawna o projekcie ustawy o zmianie ustawy o służbie cywilnej oraz niektórych innych ustaw*, druk sejmowy nr 119 z 15 grudnia 2015, Biuro Analiz Sejmowych, Warszawa 2015, source: http://orka.sejm.gov.pl/rexdomk8.nsf/Opdodr?OpenPage&nr=119 [access: 7 II 2018].

There are no problems with giving examples of attractive state sinecures, which are taken by arbitrary decisions in the legal form of appointment for the position. It means that all decision making processes connected to filling the positions can be assessed and interpreted on the ethical and moral plane, but they cannot be questioned from the legal point of view. Information given to the public on certain nominations describes in fact the final effect of other backstage activities (recommendations, support) of some people having a direct or indirect impact on the course of events. The awareness of these processes is not for the public and is of **secret nature**. The most constitutive feature of the described personnel processes is their efficiency in the sense that every time informal arrangements, which were made previously (in a narrow circle of **influential** people), are next implemented without any obstacles and according to the scenario required.

This is exactly the same situation with **legal corruptive practices** in personnel area, their effects are overt but **the course of events prior to a certain legal action is covert**. This mechanism within benchmarking is duplicated as a model of efficiency in other recruitment processes where, according to the law, the institution is obliged to publish vacancy notices. First, preliminary decision is taken in a narrow circle of important people about the need to employ a particular candidate. Then, next actions regarding the so called "open and competitive" procedure are subordinated to the idea. Proper criteria and formal requirements are prepared, which need to be fulfilled by the employee. Without much effort one can profile formal requirements like detailed education, postgraduate studies, specific courses, trainings and necessary professional experience on particular positions to successfully constrain the number of potential rivals and only on a preliminary stage show **favouritism** of a particular person. In other words, one can dedicate, fix a vacancy notice for a particular person so that the requirements could be filled only by the one and only candidate. In practice, there is also a second, more sophisticated and subtle method to lend colour to fairness of the proceedings and competitiveness of the choice. The requirements formulated then are less precise to let other candidates show up. Then no one could say that others did not have a chance. In the end, of course the predefined beneficiary wins and it can be said that the winner was assessed as the best by the "independent" recruitment commission.

With regard to presented considerations one might wonder from which perspective the **fixing of competitions** and interfering with their course should be assessed. And how such behaviours shall be assessed from the legal perspective? In fact it is a very important question because depending on the criteria and the reasoning different conclusions and opinions could be drawn.

From the perspective of a person representing an employer the following arguments will be given that according to competences he/she does have the right to take autonomous personnel decisions as well as to profile detailed formal requirements crucial for a particular position in order to conduct effectively tasks on the highest possible level. The fact that there was only one candidate who fitted formal criteria

given in the notice can give only satisfaction that the person with required qualifications and expected experience was managed to be found. All procedures took place in accordance with the law, so it is completely unfounded and unauthorised to raise any objections in the case.

Looking at a particular case from the other side one should undoubtedly admit that **fixing formal criteria so that a concrete candidate** would fit in is an activity that has a direct impact on the whole competition procedure. As a result a particular beneficiary gets tangible personal and material benefits. The person chosen is treated specifically and their position of dominance compared to other potential candidates looking for a job is guaranteed. In view of the fact that such a case happens in one of the public finances institutions, which are obliged to carry out open and competitive recruitment procedures under appropriate legal act, the actions described above completely **undermine** and **contradict** the authenticity of conduct. Further dilemmas come up whether to qualify such behaviours only as deficiencies or irregularities, or deliberate and targeted **abuse of power and acting against the public interest?**

Analysing publicly available communiqués by CBA (Central Anti-Corruption Bureau) on the web-site one can come across only one case connected to a job offer: (...) *people arrested used their positions and influenced the course and results of competition procedures relating to the recruitment of some officials, i.e. directed the recruitment process to employ only predetermined individuals*.[69] Unfortunately, the media reports give no information which would allow to comment on the legal status of the act and the grounds for detainment. From the fact that CBA do not identify more practices of this kind it cannot absolutely be concluded that fixing competitions is of incidental nature only because a separate case was found in one of local municipalities. In reality it is quite opposite because the crushing majority of recruitment procedures look exactly like this and the final result is known even before the vacancy note is published. All the people who are engaged in implementing the scenario and having real influence on the course of events, perfectly know about it and accept it.

Staying in the area, we can mention another, given in media case of influencing recruitment procedures in the Supreme Audit Office (NIK). In this case, according to the prosecutor's office a crime of power abuse was commited (Article 231 §1 of the penal code), and the acts were assessed as (...) *highly socially harmful. They caused a real damage to public and private interests.*[70] Presented interpretation of the analysed case in connection with the abuse of power and influences corresponds with former remarks on competitions, which were formulated according to the rules of the correct reasoning and knowledge and life experience. However, it is not

[69] See. The communiqué of CBA of 2 XII 2016 in the case of competition procedures in recruitment process in a local municipality, source: https://cba.gov.pl/pl/aktualnosci/3610,Zatrzymani-wojt-sekretarz-i-kontroler-NIK.html [access: 3 II 2018].

[70] See. The Chairman of NIK with allegations, 8 IX 2009, source: https://wpolityce.pl/kryminal/356851-prezes-nik-z-zarzutami-zdaniem-prokuratury-doszlo-do-przestepstwa-naduzycia-wladzy-przy-obsadzaniu-stanowisk-w-izbie [access: 3 II 2018].

the final and binding assessment of the problem because it is the court that shall settle the matter, and to be more precise indicated jury.

Completely different are recruitment processes in state-owned companies and other institutions, where the law does not impose any obligations to carry out open competition procedures for prominent management positions as well as other job places. On the basis of studies, documents analyses and open source information one can notice common and repeated practices and circumstances of the usurpation of the public sector. To be precise, only a chosen category of beneficiaries gets lucrative positions of chairpersons, managing directors, specialists in those institutions where their fellow party members hold power, thanks to their arbitrary and discretionary decisions. In brief, one can describe them as councilmen, party members, former politicians, members of their families, people linked to them and their acquaintances. What is more, the common phenomenon is combining positions in management boards and positions of directors in governmental administration or local administration with positions in supervisory boards.

Description of some aspects is needed because the mechanisms, patterns of behaviour, and more importantly, the goals of the described personnel activities, are continued in other functional areas. Decision making powers are particularly used inter alia for entering into agreements with designated outer entities, or preparing and carrying out activities when it comes to procurement and public orders. But is there anyone who can admit that? Certainly not because (...) *governance is accompanied by discretion*[71] and protecting the knowledge of interests and improprieties.

Conclusion

The remarks and analyses presented in the article entitle us to formulate a statement that corruption in wider sense is wrong against fair, compliant with the principles of the rule of law and social justice existence of the Polish country.One of the main goals of the study is proper organizing and structuring the knowledge of the phenomenon, as well as circumstances and factors which foster some practices. Such an approach makes it possible to get to know deeply and understand the nature of some events, processes and decisions in management. It also leads to broader horizons and better perception of behavioural patterns, common in organizational reality. In the literature an opinion dominates that unambiguous and precise definition of corruption with all its features and mechanisms is a difficult task.[72] Because of that the basic problem is to describe in detail and fairly characterize a notion and then express assessments, logically justified opinions and value judgements on the subject.

[71] P. Wiatrowski, *Prawne, ekonomiczne i socjologiczne aspekty korupcji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2008, no. 776, p. 102.

[72] M. Bartoszewicz, *Zagrożenia korupcyjne w polskim samorządzie*, „Rocznik Samorządowy" 2016, vol. 5, p. 24.

Andrzej Cieślik and Łukasz Goczek point out that forms of corruptive behaviours tend to change along with changes and transformations in current economy.[73] On the basis of the observation made one can come to a conclusion that the most common practices refer to the so called **legal corruptive activities**, which take a dominant position. However, it does not mean that they are less socially harmful and do not pose a serious threat to the state economic interests – on the contrary. We have to agree with the view that corruption occurs not only in public sector[74], but it may appear in activities of all entities and organisations in the ordinary course of trade.[75] Nevertheless one cannot accept such a way of thinking that would imply the existence of corruption practices only in case of post-communist countries, because the phenomenon takes place also in countries with a democracy based on firm foundations.[76]

Corruptive behaviours are mostly associated with politics and the exercise of public authority. And here a link between corruption and political pressure[77] is indicated, and it is an accurate observation. According to Piotr Solarz, there have been created dysfunctional links called "a deal", like patron-client scheme within authority and public administration environment. *These links refer to using positions and public financial means, as well as positions in administrative apparatus to benefit political clients.*[78] It is an accurate diagnosis which differs significantly from a statement that *the state makes efforts to counteract corruption by legal norms and promotion of ethical standards.*[79]

There are more and more theoretical deliberations on possible methods and ways of counteracting corruption in modern literature. There are, among them, for example the need of developing anti-corruption strategy, management by reliability[80], moving tasks connected to fighting corruption from the scope of ABW (Internal Security

[73] A. Cieślik, Ł. Goczek, *On the of Corruption Patterns in the Post-Communist Countries,* „*Equilibrium. Quarterly Journal of Economics and Economic Policy*" 2015, no. 1, p. 37.

[74] A. Cieślik, Ł. Goczek, *Korupcja, jakość rządzenia a wzrost gospodarczy w krajach transformacji*, „Rocznik Instytutu Europy Środkowo-Wschodniej" 2016, no. 5, p. 94.

[75] W.M. Grudzewski, I.K. Hejduk, A. Sankowska, *Korupcja w organizacji*, „Ekonomika i Organizacja Przedsiębiorstwa" 2008, no. 7, pp. 5–10.

[76] B. Czepil, *Zjawisko korupcji w demokracji skonsolidowanej. Przypadek Finlandii*, „Przegląd Politologiczny" 2017, no. 2, pp. 113–127; P. Grabarz, *Zjawisko korupcji w Polsce i Norwegii – zarys charakterystyki porównawczej*, „Studenckie Zeszyty Naukowe" 2016, no. 29, pp. 37–45.

[77] M. Piotrowska, *What Factors Matter for the Evaluation of Relationship between the Perceptions of Corruption and Politicization in Local Administration in Poland*, „Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu. Ekonomia" 2010, no. 136, pp. 138–149.

[78] P. Solarz, *Ekonomiczne i kulturowo polityczne przyczyny korupcji w Polsce po akcesji do Unii Europejskiej*, „Kwartalnik Naukowy Uczelni Vistula" 2013, no. 4, p. 12.

[79] T. Szewc, *Korupcja: wybrane konsekwencje prawne*, „Organizacja i Zarządzanie" 2015, no. 1, p. 127.

[80] Z. Dobrowolski, *Strategie i metody przeciwdziałania korupcji*, in: *Bezpieczeństwo ekonomiczne państwa. Uwarunkowania, procesy, skutki*, A. Jackiewicz, A. Trzaskowska-Dmoch (ed.), Warszawa 2017, pp. 122–125.

Agency) competences to CBA[81], increasing economic liberties of citizens.[82] Using modern information technologies in teaching and promoting ethical standards is also advised.[83] It is pointed out that high schools as institutions responsible for shaping young people's attitudes should play a significant role in the education process of present and future managers as far as ethical standards and anti-corruption behaviours are concerned.[84] It is recommended to include so called *Principles for Responsible Management Education* – PRME into teaching content.[85] However, an important question arises, if these proposals can truly contribute to a significant reduction of the corruption in Poland?

In view of the deliberations presented in this paper it is worth commenting on some statements by ABW: (...) *corruption is the phenomenon that facilitates illegal mechanisms of taking decisions that create relations in a public sphere. Socially entrenched corruption habits are a factor damaging state structures.*[86] This opinion should be supplemented, because the practice proves that in most cases **corruption** influences **legally taken decisions** by the authority representatives, i.e. in compliance with granted powers and competences. Referring to habits it should be pointed out that they are mostly created, promoted and reinforced by political parties and ruling authorities. The chosen by a nation, establishment, extraordinary caste, parlour society, i.e. groups holding power treat institutions under the state supervision as their own, which is contrary to the Constitution, because: (...) *the Republic of Poland shall be the common good of all its citizens (article 1).*[87] So, in whose interest would be activities against corruption and to whom they would serve?

Bartosz Czepil assesses in a logical and accurate way "the fight with corruption" as (...) *a never ending and self-justifying process.*[88] The necessity of counteracting corruption is justified by the fact that new forms of corruption enforce applying other methods and anti-corruption actions, which **will never end**. Agnieszka Turska-Kawa claims that (...) *the subject of corruption is a man, and it is his awareness, knowledge, strong psychological*

[81] P. Chodak, *Korupcja – jak ją skutecznie zwalczać*, „Journal of Modern Science" 2017, no. 1, p. 353.

[82] A. Pluskota, *Wpływ wolności gospodarczej na korupcję na przykładzie wybranych państw europejskich*, „Folia Oeconomica Acta Universitatis Lodziensis" 2017, no. 328, p. 161.

[83] E. Stawiarska, J. Machnik-Słomka, *Zastosowanie współczesnych narzędzi informatycznych w nauczaniu w kierunku zachowań etycznych i antykorupcyjnych*, „Organizacja i Zarządzanie" 2016, no. 2, pp. 143–156.

[84] Ibidem, p. 144.

[85] E. Pawłowska, K. Skowron, *Wykorzystanie nowoczesnych technologii informatycznych w procesie wdrażania zasad nauczania przeciwko korupcji w szkolnictwie wyższym*, „Zeszyty Naukowe Politechniki Śląskiej. Seria Organizacja i Zarządzanie" 2016, no. 92, p. 256.

[86] Tasks of ABW, countering corruption, source: https://www.abw.gov.pl/pl/zadania/zwalczanie-korupcji/50,Zwalczanie-korupcji.html [access: 9 II 2018].

[87] The Constitution of the Republic of Poland of 2 April 1997 (Journal of Laws 1997, no. 78, item 483 as amended).

[88] B. Czepil, *The "fight against corruption" as a never-ending and self-legitimizing process*, „Studia Socjologiczne" 2016, no. 4, p. 228.

attitude, inside integrity and reliability that should be a starting point of any anti-corruption activities.[89] In reference to these interesting remarks one fundamental question should be answered: do all the people have the same attitude to corruption and the same opinion on it?

Corruption is highly desirable and valuable for people engaged in a deal because they benefit from it, have spectacular financial successes, their career paths are ensured as well as possibilities of development. Other people from our society, people without any connections, acquaintances, the marginalized, blocked and destroyed by existing deals see things in a different way. It means that depending on the perspective corruption will be interpreted and assessed differently, in a positive or negative aspect. Corruptive practices are currently **under noticeable modification** because they adapt to new reality, challenges of modern times and that is the reason they take more sophisticated, **secure** and covert forms. Nevertheless, for many years the goals, rules and mechanisms of the deal remain unchanged.[90]

Abstract

The article presents considerations and analyses that enable detailed recognition of the essence of the corruption phenomenon perceived in the context of common management methods and decision-making processes. At the beginning, it was explained how the concept of corruption should be understood and also the main corruption mechanisms were described. In the further part of the work, corruption is analyzed as an important and crucial element of management system. At this point, particular attention is paid to threats to the economic interests of the state, as well as violating the rules regarding principles of the law and social justice. Next, the aspects and contemporary forms of corruption behaviours were discussed, as well as the main functional areas of management practice where corruption occurs most frequently. In the final part the personnel policy as an important component of corrupt practices is analyzed.

Keywords: corruption, corruption-related mechanisms, authority, influences, connections, the rule of law, social justice.

[89] A. Turska-Kawa, *Przeciwdziałanie korupcji – ujęcie wielopłaszczyznowe*, „Political Preferences" 2017, no. 17, p. 110

[90] W. Walczak, *Źródła zachowań o charakterze korupcyjnym w praktyce zarządzania***,** in: *Korupcja w administracji*, M. Myśliwiec, A. Turska-Kawa (ed.), Katowice 2016, pp. 63–88.

Mateusz Jaremczuk

The National Anti-Corruption Bureau of Ukraine cooperation with secret service agencies of other countries versus the internal security of Poland

Introduction

Due to the protests in the European Square in Kiev, the Crimea crisis, and the crisis in the east of Ukraine, which took place in 2013/2014, the then president Victor Yanukovych was removed from his office. Following the events new authorities were elected in Ukraine, and the direction of the foreign policy was reversed, as up to that moment it was pointed to Russia. The new government and the president, in line with the Ukrainian people, started in 2014 a process of restoring ties with the West, particularly with the European Union and the United States. Ukraine thereupon was forced to implement a wide array of reforms regarding internal system of the state, to limit, inter alia, abuses from the power and oligarchs.[1] Implications of the Ukrainian crisis lasting since November 2013 refer also to the internal security of Poland. The Ukrainian and Polish border is, at the same time, the border between NATO and the European Union and Ukraine.

A goal of this article is to establish the influence of the National Anti-Corruption Bureau of Ukraine cooperation with other countries' special services on the internal security of Poland. The problem of corruption in Ukraine is particularly important in view of the fact that hundreds of thousands Ukrainian nationals migrate to Poland. In this context it is crucial to establish the destabilizing effect of corruption on the security of Poland. Since the problem pertains not only to those nationals, who are led to emigrate due to the internal situation of the country, but also to the country as a whole. Destabilisation of such a large country in Central and Eastern Europe affects geopolitics in the region. Consequently, it seems justified that the EU countries (particularly countries that border Ukraine) and the United States as a superpower taking care of the international order, should assist Ukrainian services responsible for combating corruption, because they have a vested interest in it. Institutions responsible for combating corruption in Ukraine have no relevant experience in that field, that is why the proper cooperation with their counterparts in other countries will affect their efficiency. In the long term the quality of cooperation will influence either the improvement or deterioration of security not only in Ukraine, but also in Poland.

[1] W. Głowacki, *Rok w którym Europa osiwiała*, Polska The Times, 21 November 2014.

Corruption versus internal security

Andrzej Barcikowski in his article *Bezpieczeństwo wewnętrzne – różne perspektywy analityczne i doktrynalne*[2] points out that internal security is not a separate scientific field, nevertheless, it can be regarded as related to political sciences and constitutional law, since analyses in this area have primarily a practical dimension. The author also notices that (...) *precise categorization, explication, and prediction in the field of internal security can and should influence the choice of instruments and areas of the state activity.*[3] Although, he points out that internal security refers to a state as a whole, not to its individual components. Furthermore, Stanisław Sulowski emphasizes that security is not of a permanent nature and its understanding is subjective, particularly in cultural and political context.[4]

One of the factors directly influencing internal security of the state is corruption. The definition of this phenomenon shows that it takes place with the participation of two consciously acting sides. One side affects the other by means of certain goods, and this way a certain activity is enforced. Partners committing an act of corruption in conjunction and shall seek to conceal the transaction concluded to avoid responsibility. Such definition is proposed by Piotr Sulowski in his article *Korupcja zagrożeniem dla bezpieczeństwa wewnętrznego państwa.*[5] It should be added that corruption can be committed also by one person. This applies in particular to people performing public functions, who can defraud or take the public property over, or cause it is wrongly handled while using the public position. It is also possible that people who do not perform public functions commit a criminal act. By their expertise or formal opinions they do not comply with the law and shall aim to achieve a profit.[6] Apart from bribery and venality, corruption is also misuse of the function, nepotism, favouritism, and influence peddling. Apart from the definition, another vital factor characterizing corruption is its almost unlimited multiformity. The subject of corruption is shaped by many determinants depending on the country, by its frequency, universality, and the time this criminal act was committed. It may relate to both developed and underdeveloped countries, public and private sector, NGOs, and foundations.[7]

Speaking about the influence of corruption on the internal security of the state, Ukraine in particular, it is justified to indicate its kinds and its effects. Undoubtedly each kind of corruption brings with it negative consequences for the security

[2] A. Barcikowski, *Bezpieczeństwo wewnętrzne – różne perspektywy analityczne i doktrynalne*, Internal Security Review 2014, no. 11, p. 11.

[3] Ibidem, pp. 11–12.

[4] S. Sulowski, *W poszukiwaniu definicji bezpieczeństwa wewnętrznego,* www.abw.gov.pl/download/1/1756/Majew.pdf [access: 25 July 2018]

[5] P. Sulowski, *Korupcja zagrożeniem dla bezpieczeństwa wewnętrznego państwa*, „Annales Universitatis Paedagogicae Cracoviensis. Studia Politologica" 2012, no. 8, pp. 57–58.

[6] Ł. Szwejkowski, *Korupcja, wybrane zagadnienia,* „Materiały dydaktyczne Centrum Szkolenia Policji" 2013, no. 87, pp. 7–8.

[7] P. Sulowski, *W poszukiwaniu definicji*..., p. 57.

of the country, both in the long term as well as in the short term. Corruption can be classified with regard to several factors. For the purposes of this article a breakdown by the spheres of the state activity has been adopted, i.e. administrative, economic, and political. Sometimes there is an overlap between these spheres, the phenomenon of corruption is also quite often present on several levels. Administrative corruption (clerical corruption) relies on taking by the public administration workers additional perks of the job in official affairs for realising or withdrawal of an obligation resulting from the policy of this certain institution. Corrupted public administration workers in return for personal benefits, generate economic losses, and make it impossible for the country to act properly. Economic corruption is connected to clerical corruption. It happens where administrative decisions are made, followed by spending money from the state budget. It relies mainly on bribery and venality. These are the instruments, owing to which businessmen can influence the clerks and politicians in order to achieve favourable conditions for their businesses. It causes disturbances in economic processes of the state, and in consequence inhibition of development, and fall in productivity by intervention in the market. Furthermore, it paralyzes proper functioning of the country, and decreases the authority of state institutions. Third kind of corruption is political corruption. It means illegal activities in favour of political parties and their members, that aim at getting or maintaining power illegally. Political corruption has a particular impact on the functioning of a country by direct influence on the governance, which leads to a destabilization of the political scene. This kind of corruption is very often connected with the culture and history of a country, since it is followed quite often by social acceptance and regarding the phenomenon as a common practice.[8]

Furthermore, Olgierd Chybiński devoted a lot of attention to the phenomenon of influence peddling.[9] He pointed out a danger coming from the fact that it is rooted in society. Since in many countries it is accepted that in order to settle formalities you need to have contacts, or bribe a contact man. This practice is often used by frauds, who often have nothing to do with this particular institution.

The main implications of corruption for the state internal security are as follows: generating costs of the state, which eventually must be covered by citizens, slowdown in the economy, political decision making dependence on outer entities, drop in attractiveness for foreign investors, lowering the confidence of citizens in the state institutions, and restriction of competition in the economy. A particularly harmful factor to a country is also the fact that the level of corruption is directly proportional to difficulties in getting rid of the problem. It comes from a dependence of authorities and clerks on the money from corruption. The bigger the dependence, the less motivation to introduce legal regulations to fight the phenomenon.[10]

[8] Ibidem, pp. 58–64.
[9] O. Chybiński, *Płatna protekcja*, Warszawa 1967, pp. 7–8.
[10] A. Barcikowski, *Bezpieczeństwo wewnętrzne*..., pp. 18–19.

Fight against corruption in Ukraine

Corruption is one of the major problems in Ukraine, which separates the country from the west effectively. One of the reasons for demonstrations and protests known as Euromaidan was President Yanukovych declaration of suspending the Ukraine-European Union Association Agreement on 18 November 2013. Experts point out that by signing the document and declaring the will of cooperation with the European Union, Victor Yanukovych would have pledged state reforms also as far as combating corruption is concerned. The President, under influence of Russia and groups of oligarchs, had decided to demonstrate attachment to former style of power and had not appeared in Vilnius, where the agreement was supposed to be signed.[11] It caused escalation of riots in the Ukrainian society hoping for change, particularly among dysfunctional authorities.[12] The overthrow of President Yanukovych followed the so called Revolution of Dignity. Coming into power by Petro Poroshenko and the change of government in 2014 gave hope for reforms in the state and elimination of irregularities from the public life.

According to the Global Corruption Barometer published by Transparency International in January 2017, Ukraine takes 131 position as regards corruption among 176 countries in the rank.[13] In a 2016 poll[14] Ukraine scored 29 points out of 100 (the higher the score of points the higher transparency and less problems with corruption). In view of this Ukraine was among the most corrupted countries in the world. Respondents from Ukraine perceive corruption as one of the crucial problems of the country (56% of those surveyed; 69% stated economic problems in the first place). They claim that the level of corruption in Ukraine has not changed for the last several years (72% of respondents), and President Petro Poroshenko is considered to be guilty of the situation (60% of respondents). The incumbent President of Ukraine does not enjoy public confidence. Only 13% of the respondents are convinced that the authorities of Ukraine are heading to deal with the problem of corruption which translates into a negative attitude toward the president (70% does not trust him). Furthermore, the report states that decline in support for the present authorities translates into a growth of support for populist parties, that are not, paradoxically, interested in fighting corruption. As far as the self-reflection of the Ukrainians alone regarding the subject of corruption, the poll's results are also not a positive prognosis for possible changes. Admittedly, ca. 33% of respondents point out bribery as one of three main causes of inefficient struggle with corruption, and only 25% of respondents claim that the society is

[11] M. Czech, *Kres zbliżenia Ukrainy z Europą: Janukowycz wywrócił stolik*, Gazeta Wyborcza, 22 November 2013.

[12] K. Kwiatkowska, *Mustafa odbije Ukrainę*, Gazeta Wyborcza, 29 November 2013.

[13] www.transparency.org, *Corruption Perceptions Index 2016* [access: 03 I 2018].

[14] At the time of publication of this article the 2017 poll will be accessible; its publication is scheduled for 27 January 2018.

co-responsible for that. The fact that 2/3 of Ukrainians consider corruption as an integral part of their lives deserves particular attention.[15]

Despite the fact that the poll's results show that Ukraine is deeply plunged into corruption, it should be noted that in view of the Global Corruption Barometer results, some slight and subtle positive changes are observed. In 2012 Ukraine scored 26 points, in 2013 – 25 points, in 2014 – 26 points and in 2015 – 27 points, according to Transparency International reports.[16] A growing tendency can be seen, except the year of 2013. However, it was just the year of 2013 regarded as the breakthrough in Ukrainian society.

In view of the fact that the material and financial support for Ukraine was conditional and dependent on the struggle with corruption in the country, a number of specific actions were taken. Eradication of corruption from public life has become one of the key tasks of the new government by Arseniy Yatsenyuk and then by Volodymyr Groysman. In October 2014 Ukrainian parliament adopted a set of anti-corruption acts being a formal basis for establishing institutions to fight corruption, i.e. the National Agency of Ukraine for finding, tracing and management of assets derived from corruption and other crimes, the National Agency for Prevention of Corruption, the Specialized Anti-Corruption Prosecutor's Office and the National Anti-Corruption Bureau of Ukraine (NABU).[17]

One of the watershed moments in the struggle with corruption in recent times in Ukraine was the disclosure of financial statements of more than 100 000 public administration personnel and politicians, including the highest-ranking politicians. The system of electronic financial statements caused quite a stir among the Ukrainian society. It became apparent that, according to Reuter assessments, it was almost 300 000 USD savings per one member of Ukrainian government on average, whilst they got 200 USD parliamentary salary per month each. Making the data public met with the discontent of the Ukrainian parliamentarians.[18]

Implementation of the ProZorro electronic open source government e-procurement system can be regarded as a success in struggle with corruption. It allowed to save only in 2016 ca. 320 million USD in central budget.[19]

Piotr Kościński informs, referencing the Ukrainian Web site "Nashi Groshi", that still the biggest problem in Ukraine is corruption of the most important institutions in the country, including courts. It is in the interests of judges and prosecutors to maintain the present status quo. The daily says that from among ca. 1000 people charged with corruption between July 2015 and June 2016, only 3% of them were finally given a legally valid sentence. As far as losses for the state budget are concerned, the assets from corruption offences confiscated between 2015 and 2016 only amounted to

[15] V. Rybak, *Ukraine's fight against corruption, explained*, Euromaidan Press, 16 December 2016.
[16] www.transparency.org/cpi [access: 3 I 2018].
[17] P. Kościński, *Problem korupcji na Ukrainie*, Biuletyn PISM, no. 3 (1445), 13 January 2017.
[18] V. Rybak, *Ukraine's fight against corruption ...* .
[19] www.transparency.org, *Co-Creation of ProZorro,* [access: 3 I 2018].

10 000 USD in spite of the assumed 368 million USD. It is easy to calculate that the budget income was 36,800 times smaller than expected.[20]

Nevertheless, the start of struggle with corruption by the Ukrainian country, observed after Euromaidan, should be regarded as a positive. It is hard not to notice though that the motivation of the government and the administration, as well as of the whole society seems to be limited in this struggle. Thus it seems justified to claim that without any help from abroad Ukraine is not able to tackle such a big problem. Maria Jarosz confirms that and describes the phenomenon of corruption as both the cause, and the effect of the institutional failure of the state.[21]

The National Anti-Corruption Bureau of Ukraine

On 14 October 2014 Verkhovna Rada of Ukraine adopted the Law "On the National Anti-Corruption Bureau of Ukraine"(NABU), which entered into force on 25 February 2015.[22] Founding and launching the National Anti-Corruption Bureau was one of the requirements set by the International Monetary Fund and the European Commission for liberalization of visa restrictions between Ukraine and the European Union.

Article 1 of the Act says that **the National Anti-Corruption Bureau of Ukraine is a state law enforcement agency with the key objective of preventing, exposing, stopping, investigating and solving corruption-related offences committed by high officials, and averting new ones. Article 4 of the Act says about guarantees of NABU independence. It is to be reassured by specific procedures of appointment a director of the Bureau, appointing the employees of the Bureau based on the open competition results, specific procedures of financing the Bureau, and specific measures described in legal act, which ensure safety of the Bureau employees and their families. According to Article 5 of the Act, the maximum stuff number of the Bureau is 700 employees, including 200 high level personnel**.[23]

In January 2015 for the first time in the history of Ukraine an open competition for position of director of a state agency was announced. 186 candidates applied for the position of Director of the National Anti-corruption Bureau of Ukraine. The winner of the competition was Artem Sytnyk.[24]

According to Ruslan Minich in NABU there are good experts by Ukrainian standards employed. It allowed to start investigating hundreds of cases concerning corruption offences. The problem for the institution is dependence of its activities on other services and institutions. Minich gives an example of dependence on the Security

[20] P. Kościński, ibidem.

[21] M. Jarosz, *Władza, przywileje, korupcja*, Warszawa 2004, p. 249.

[22] The full text of the Act on http://zakon4.rada.gov.ua/laws/show/1698-18 [access: 4 I 2018].

[23] *Krajowe Biuro Antykorupcyjne Ukrainy*, „Przegląd Antykorupcyjny" 2016, no. 1 (6), pp. 225–227.

[24] https://nabu.gov.ua/en/history-nabu [access: 4 I 2018].

Service of Ukraine (SBU) in regard to wiretapping and releasing by courts individuals arrested by NABU. The author points out the need to appoint an independent anti-corruption court as a totally new institution, which would supplement NABU activities and the activities of the Specialized Anti-Corruption Prosecutor's Office. Furthermore, the Bureau's activities are disturbed by incumbent politicians, who start to cease to feel impunity and try to take control of the Bureau. It is a very popular idea among Ukrainian MPs to delegate control of the NABU to the Prosecutor's General Office (dependent on politicians).[25]

Igor Shevliakov, the author of article *Ukraine*[26], referring to challenges of Ukrainian institutions in struggles with corruption points out that NABU is not able to function properly without any outside assistance. Establishing of NABU was certainly a symptom of the Ukrainian struggle with corruption. Although weighing the ideology of its establishment against pragmatism is ruthless. The Bureau with the assistance of services from other countries, particularlythe Federal Bureau of Investigation (FBI) functions, as far as possible, independently of authorities. Maintaining this tendency is a huge challenge, because currently it is the only institution acting independently. In case of struggles with corruption it is sine qua non. It was a great success when the Bureau was established, but if it loses its autonomy the success will be worthless. The struggle with corruption in Ukraine cannot be successful without effectively acting NABU. Igor Shevliakov adds that corrupted Ukrainian authorities are very well aware of that and try to influence its activities.

The National Anti-Corruption Bureau cooperation with other countries' special services

Founding NABU was initiated from outside as one of the requirements for further talks between the European Union and Ukraine on relaxation of visa policy. Its founding does not, however, mean that the problem of corruption in Ukraine has been solved yet. In reality it was a signal for changes, whereas it gets more and more opponents in the course of time. What is important, these opponents come from Ukraine and very often hold key positions for the country. Taking into account the scale of the problem in Ukraine, it is necessary to get external support for NABU activities. The assistance for the Bureau comes mainly from the west, the support is offered by Americans, Poles, and those countries that have a vested interest in stopping further destabilization of Ukraine.

The United States as a superpower shall endeavour to maintain or even widen their sphere of influence. Ukraine is a good example. Just after Victor Yanukovych had been overthrown, Ukraine became a partner for the European Union and

[25] R. Minich, *Ukraine's Fight Against Corruption: Stumble But Not Fall*, Internews Ukraine, 14 April 2017.

[26] I. Shevliakov, *Ukraine*, in: *Anti Corruption in Moldova and Ukraine*, A. Sobjók (ed.), Warszawa 2015, pp. 27–33.

the US. Ukraine is the NATO direct neighbour and a crucial country in a strategic and geopolitical sense. Ukraine is also within Russia's interest, mainly because it had belonged to the USSR.[27] After the annexation of Crimea and destabilizing eastern parts of Ukraine, Russia chose not to get into an open conflict with Ukraine. Destabilized Ukraine is an attractive partner for the US. By financial means, the US influence Ukrainian authorities and create a buffer zone in the form of Ukraine between NATO and Russia.[28] It should also be stressed that it is crucial for the security of Poland as well.

In the last three years only, the United States have provided a financial assistance to Ukraine in the official amount of 1,5 billion USD. During President Obama presidency, in March 2014, the US Congress authorized financial aid to Ukraine amounting to 1 billion USD.[29] It was period of significant change in Ukraine, taking place mostly at the highest levels of government, and the money was to be dedicated to pro-democratic reforms and combating criminality. The next amount of money totalled 220 million USD. According to Reuters agency, it was transferred in June 2016.[30] The money was transferred two months after Volodymyr Groysman took over as a prime minister. Joe Biden, the US Vice President, while informing about this financial aid praised the reforms undertaken by Ukraine. On 12 December 2017 Blair Guild informed on the CBS web site that President Donald Trump signed the new 2018 US defence budget which grants 350 million USD financial aid to Ukraine.[31]

Transfer of such large amounts of money for reforms in Ukraine is not done hastily by Americans. Having the awareness of how big the problem of corruption in Ukraine was and how risky the transfer of huge sums of money to the Ukraine administration was, the Americans indirectly contributed (via the IMF) to the establishment of NABU. One of the most important partners of the Bureau and a role model was the FBI. In January 2016 the director of NABU Artem Sytnyk paid a visit to Washington, during which he signed an official agreement on mutual cooperation with the FBI. As Sytnyk stressed in the Voice of America[32], a particularly important aspect of cooperation is the fact that the FBI has instruments to follow dollars transactions, which is invaluable in struggling with corruption. The Director of NABU pointed out as well that the problem of corruption in Ukraine extends far beyond its boundaries, and detection of means flowing out of his country would be extremely difficult without the assistance of the FBI. The agreement established cooperation in combating money laundering, recovery of assets and combating corruption among high-level officials in Ukraine.

---

[27] M. Czech, *Rosja bez Ukrainy jak bez ręki. Plan przezbrojenia armii poważnie zagrożony*, Gazeta Wyborcza, 23 June 2014.

[28] K. Przybyła, *NATO wobec konfliktu na Ukrainie*, „Bezpieczeństwo Narodowe" 2016, no. 37–40, pp. 118–120.

[29] J. Weisman, *Congress Approves Aid of $1 Billion for Ukraine*, The New York Times, 27 March 2014.

[30] www.reuters.com, *U.S. to give Ukraine $220 million in new aid: White House* [access: 4 I 2018].

[31] www.cbsnews.com, *Trump signs National Defense Authorization Act* [access: 4 I 2018].

[32] www.zik.ua, *NABU and FBI will sign Memorandum of cooperation* [access: 5 I 2018].

Furthermore, the American agency promised to provide the Ukrainian service with proper equipment. It is worth noting that the equipment for digitalization of documents provided by the FBI was already used in June 2016 during Black Accounts affair linked to the Ukrainian Party of Regions headed by Victor Yanukovych. Using techniques transferred by Americans made the job of this Ukrainian service much easier.[33]

It was already in February 2016 when Artem Sytnyk informed in a radio interview that an FBI agent had been assigned to the Bureau to cooperate with NABU detectives and supervise their activities in terms of their compliance with American standards.[34] In May 2015 American Ambassador to Ukraine, Geoffrey Pyatt, visited the NABU.[35] He paid attention to the role of the Bureau in changes taking place in Ukraine. He assured that the US were to continue to support the NABU in their struggle with corruption, mainly in terms of performing orders relating to high risks.

The memorandum of cooperation between the FBI and the NABU came officially into force on 29 June 2016. Two weeks later, first FBI agents came to Ukraine to conduct training for Ukrainian employees of the Bureau.[36] First special training lasted 10 days and covered, inter alia, tactical training, arms practice, methods of arresting criminals in a building and in a car, as well as ways of clearing buildings.

The year 2017 proved to be very fruitful for cooperation between the NABU and the FBI. In June 2017 detention took place in connection with the Amber case[37] conducted by the NABU with cooperation with the FBI. The cooperation between the two institutions allowed to detect illegal process of amber mining in the western Ukraine and to arrest some officials, including the regional deputy prosecutor. Moreover, a Ukrainian parliamentarian is also under suspicion. The Director of the NABU stressed that the operation would not be possible without the FBI assistance. High rank individuals involvement in the case led to a conflict among Ukrainian institutions responsible for struggle with corruption. Organs directly supervised by politicians opposed the way the NABU had conducted the case. It also highlighted the scale of the problem the NABU has to deal with. Few days after details of the operation had been revealed, Kyiv Post informed via Interfax-Ukraine agency that the memorandum of understanding between the two agencies was prolonged for another two years.[38] Both sides stated that they are satisfied with their mutual cooperation and are willing to continue and develop it.

---

[33] www.nabu.gov.ua, *The NABU Director calls upon individuals mentioned in Trepak`s lists to provide their handwriting samples voluntarily* [access: 5 I 2018].

[34] www.nabu.gov.ua, *FBI representative will work together with the NABU detectives* [access: 5 I 2018].

[35] www.112.international, *US Ambassador visited Ukrainian National Anti-Corruption Bureau* [access: 5 I 2018].

[36] www.112.international, *FBI train Special Forces of Ukraine's National Anti-Corruption Bureau* [access: 6 I 2018].

[37] www.interfax.com.ua, *Amber case first joint NABU-FBI operation* [access: 6 I 2018].

[38] www.kyivpost.com, *NABU,* ФБР розширюють співпрацю ще на *2* роки [access: 6 I 2018].

The Amber case was not the only operation carried out in cooperation with the FBI in 2017. In September there was a crisis of state institutions responsible for combating corruption in Ukraine. The NABU in cooperation with the FBI and the Specialized Anti-Corruption Prosecutor's Office started a case on a possible illegal enrichment of the chief of the Prosecutor General Office of Ukraine, Yuriy Lutsenko, and possible corruption at the State Migration Service of Ukraine. Its head staff was to make profits from legalization of foreigners' stay in Ukraine. The case was described by James Marson in The Wall Street Journal.[39] The reporter stressed that the efficiency of anti-corruption activities in Ukraine is closely linked to financial means from the IMF or the World Bank. In November 2017 the Security Service of Ukraine and the Prosecutor General Office came into conflict with the NABU and Specialized Anti-Corruption Prosecutor's Office. An NABU agent was arrested at that time, acting undercover in a case concerning irregularities in the State Migration Service of Ukraine. The agent was arrested by order of the Prosecutor General, who claimed that the NABU had acted outside the law. The case got a lot of publicity in the West. Christine Lagarde, representative of the IMF expressed her concern over the events that might stop development of independent institutions designated for combating corruption in Ukraine. The World Bank and the US State Department issued statements in a similar tone, suggesting that any restrictions on the NABU independence may have some serious implications in support of Ukraine by western countries. Ukrainian authorities, despite strong pressure, decided to submit in Parliament a draft act on possibilities to call off the Director of the NABU by a parliamentary vote of no confidence. Eventually, the bill was not proceeded by the parliament at all. According to some commentators, President Petro Poroshenko and other top politicians in Ukraine are not satisfied that the NABU, in cooperation with the FBI and other services, is an independent institution, detaining on charges also significant politicians or people linked to them (for example, the son of the Minister of the Interior).[40] Commentators stress also that bearing in mind the pressure from the West, President Poroshenko and his party will not decide on radical changes in the NABU, although fruitful cooperation between them cannot be expected.[41]

Cooperation between the NABU and the FBI seems to be crucial for further development of the service and its further existence. In fact it is hard to imagine independence of the Bureau in Ukrainian reality without the outside assistance of services and organizations. Although the cooperation with Americans is not the only one, the NABU established.

Few months after the NABU had been established, it started cooperation with its Polish counterpart – the Central Anti-Corruption Bureau (CBA). According to the news

[39] J. Marson, *Corruption Battle Roils Ukraine*, The Wall Steer Journal, 12 September 2017.

[40] T. Vorozkho, *FBI Says Its Support for Anti-Corruption Unit Abides by Ukrainian Law*, Voice of America, 7 December 2017.

[41] J. Donati, *Feud Thwarts FBI-Backed Anticorruption Efforts in Ukraine.* The Wall Street Journal, 7 December 2017.

by the Polish Press Agency (PAP)[42] – the then Prime Minister Arseniy Yatsenuk invited a delegation of the CBA in May 2015, stressing that Ukraine wanted to benefit from the experience of the Polish bureau in the fight against corruption and that he counted on CBA assistance in choosing the best anti-corruption measures for Ukraine. The meeting of the Polish delegation with Ukrainian authorities took place in May 2015.

One year later, in May 2016 in Warsaw a memorandum of understanding between the NABU and CBA was signed. It was the first agreement reached by the Ukrainian Bureau with a foreign anti-corruption service. During his visit to Warsaw, the Director of the NABU stressed that the choice was not accidental. His service studied other countries' experiences in fighting corruption, but in the end it decided to follow the Polish model, applied for 10 years. Apart from signing the memorandum, other elements of the cooperation were established, inter alia, frames of investigative, analytical, supervisory, or operational cooperation between the two services.[43]

Signing the agreement on preventing corruption threats in October 2017 was the next step in tightening cooperation between the Polish and Ukrainian organizations. It was connected with the fact that Polish government granted Ukraine a 100 million Euro loan. This financial support is to be spend on improving border infrastructure on the Ukrainian side.[44]

Apart from American and Polish services, the NABU established cooperation with institutions of other countries. The cooperation is possibly not so strong as in case of the cooperation with the FBI and the CBA. Nevertheless, it is worth pointing out that the level of corruption in Poland, let alone in the US, was never so high like in Ukraine and not all means used by the services to fight corruption are adequate to situation in this country. In view of this, the Director of the NABU established official cooperation with the Specialized Investigation Service, Lithuania and the National Anticorruption Directorate (DNA) at the Prosecutor's Office, Romania.[45]

Only outwardly we may seem surprised at cooperation between the Ukrainian Bureau and Hong Kong Corruption Independent Commission Against Corruption. First of all, the institution has a vast experience, it has been functioning since 1974, which can have an educational dimension for Ukrainian side. Second, from a pragmatic point of view it should be pointed out that, according to the NABU, 15 759 million USD from corruption offences was transferred to Hong-Kong. At present, a proper memorandum of understanding is being prepared, like those already signed by the NABU.[46]

It should also be noted that the NABU cooperates not only with services from other countries, but also with international organizations dealing with corruption.

[42] www.pap.pl, *Ukraińcy chcą walczyć z korupcją*, [access: 7 I 2018].

[43] www.pap.pl, *Memorandum o współpracy polskich i ukraińskich służb antykorupcyjnych*, [access: 7 I 2018].

[44] www.antykorupcja.gov.pl, *Umowa CBA i ukraińskiego NABU* [access: 7 I 2018].

[45] www.nabu.gov.ua, *NABU will strengthen cooperation with the Special Investigation Service of the Republic of Lithuania* [access: 7 I 2018].

[46] www.nabu.gov.ua, *NABU will strengthen cooperation with anti-corruption agencies of Hong Kong* [access: 7 I 2018].

Cooperation with Europol is one of the priorities for the Bureau. Within the framework of the cooperation common investigation teams are created to fight trans border crimes, which is really important when the money is transferred beyond Ukraine. According to the Bureau the money is transferred to 41 countries.[47]

Influence of the National Anti-Corruption Bureau of Ukraine activities on internal security of Poland

Since the beginning of its establishment in 2015, the NABU have arrested 149 persons in connection with corruption offences in 461 cases. The Bureau established that during that time the country lost more than 3 billion USD because of corruption offences. It is a huge amount of money for a country in crisis, taking into consideration the fact that almost all corruption offences are committed by nationals of the country.[48]

In spite of the inefficient fight with corruption by the present Ukrainian authorities, it seems that the future of Ukraine will depend on changes in this area. It is with close connection with politics of conditionality applicable by the West. It seems that the one and only effective solution is to make financial aid conditional on further reforms, mainly fighting with corruption. Struggle with corruption in Ukraine is the only chance to come out of the crisis. Lack of changes would mean further plundering of the country assets by rulers, and in the end it would lead to a collapse of the country.[49]

Security of Ukraine is strongly linked to security of Poland. Possible deepening of the crisis in the country can have negative effects on the internal security of Poland in several areas.

Exports by Polish companies to Ukraine in 2017 was at the highest level since many years. According to the Main Statistics Office (GUS), it amounted to 8 877 million PLN only in the first half of 2017, and in comparison to the same period of time in the last year it increased by 41%. According to reports by GUS, this increasing tendency in exports to Ukraine has been more and more visible since the change of power in the country in 2014. We cannot ignore the fact that it is the time when Ukrainian reforms started, including combating corruption offences, which made the country more interesting for Polish companies.[50]

Marcin Lis, the editor of money.pl, informed that by the end of 2017 there will have been 2 million Ukrainian citizens employed legally in Poland, and by the end of 2018 the number will have increased up to 3 million.[51]

---

[47] www.nabu.gov.ua, *The NABU will cooperate with Europol while investigating cross-border corruption offenses* [access: 7 I 2018].

[48] www.nabu.gov.ua [access: 7 I 2018].

[49] P. Kościński, *Problem korupcji na Ukrainie...* .

[50] www.businessinsider.com.pl, *Polska wraca na Ukrainę w wielkim stylu. Eksport wystrzelił* [access: 7 I 2018].

[51] www.money.pl, *Za rok w Polsce będzie pracować 3 mln Ukraińców. Ich pensje rosną szybciej niż przeciętne* [access: 7 I 2018].

Indirect reason for such a big number of migration is the phenomenon of corruption, which stops development of the country and makes its citizens to seek job abroad. The editor, Lis is of the opinion that it is a positive piece of information from the perspective of Polish economy. He also notices that together with the influx of so many Ukrainians to Poland, the problem of the so called grey economy, viz., illegal employment grows as well, which poses a risk to the economic security of the country.[52] The influx of so many citizens of Ukraine, which has been expanded significantly in a relatively short time, made the risk of criminal offences by migrants higher.[53] It is worth noting that citizens of Ukraine more often commit offences against economy of the country, mainly extortion of VAT.[54]

Having in mind the significance of Ukraine as a large country in crisis, in the vicinity of Poland it should be obvious that its future is strongly linked to the security of Poland. Economic ties, the number of Ukraine citizens and geopolitical significance of the country, determine support for Ukraine in reforms to improve its situation. Having also in mind that currently the NABU is the only independent institution assigned to struggle with corruption offences in the country, western services should give as much assistance as they can. Apart from financial aid, western institutions should first and foremost influence Ukrainian politicians, who seem to be the biggest problem in the fight with corruption at the moment.

By induction by meaningful analysis of source materials it was confirmed that the quality of the NABU activities is dependent on its cooperation with western services and its effectiveness has direct impact on the level of security in Ukraine. This causal link influences the internal security of Poland as a result of the geopolitical location of Ukraine and the effects of internal crisis in that country.

Abstract

Events related to the so-called Euromaidan led to a change of power in Ukraine, and, consequently, to the country's turning to the west. The newly elected authorities were forced to take appropriate measures to combat the problem of corruption. It was a condition for Ukraine to receive financial support from the European Union and the United States. The problem of corruption is one of the main reasons for the stagnation of this country. In 2014, institutional foundations were created in Ukraine to fight corruption, including the National Anti-Corruption Bureau of Ukraine. It is the only independent body operating in the Ukrainian state, intended to fight corruption. The destabilization of Ukraine resulting from the violation of law by the highest-ranking politicians and officials brings consequences for Poland as a Western neighbour and

[52] www.businessinsider.com.pl, *Brakuje rąk do pracy, a problem pogłębia szara strefa* [access: 7 I 2018].

[53] www.antykorupcja.gov.pl, *Handel lewymi fakturami* [access: 7 I 2018].

[54] www.antykorupcja.gov.pl, *Handel lewymi fakturami* [access: 7 I 2018].

the entire region of Central and Eastern Europe. The decline in security in Ukraine results, inter alia, in emigration of citizens of this country, mainly to Poland, which affects directly its internal security. Supporting the activities of the National Anticorruption Bureau of Ukraine in the fight against corruption in Ukraine lies in the interest of the European Union and the United States.

Keywords: corruption, internal security, Poland, Ukraine, secret service.

Krzysztof Izak

What happens after the Islamic State of Caliphate is destroyed? Current state and trends in global terrorism threats

The name the Islamic State of Caliphate in the title of this article requires some explanation. Although it may seem inconsistent or even wrong from the semantic point of view, it is the most appropriate though. It is one of the names one can come across in personal, administrative or military documents of the Islamic State. On 29 June 2014 ad-Dawlah al-Islamiyah fi al-Iraq wa-sh-Sham – Daesh, the Islamic State of Iraq and the Levant/Sham – ISIL/ISIS proclaimed itself to be a caliphate. From that moment on the name ISIL or ISIS was not applicable any more. The name ad-Dawlah al-Islamiyah fi al-Iraq wa-sh-Sham (Islamic State – IS) was introduced instead without any geographic references. This way two structures appeared under the name of Islamic State, one was an organization, the second was a state. In spite of this, as if to minimize the event and its consequences, journalists and politicians have still been using acronyms of the organization from before June 29, 2014. After central and local administration had solidified in the provinces the Islamic State issued thousands of documents with Arabic or English inscription "Islamic State", or "Caliphate", or even "Caliphate of the Islamic State", or "Islamic State of Caliphate". The last inscription was located on passports of the self-proclaimed state, described in literature as "proto-state" as it is very hard to describe this new political and territorial structure as something more.[1]

In mid-October 2017 the Syrian Democratic Forces – SDF captured Raqqa in eastern Syria, the capital city of the caliphate. The bombardment lasting many weeks preceded the assault on the city which had weakened the IS fighters' morale and their operation capabilities. Despite promises of terrorists liquidation in Syria by Western politicians and servicemen, several hundreds of IS fighters and their families escaped from Raqqa. They were evacuated on the basis of secret agreement with the SDF General Command which allowed to decrease the number of victims on both sides of the conflict and among civilians. A convoy of vehicles several kilometers long left the city. The Kurds, who constituted the core of the SDF, supplied it with some vehicles. There was weapon, including heavy weapon and huge amounts of ammunition and explosives on the heavy goods vehicles. There were no black flags over the convoy and that is the reason it was not attacked by drones or aircraft. It is hard to believe that the command of the American forces and their allies leading air operations and special operations in Syria did not have any knowledge

[1] A. Wejkszner, *Państwo Islamskie. Narodziny nowego kalifatu?*, Warszawa 2016, pp. 41–49, opts for the name „proto-state" and not a state with its attributes. He lists factors in favour of such terminology as far as the Islamic State and other jihadist proto-states established since 1989 by different extremist Islamic organizations in the Muslim world are concerned.

of the event. The town of Deir az-Zaur, still under the IS, was the destination. Syrian forces took it over only at the beginning of November but IS fighters still controlled the western part of the Iraqi province Al-Anbar with cities of Rava and Al-Kaim. Reportedly, a few days after leaving Raqqa, the manhunt for runaways started. This delay was enough for fighters to spread out and attempt to cross the border with Turkey. The traffickers demanded 600 USD per person and at least 1,500 USD per family to get them over the border. Some of the fugitives got into the hands of Turkish security forces, which had turned a blind eye when the foreign fighters headed into the opposite direction. Now they wanted to take advantage of the turmoil and get to their home countries via Turkey. Probably we shall never know how many of them managed to do so. But the journeys of jihad volunteers to and from Syria and Iraq had taken place since 2012. Since then, according to the American analytical center, The Soufan Center (TSC), in the fights attended ca. 40,000 volunteers from outside of Syria and Iraq and neighboring countries. They represented more than 100 countries (other sources quote more than 80 countries). The greatest number of volunteers came from Tunisia – more than 6,000. When it comes to Europe, the greatest number of fighters who joined caliphate troops came from the Russian Federation – almost 3,500, then from France – more than 2,000, the UK and Germany – 1,000 each, Belgium – ca. 500, Sweden – more than 300. Several hundreds of fighters came also from Albania, Bosnia, Denmark, Spain and the Netherlands.[2] According to different sources, from 100,000 to 120,000 jihadists could have taken part in the fighting in Syria and Iraq. In August 2014 it was already assessed that 80,000 fighters were affiliated with the IS, including 50,000 fighting in Syria and 30,000 in Iraq. According to general Valeriy Gerasimov, the commander of the Russian army, the IS had a well-organized and commanded army which was headed by former officers of the Iraqi army and many fighters and commanders had been trained by trainers from the Middle East countries. The Islamic State had ca. 59,000 people in arms, including ca. 2,800 from Russia, 1,500 tanks and 1,200 cannons. Their way of acting and tactics indicated that it was more like a regular army than a group of terrorists. Nowadays they return home, mostly to Libya, Afghanistan and South-Eastern Asia.[3] It is known the identity of ca. 20 Polish nationals, individuals of Polish origin living abroad or having a stay permit in Poland, who had stayed in the conflict zone for a longer or shorter period of time or supported the IS in any other way.

In March 2016 the *Sky News* television station possessed a memory card with data of more than 22,000 jihadists from the Islamic State. They got it from a certain Abu Hamid, who had belonged to the Free Syrian Army, then joined the IS. He had stolen the memory card from the chief of intelligence and security service

[2] http://thesoufancenter.org/wp-content/uploads/2017/11/Beyond-the-Caliphate-Foreign-Fighters-and-the-Threat-of-Returnees-TSC-Report-October-2017-v3.pdf [access: 29 X 2017].

[3] https://wiadomosci.wp.pl/rosyjska-armia-jest-coraz-bardziej-niebezpieczna-to-juz-nie-sa-uprzejme-zielone-ludziki-6203212097816193a [access: 28 XII 2017].

of the organization, Abu Luqman as-Suri. Then, with his haul, he defected further to Turkey. The memory card contained application forms with 23 questions. Apart from their names and surnames candidates put there their phone numbers, information on their families, their educational background, their combat experience and their knowledge of Sharia law. They also provided information on the people who had given them recommendation for the Islamic State. They could also declare readiness to take part in training for suicide bombers. According to the *Sky News*, some of the names were well known before but new documents could help in identification of extremists from countries whose authorities had been totally unaware of their existence. The forms were filled in by volunteers from 51 countries, including the UK, some countries of northern Europe, the USA, Canada and from North Africa and the Middle East countries. Also, *Süddeutsche Zeitung* daily magazine together with German regional public TV stations NDR and WDR informed about the leak of secret personal data of the IS fighters claiming that they managed to look into several dozens of forms with German jihadists data. The forms had been filling in for entry to Syrian territory possessed by the IS. Representatives of German services informed that the data regarded also Germany nationals known to them, who had not been charged because of the lack of evidence that they had joined the IS. The documents did not contain photos of foreign defenders of the caliphate, unlike the forms filled in by local fighters from Syria and Iraq, to which photos were attached.

According to the European Counter Terrorism Centre – ECTC data at the end of June 2017, there were ca. 5,000 EU citizens who had joined the IS in Iraq and Syria (other sources say more than 6,000), 1,650 returned, although the number of returnees is lower than expected. According to the ECTC, most of the returnees to Europe were detained or have been under surveillance in their home countries. It was pointed out that there is a need for closely monitor a flow of terrorists and observed in 2017 an increase of women and minors among those who were recruited by terrorist organizations. There has also been observed an increase of terrorists influx to destabilized countries like Libya, Somalia and Yemen.[4]

Current state of play resembles the situation at the end of the 1980s, the beginning of the 1990s, when the war in Afghanistan ended Mujahedeen returned to their home countries (in Afghanistan in the 1980s there were ca. 20,000 foreign fighters) joining radical organizations there or establishing new ones and taking the lead in them. The examples are: Abu Sayyaf in the Philippines, Jemaah Islamiyah in Indonesia, Lashkar-e-Taiba in Pakistan, Al-Jama'at at-Tawhid va al-Jihad in Jordan, Al-Jama'a al-Islamiyya al-Mukatila bi Libia in Libia, Al-Jama'a al-Islamiyya al-Mukatila fi Tunisiyya in Tunesia or Al-Jama'a al-Islamiyya al-Musallaha in Algeria. A large number of Afghan veterans participated in the war in Bosnia and Herzegovina between 1992 and 1995 (there were between 2,000 and 5,000 foreigners fighting in Bosnia and

[4] https://businessinsider.com.pl/wiadomosci/dzihadysci-w-europie-ilu-wrocilo/ldczlxw [access: 30 VI 2017].

Herzegovina), after which they got a citizenship of the country. They also took part in the bloody civil war in Algeria which started in 1992 and lasted almost to the end of the 1990s. One of its effects was establishing Al Qaeda branch in Maghreb. Nevertheless, while those who had been returning from Afghanistan to their home countries were greeted as heroes, at present those foreign fighters who are returning from Syria have to count with the possibility of being arrested and charged with taking part in terrorist organization of armed nature and mass murders. Times have changed, international situation as well but terrorist threat initiated years ago by Afghan veterans, has become disproportionately high nowadays in comparison to that in the past. It is *inter alia* the reason why there is a dispute over returnees in the EU. The idea of their elimination there on the spot in Syria has appeared utopia. In the past the CIA carried out a selective elimination of Al Qaeda members and its affiliates with the attacks from the air. In the case of the Islamic State it was not so easy though. The British Defense Minister made a decision to intensify airstrikes in order to eliminate British nationals fighting for terrorist organizations. Asked whether some of the British nationals should have the chance to come back home, he answered that he did not trust any terrorists. And it did not matter whether the person came from the UK or any other countries. In his opinion a dead terrorist could not do any harm to the country, so British jihadists had no right to come back home. Cooperation with them is tantamount to the death sentence. At that time it was claimed in the UK that those persons who confessed to cooperation with jihadists and hang their heads should be admitted to the country. Some British people think that those people should be judged. Instead of death sentence the country should try to re-integrate them.[5] Although according to others, such re-integration with societies in their home countries means only a waste of taxpayers' money because there is little hope they come back to a regular life. In the article *Restraints and problems in the field of combating terrorism and crimes committed by immigrants in Europe,* published in Internal Security Review No 17 (10), I wrote, *inter alia*, about a dubious effectiveness of de-radicalization programs in the UE.

There is also no shortage of votes against. According to a statistic analysis by Norwegian expert Thomas Hegghammer, historically ca. 11 percent of returnees from jihad pose a terrorist threat. But in the case of the war in Syria this ratio is much smaller – ca. 0,5 percent. As Charles Lister, Brookings think tank expert proves, if these calculations are correct, "soft attitude" makes greater sense than pressure to confine returnees to jails which can cause their re-radicalization and spreading radical ideas to other jail mates. Rehabilitation programs are conducted in some European countries, including Germany, the Netherlands and Denmark. Reportedly some of them have positive effects. For example in Denmark the so called "Aarhus method" is used based on the cooperation with local mosques and assistance in finding a job and education. As a result, none of the 16 jihadists from Aarhus who have gone to Syria

[5] http://wolnosc24.pl/2017/12/07/brytyjski-rzad-kazal-wyeliminowac-wlasnych-obywateli-podejrzanych-o-kontakty-z-isis-licencja-na-zabijanie-szokujace-wyznanie-ministra/ [access: 7 XII 2017].

and returned since 2013, have not committed any serious crime up to now and almost all of them work or study.[6] But it is only one example of this kind whereas statistics regarding such programs in other countries are not known. In the meantime, even if isolated cases from more than 1,600 returnees to the EU appear to be recidivists, the consequences may be major. We have to reckon with even more serious threat in case of jihadists who come back to non-EU countries. TSC, as mentioned above, based on reports from 33 countries, assessed that between March 2016 and August 2017 there were at least 5,600 such returnees, for example, 400 to Russia, 760 to Saudi Arabia, 800 to Tunisia and 800 to Turkey. On the battlefield there might have died from 60,000 to 70,000 caliphate fighters. That is the reason why most countries prefer hard methods while dealing with the problem, even if sometimes there is a lack of evidence to put returnees in prison. In the UK such a solution are the so called TPims (Terrorism Prevention and Investigation Measures) introduced by the Act of 2011, i.e. subjecting suspects to special supervision. According to the law, authorities are able to monitor such radicals' activities, for example, with electronic wristbands and the obligation to report to a police station. The problem is that such attitude is also not 100 percent effective bearing in mind the number of extremists known to services and constant lack of police forces to monitor them. For example, in Germany in 2017 the number of prosecutor proceedings connected to terrorism has increased several times. Many of them regard German nationals returning from Syria and Iraq. In a result investigative officers are overworked and prosecutor's offices suffer from a lack of manpower. That is why another approach is proposed, that is leaving alone at least a part of those who have returned. First and foremost, those who had left as naive teens, possibly brainwashed and now return with a feeling of total disappointment. Such a strategy is used by the British counterintelligence, MI5.[7] It remains to be seen whether it is right .French services announced that there are already children who were born in the territories under the IS and those who had left France with their mothers in the country. They are traumatized by war, some were used for propaganda purposes, some were trained how to use weapons or were indoctrinated, some watched executions or even carried them out by themselves. Footage with such scenes spread on the web.

Presence of jihadists from the Islamic State in Europe poses a terrorist threat to residents of our continent. Its scale will be growing together with the refugees and illegal migrants influx, not only from Asia, but also from African countries. Despite the collapse and destruction of the IS administration structures, their military forces and gaining control over territories formerly under the IS in Iraq and Syria, the future

[6] http://trybun.org.pl/2017/08/10/dania-w-miejscowosci-aarhus-rusza-program-przytul-terroryste/ [access: 10 VIII 2017].

[7] http://www.bbc.com/news/world-middle-east-41734069[access:26X2017];https://wiadomosci.wp.pl/ dzihadysci-wracaja-do-europy-nie-wiadomo-co-z-nimi-zrobic-6180903806875777a [access: 26 X 2017]; https://wiadomosci.wp.pl/czy-terrorysci-moga-byc-resocjalizowani-wielki-spor-o-powracajacych-dzihadystow 6193366738753665a [access: 30 XI 2017].

of the two countries is a big if. On 9 December 2017 the Iraqi Prime Minister Haidar al-Abadi announced victory over the IS. It was not the first time the PM had made such an announcement. They were also made after Mosul, Tel Afar and Al-Havijja were recaptured from jihadists, nevertheless the fighting went still on. The last operation by Iraqi forces in western part of Al-Anbar province means total failure of caliphate in Iraq. Its troops were cut off. Recapture of jihadists positions along the border between Syria and Iraq was the element of purging the province from the IS – the last territory under IS control in the country. Fighting in Iraq caused huge losses. Only during the operation of Mosul recapture, from October 2016 to July 2017, 23,000 Iraqi soldiers died and the number of wounded was three times bigger than the death toll. In addition, from 9,000 to 11,000 civilians lost their lives and material losses amounted to 3 billion USD. In addition to this there are tons of used ammunition, damaged weapon and thousands of vehicles.[8]

Military victory over the Islamic State in a battle does not mean defeating the terrorist organization, members of which will move on to conspiracy and will still carry out attacks. The caliphate certainly had its supporters among the inhabitants of recaptured cities, mostly among former officers of the Iraqi army and intelligence and security services from the times of Saddam Hussein. Owing to them IS fighters achieved spectacular victories. Many of them and also privates certainly survived the last 18 months of military operations, during of which almost all controlled territory was lost. They have also many sympathizers among Sunni minority in Iraq, they can count on their support and assistance in their conspiratorial activities. Terrorist attacks in cities and districts dominated by Shiites are a manifestation of their activity. And this particular Sunni and Shiite conflict, although on a minor scale, but carrying destruction and victims will mark the immediate future of this country.

In Syria the situation is much more complicated. Apart from regime forces, SDF forces led by Kurds are extremely active. Their opponents are not only IS fighters but also Harakat Ahrar al-Sham al-Islamiyya with its allies, and Hayat Tahrir ash-Sham, i.e. former Jabhat an-Nusrah li-ahli ash-Sham, subsequent Jabhat Fateh ash-Sham (a Syrian branch of Al Qaeda, which reportedly broke with it and after merging with other smaller groups on 28 January 2017 became OWL[9]). Those two organizations, fighting in the past together against regime forces and the IS, over the last year fought battles between each other interspersed with talks, truces, or common operations in case of threat from a common enemy. OWL has still control over the territory of Idlib and Hama provinces, which are targets of air attacks by the governmental forces. There are also other smaller groups fighting in Syria for the last couple of years creating more or less permanent alliances. However, under the guise of religious or national ideology ordinary criminal activities were often hidden. The number of all organizations and military groups active in Syria and Iraq since 2012 is estimated to be between 300

[8] http://gpcodziennie.pl/77109-ogromstratwwalceomosul.html [access: 27 XII 2017].

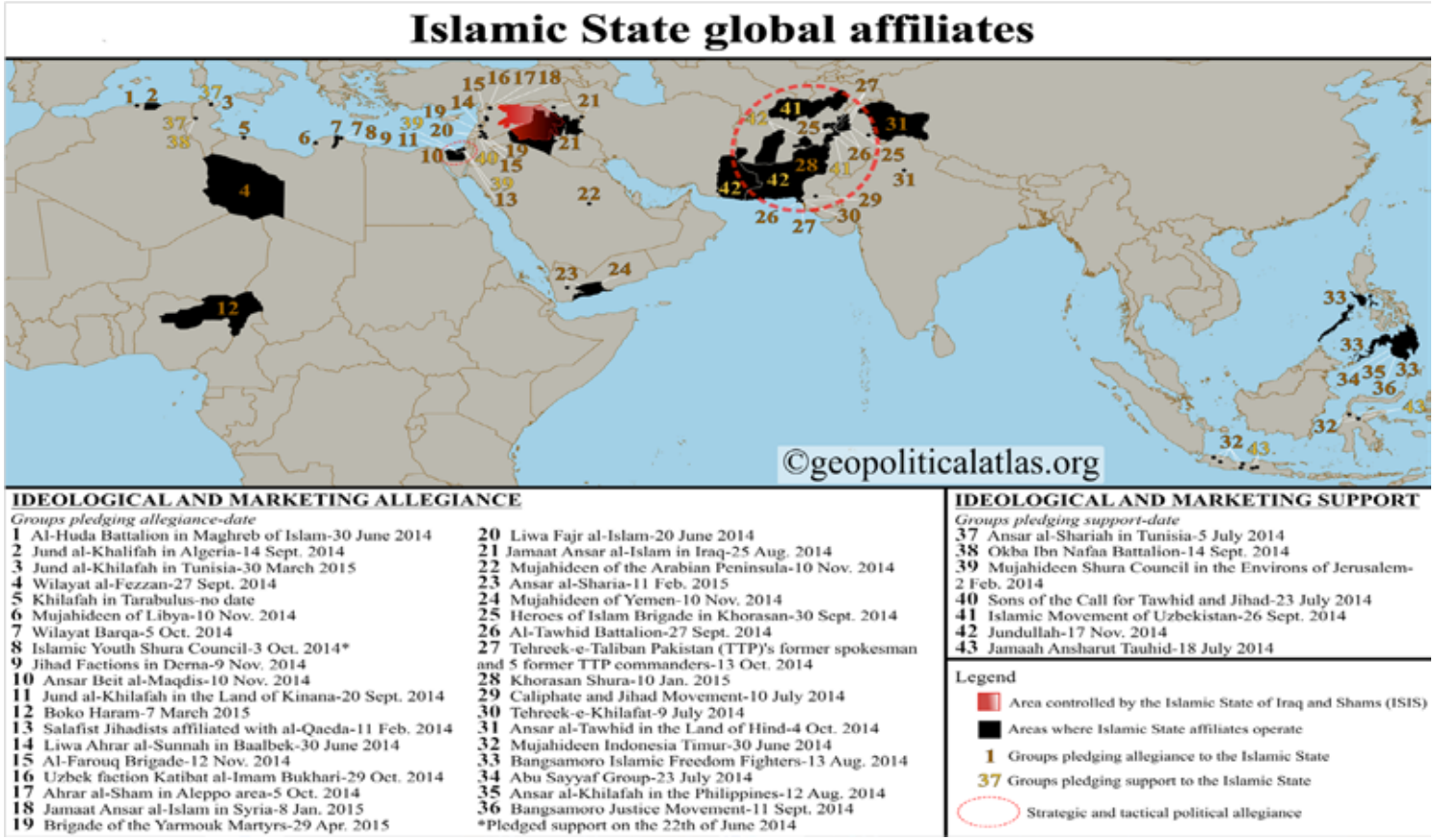
[9] M. Weiss, *H. Hassan, ISIS. Wewnątrz armii terroru*, Warszawa 2015, pp. 281–326; https://alshahidwitness.com/ identifying-hts-syria-revolution/ [access: 6 VI 2017].

and 800. In February 2016 only almost 100 groups composing the Free Syrian Army and the so called armed opposition agreed for American and Russian ceasefire agreement, which was anyway broken soon.[10] Therefore, it is very hard to consider that the IS liquidation in Syria is going to bring peace in the country. Religious and ethnic divisions and contradictory interests of Russia, the US and Western countries will fuel domestic conflicts and facilitate destabilization in the country and its territorial dismantling.

Organizations allied with the Islamic State and operating in foreign vilayahs (provinces) of the caliphate, i.e. on the Sinai Peninsula, Libya, Nigeria or Afghanistan, are still active. Other groups, leaders of which between 2014 and 2015 had sworn allegiance to caliph Ibrahim (Abu Bakr al-Baghdadi)[11] are also active. The groups used to be linked to Al Qaeda or its affiliates. There were more than 40 of such organizations. Some of them got divided following internal arguments concerning taking the side of either Al Qaeda or ISIS, feuding with each other since 2013. Initially this change of alliances was not clear. Only the analysis of information published by the groups in the cyberspace allowed to identify those who "had betrayed" Al Qaeda (Pic.1 and Pic. 2). Those organizations which had "Al Qaeda" in their names took its side, and the Somali Harakat al-Shabaab al-Mujahideen to name the most important ones. Further in the article those groups' activities are briefly described in the face of growing competition from the ISIS/IS and its allies. It should be mentioned at this point that at the beginning of September 2014 Ayman al-Zawahiri announced establishing of the Jamaa'at Kaidat al-Jihad al-Karrah al-Hindiyyah. One month later the Al-Ansar-ut Tauhid fi Bilad al-Hind group issued an official statement with declaration of loyalty to the Islamic State. It also called for attacks on western nationals staying in India. The attacks were supposed to be a retaliation for activities of the international coalition against the Islamic State.

[10] https://www.polskieradio.pl/5/3/Artykul/1587568,Syria-100-ugrupowan-opozycji-przystapi-do-rozejmu [access: 26 II 2016].

[11] More on caliph Ibrahim in: S. Laurent, *Kalifat terroru. Kulisy działania Państwa Islamskiego*, Warszawa 2015, pp. 109–125; J. Warrick, *Czarne flagi. Geneza Państwa Islamskiego*, Warszawa 2017, pp. 356–377.



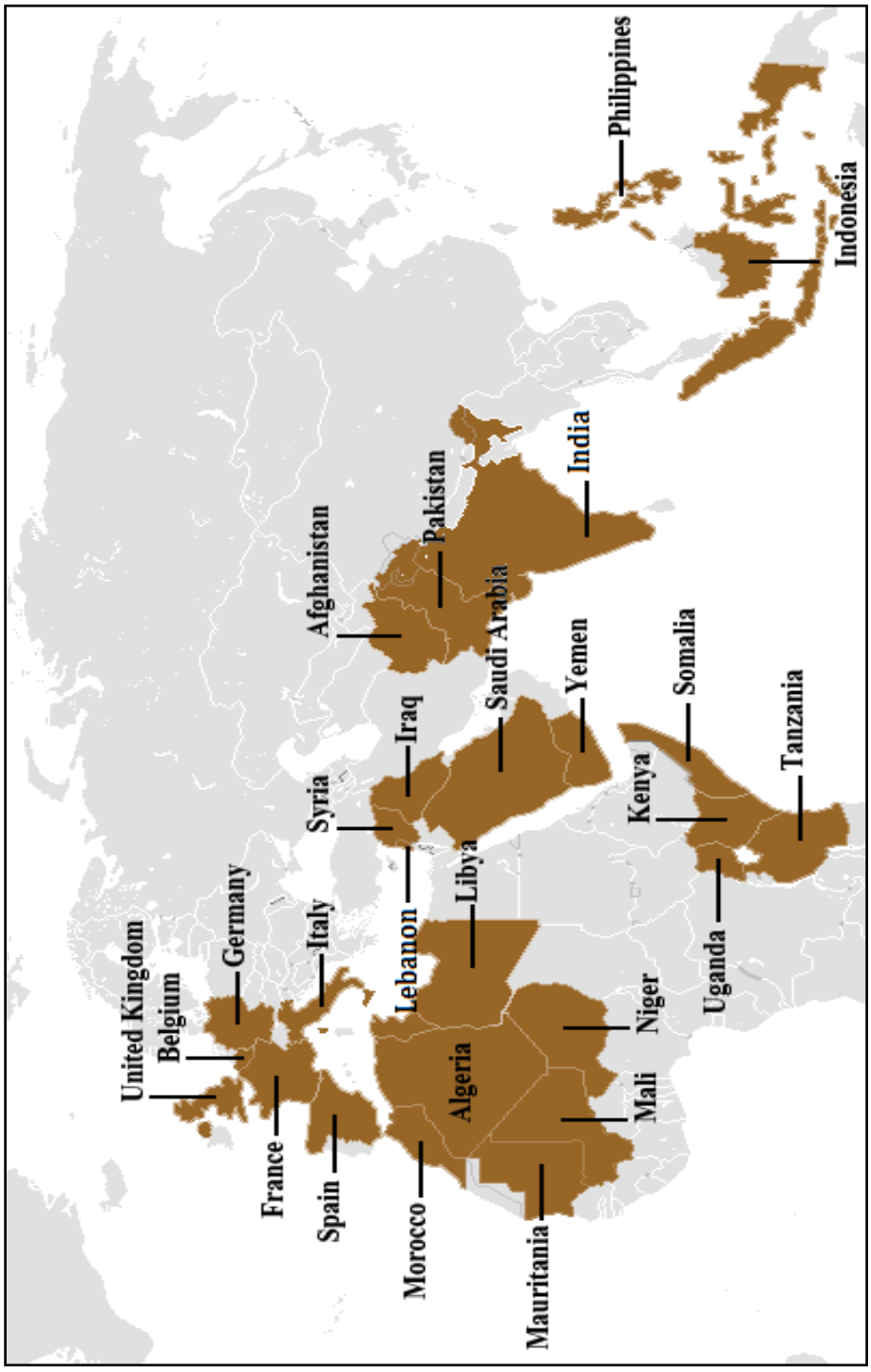
Pic. 1. Muslim extremist organizations allied with the Islamic State. Together with the name of the organization the date of baja, oath of loyalty to caliph Abu Bakr al-Baghdadi or its announcement.

Source: https://intelcenter.com/maps/is-affiliates-map.html#gs.mm1jPv0 [access: 4 III 2016].

Ideological divisions between Al Qaeda and the IS are much more complicated and according to the author they will influence the security of many countries worldwide. Because of that they require much more attention. Marc Sageman in his book *Sieci terroru* defines and describes the idea of a close and distant enemy and the idea of local and global Salafi jihad by Al Qaeda.[12] This discrepancy between strategies had its supporters and opponents, which led to significant fractures between different radical groups linked to Osama bin Laden organization. Some of them were rather interested in local activities, for example in gaining and maintaining influences in their own region or country. Despite the fact that some Muslim theologians accepted the idea of a global jihad, which Osama bin Laden supported , the majority of radical religious scholars opted for the necessity of Muslim territories defense against foreign intervention. There were also significant discrepancies in the treatment of Shiites. Al Qaeda leaders were for example against a strategy of jihad supported by Abu Musab al-Zarakwi which assumed primarily starting a civil war between Sunnis and Shiites in Iraq. They acknowledged that the priority is to concentrate on fights against Americans and their allies. For the ISIS/IS Shiites are natural enemy that should be destroyed. Al Qaeda's strategic goals were characterized by hostility to the US and Israel, which was announced in a fatwa issued on 23 August 1996 declaring war on "Americans occupying the Land of two Holy Places" and confirmed on 23 February 1998 by establishing the World Islamic Front for Combat Against the Jews and Crusaders.

After the death of Osama bin Laden on 2 May 2011, his successor Ayman al-Zawahiri decided to concentrate on close enemies, particularly pro-western regimes in North Africa and the Middle East. From the documents found in bin Laden's Pakistani haven one could recognize significant differences of opinion between himself and his successor as far as priority terrorist attacks goals were concerned. While bin Laden was ready to attack Americans on their territory, al-Zawahiri rejected the idea, claiming that the US territory was simply too well secured. The Islamic State defended and widened the control over Iraq and Syria and, at the same time, it did not hesitate to strike wherever possible because it had bigger financial and logistic and military means as well as operational, propaganda and recruitment possibilities. In the context of the Islamic State activities, Ayman al-Zawahiri strongly rejected any form of an usurped caliphate or any attempts to impose supervisory and creating caliphate with force. He proposed restitution of caliphate by evolution not revolution. At the same time, the present leader of Al Qaeda strongly condemned terror methods used by the IS fighters towards Muslims living on territories in Iraq and Syria under self-proclaimed caliphate supervision. Unlike the Islamic State, bin Laden and al-Zawahiri mentioned the idea of caliphate in the long term perspective and treated it as a kind of mobilization factor than the task to be accomplished in the near future. It is also worth noting the clear difference between the scale of planning by political

[12] M. Sageman, *Sieci terroru*, Kraków 2008, pp. 21–74.



Pic. 2. Al Qaeda net.

Source: https://en.wikipedia.org/wiki/Al Qaeda [access: 4 III 2016].

and economic institutions of the West and the time horizon of Al Qaeda strategy. Based on its presumptions short term goals should be achieved during decades, while a long term plan of establishing the caliphate can take from 50 to 100 years.[13] Artur Wejkszner, one of the researchers in this problem area, also tries to answer the question when Al Qaeda's caliphate is established, giving different scenarios.[14] Since, there is nothing to prevent two caliphates from existing alongside. In the tenth and eleventh centuries there were even three caliphates alongside one another: the Abbasid Caliphate with its capital in Baghdad, the Fatimid Caliphate with its capital in Cairo, and the Umayyad Caliphate with its capital in Córdoba.

Terrorist competition between the Islamic State and Al Qaeda[15]

Announcement of the Islamic State in June 2014 as a territorial entity and organization of global Salafi jihad meant a significant change on the map of Islamic terrorism, against which the US and allies have been waging a war for 15 years. The IS deprived Al Qaeda of the role of the key terrorist organization in the world. It filled the ideological and logistical void after the significance of Al Qaeda decreased. The IS also took over most of its sponsors, members and influence. Furthermore, it demonstrated more dynamics, brutality and operational abilities. The proclamation of the caliphate led to confrontation between the IS and al Qaeda, and competition for money, fighters, prestige and popularity. The competition came mainly from personal animosities between leaders of the two structures and took different forms, for example, fights in Syria between the IS and Jabhat an-Nusra li Ahl ash-Sham and its further incarnations and allies, contradictory information on the mastermind behind attacks, competition for influence, killing leaders of the opposite side, or mutual discrediting in the media.[16]

In this confrontation Al Qaeda lost its monopoly and its influence rapidly declined. Apart from Al Qaeda and the IS there are also other active Islamic extremists groups. Their activities cause sometimes deep differences between state authorities' positions. The Muslim Brotherhood (al-Ichwan al-Muslimin) movement is a good example. Like the Islamic State and Al Qaeda, it is a transnational organization, active in many Muslim countries and in Europe (organizations linked to the Muslim Brotherhood are often independent structures). At present the organization is considered a terrorist organization by some Islamic countries: Egypt, Saudi Arabia and the United Arab Emirates (other countries allow its activity or just tolerate it). The UAE has put on the list of terrorist organizations also most institutions and groups linked to the Muslim Brotherhood acting in Europe autonomously and recognized by some governments

[13] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*, Warszawa 2017, pp. 174–175.

[14] A. Wejkszner, *Globalna sieć Al-Kaidy. Nowe państwo islamskie?*, Warszawa 2017, pp. 332–342.

[15] Information on the events in Africa and Asia in this part of the article come from the electronic media. Only the most important for this article have been mentioned.

[16] S. Wojciechowski, P. Osiewicz, *Zrozumieć współczesny terroryzm*…, p. 206.

of the EU countries as a representation of Muslim society. Saudi Arabia officially fights the IS but unofficially it supported them financially and military. Most terrorist organizations are inspired by Salafist doctrine.[17] As a rule Salafis reject democracy and election process as inconsistent with sharia. They also reject secular law as inconsistent with the Koran and strive for implementation of Koranic law as the only source of the law. Salafi groups do not create a homogenous block in the Muslim world, they have different international links (mostly with competing with each other Qatar and Saudi Arabia), and sometimes despite their opinions on democracy and elections take part in elections (for example, in Egypt). Wahhabism as one of the Salafism branches forms the ideological and religious foundation of Saudi Arabia. Owing to the money from the Kingdom this formerly vestigial Islamic group managed to expand in the last decades of the twentieth century and at the beginning of this century forming a foundation for both Al Qaeda and the Islamic State.

Apart from the Middle East, the main arena for activity and competition between jihadist groups is North Africa embracing Sahara and Sahel countries where, since the second half of 2014, the Islamic State has expanded its influences. Provided the Islamic State was defeated in Syria and Iraq, its position in Africa has also been weakened and the organization lost control over formerly supervised territories, for example, in Libya where, since July 2017, the IS has not controlled the middle part of the coast (the IS Sirte wilayyat) and the borderland of Tunisia. Though, it is still capable to carry out terrorist attacks. In North Africa one of the most important terrorist structures is Tanzim Qaedat bi-Bilad al-Maghrab al-Islami (The Organization of Al-Qaeda in the Islamic Maghreb – AQIM), linked to Al Qaeda. Following the disintegration of the Republic of Mali in 2012, The Organization of Al-Qaeda in the Islamic Maghreb took over almost all the northern territory of the country, including the cities of Timbuktu and Gao. This way Al Qaeda in the Islamic Maghreb was able to create an Islamic state structure in Africa. The new administration with the radical version of the Koran was introduced, ancient buildings were destroyed, including mausoleums, old documents and tribal art artefacts.[18] The leader of the organization

[17] *Salafiyya* – religious and political stream in Islam referring to the first generation of Muslims (*as-Salaf as-Salih* – pious predecessors). It comes from the belief that only strict following the established tenets presented as the rules established by the Prophet Muhammad once and for all following the Revelation can restore Islam the position of the first power in the world lost after walking away from the Koran. The ideology was developed in the late 19th and the beginning of 20th centuries by Jamal al-Din al-Afghani, Muhammad Abduh and Rashid Rida. It calls for rigorous law, praises strict orthopraxy (getting dressed like the Prophet Muhammad, wearing long beards, sleeping on the right side on the mat and so on). *Fatwas* are formulated according to s*alafiyya* rules in a strict way. They refer only to the sacred text of the Koran and *sunnah*. At the same time they disregard European social context (often demonized) when compared to norms of the Islam world. *Salafiyya* is divided into three categories: quietist, political, and jihadist.

[18] In August 2016 Ahmed al-Faqi al-Mahdi, leader of Ansar Dine militia pleaded guilty in the International Criminal Court for the war crime of attacking religious and historical buildings in the city of Timbuktu which were World Heritage Sites. Al-Mahdi pleaded guilty to the charges of destroying the monuments. He had ordered to destroy nine mausoleums from the XIth and XIIth

Abdel Malek Droukdel alias Abu Musab Abdel Wadoud ordered a slowdown in the pace of changes and expansion in order not to discourage local people and not to provoke any foreign intervention. However, one of the weaknesses of the new Islamist state was the internal competition between the leaders. Apart from AQIM, there were also other groups active like Ansar Dine, based on radicalized Tuaregs in Kidal, and Jamaa'at at-Tawhid va al-Jihad fi Gharbi Ifrikiyya, Mouvement pour l'Unicité et le Jihad en Afrique de l'Ouest – MUJAO, based in Gao embracing Sahrawi people (indigenous people of the Western Sahara, whose political interests have been represented by the Polisario Front for many years), local Arabs and Songhai people (one of the biggest ethnic groups in northern Mali). Mokhtar Belmokhtar, one of the AQIM leaders, antagonized with Droukdel, at the end of 2012 established his own group called Al-Mulathameen Brigade (Brigade of the Masked Ones), also known as the al-Mua'qi'oon Biddam (Those who Sign with Blood Brigade). Following the French intervention in Mali, on 16 January 2013, the organization attacked Amenas gas facility taking more than 800 people hostage, including 132 foreigners. According to terrorists, it was a revenge for French attacks on jihadists positions in Mali. After a 4-day siege the facility was recaptured by the Algerian special forces and the hostages were released, although 39 of them were killed. After the attack on Amenas Mokhtar Belmokhtar became one of the most wanted terrorists. On 22 August 2013 the leader of MUJAO, Ahmed al-Tilemsi together with Mokhtar Belmokhtar joined their groups to form Al Mourabitoun group (The Sentinels). The leader of Al Qaeda, Ayman al-Zawahiri backed strongly the fusion. An Egyptian, Abu Bakr al-Nasri led The Sentinels group. After his death in April 2014 Ahmad al-Tilemsi took the leadership of the group, with Belmokhtar's consent. In December 2014 al-Tilemsi also died. While Belmokhtar was away, one of the former deputies of al-Tilemsi, Adnan Abu Walid al-Sahraoui declared himself the leader. Belmokhtar did not accept him. In May 2015 al-Sahraoui declared alliance with the Islamic State, however, a few days later Belmokhtar rejected it, and accused the IS of killing innocent Muslims, and pledged allegiance to Ayaman al-Zawahiri, the leader of Al Qaeda. On 14 June 2015 Libyan authorities informed that Belmokhtar was killed during American airstrikes inside Libya. Nevertheless, no concrete evidence was presented. In January 2016 the US State Department removed Belmokhtar from the list of terrorists.

Despite activities of French troops and the United Nations Multidimensional Integrated Stabilization Mission in Mali (MINUSMA), AQIM still poses a serious threat. On 20 November 2015, the terrorists attacked Radisson Blu Hotel in Bamako, Mali. Twenty one people were killed. Thirty people were dead and 56 were wounded in another terrorist attack on Splendid Hotel in Ouagadougou, the capital of Burkina Faso, on 15-16 January 2016, by AQIM. On 13 March 2016, terrorists opened fire on guests at Grand-Bassam resort, near Abidjan, the capital of Ivory

centuries and Sidi Yahiya Mosque from the XVth century. In September 2016 he was sentenced to nine years in prison and 2,7 million Euro financial penalty. http://www.tvp.info/27101180/dzihadysta-skazany-na-zniszczenie-zabytkow-w-timbuktu-kierowaly-mna-zle-duchy [access: 27 IX 2017].

Coast. Nineteen people were killed. On 18 June 2017, a group of gunmen attacked Le Campament hotel in Dougourakoro, east of Bamako, Mali, and took 36 people hostage. They were released by special forces. Three attackers were killed. Two months later, on 13 August, AQIM militants attacked visitors to a restaurant and a hotel in Ouagadougou. Eighteen persons were killed and 22 were wounded. Apart from that terrorists tend to attack governmental military forces of Mali and MINUSMA. Jihadists take advantage of the fact that border lines between Mali, Niger, and Burkina Faso are poorly controlled by the military forces of those countries. On 2 March 2017, Jamel Okaha, Iyad Ag Ghaly, Ansar ad-Din leader, Amadou Kouffa, founder of the Macina Liberation Front[19] declared the creation of the Jamaa'at Nusrat al-Islam. Saharan structures of Al Qaeda were loyal to al-Zawahiri, nevertheless in July 2014, there was a fracture in AQIM near Kabyla, northern Algeria. A group under the powerful leader of the organization, Abdelmalek Gouri took an oath of allegiance to caliph Ibrahim adopting the name Jund al-Khilafah fi Ard al-Jazair (Soldiers of the Caliphate in Algeria or Caliphate Soldiers of Algeria). The organization was responsible for kidnapping and killing a French mountaineering guide, Hervé Gourdel, which caused tracking down and killing Gouri by Algerian military. In February 2016 the group killed three Algerian soldiers. At the same time the Tuareg rebellion in the Republic of Mali in 2012 was welcomed by the part of their countrymen from Ahaggar in eastern Algeria and from the Libyan town of Ghat, who established Mouvement des Fils du Sahara pour la Justice Islamique – MFSJI. The militants of the group planned to attack the cities of Hassi Messaoud and Djanet, southeast Algeria. Attacks in northern Algeria target security forces of the state. In February 2017 three policemen were wounded in Constantine and three others were killed in Tijarat in August of the same year. In view of the possible serious attack in the beginning of September 2017 the Algerian authorities raised the level of threat to the highest possible in strategic civilian and military regions, including borderline.[20]

The Islamic State is much more successful in Libya, which is still very far from a stabilized country. An eight hundred-member Islamist unit faithful to the IS was already established in April 2014 in the seaside town of Dernie, and then reinforced with 300 Libyans from Battar Brigade fighting up to that moment in Syria for the IS.

[19] The Macina Liberation front is based mainly on ethnic Fulani shepherds, affiliates of Ansar Dine. Apart from the radical imam Amadou Kouffa, Suleiman Keita was in charge of the group. They are active in Mali and Ivory Coast, where seven members of the group were arrested while preparing the attack in the capital of Mali. In 2015 and 2016 the group organized attacks on representatives of the Mali security forces and international facilities in Bamako and in the Mopti region. On 7 August 2015, it carried out an attack on Byblos Hotel in Sevare, where the UN mission members stayed. Security forces recaptured the hotel the next day. At least thirteen people were killed, including five UN mission workers and four soldiers. Four terrorists were also killed and seven others were arrested; https://www.timesofisrael.com/mali-arrests-suspected-mastermind-of-hotel-terror-attack/ [access: 25 IV 2016].

[20] More on the conflict in the Republic of Mali: K. Danielewicz, *Terroryzm w Afryce. Geneza oraz przebieg konfliktu w Mali w latach 2012–2014*, Oświęcim 2016, pp. 82–151.

In October 2014 these troops overran Derna and Al-Baghdadi sent there Abu al-Bar al-Azdi, a Yemeni to become an emir in the newly established emirate of the Islamic State called Wilayat al-Barqa (Cyrenaica Province). He also sent there his deputy, former general in Saddam Hussein army, Abu Nabil al-Anbari to strengthen the organization's influences in relation to Al Qaeda's competition and other groups. In February 2015 Libyan branch of the IS was empowered even more after the city of Sirt and nearby oil fields were captured. In May 2017 Ansar al-Sharia Libyan organization, affiliated with Al Qaeda, decided formally to dissolve itself. The reason for this was human loss and death of the most important leaders. The group which had been trying to consolidate in eastern Libya was combated both by the self-proclaimed Libyan National Army under gen. Khalifa Haftar, and the troops under the General National Congress. The members of the group called all radical forces of Islam in Libya to form a united front. Ansar al-Sharia claimed responsibility for the attack on a consulate compound and CIA cell in Benghazi on 11 September 2012. Four Americans died at the time, including the U.S. Ambassador Christopher Stevens, Sean Smith, a consulate employee and CIA agents, Tyrone S. Woods and Glen Doherty. On 27 January 2015 a car bomb was detonated at the Corinthia Hotel entrance in Tripoli, some gunmen stormed past the guards and entered the hotel lobby shooting at random people. After the police entered the hotel, terrorists detonated explosive belts. In the attack 11 people died, including 6 foreigners. It is probable that the same perpetrators had attacked the Embassy of Algeria in Tripoli ten days earlier, wounding three guards. In the announcement posted online the IS affiliated militants claimed responsibility for the attack. The attack was supposed to be a retaliation for Abu Anas al-Libi death in an American prison, the mastermind behind the attacks on the US Embassies in Kenya and Tanzania on 7 August 1998.[21] On 23 August 2017 jihadists affiliated with the IS attacked gen. Haftar's troops in the Al-Jufra district in the west of Libya. Nine soldiers, who were taken hostage, were beheaded and two other civilians died. In February 2015, on the beach near one of the hotels in Sirte, 21 of Egyptian Copts working in Libya were also beheaded. The execution was filmed. The bodies of the victims were found at the end of September 2017. Libyan, Mali and Algerian organizations linked to Al Qaeda established their Council in Africa, made up of Al Qaeda Brigade in Sirte, Al Al-Kaka ibn Amr Brigade in eastern Libya, AQIM and Muwaka'un bi ad-Dima in Mali, and several smaller groups from Libya and Algeria, also affiliated with AQIM.

Organizations with Ansar al-Sharia in their name are also present in other African countries: Egypt, Morocco, Mauretania, and Tunisia. These structures did not pledge allegiance to Al Qaeda or the Islamic State. They act locally. Tunisian Ansar al-Sharia showed quite a significant operational activity. Originally following the revolution in 2011, Salafis acted legally under the protective umbrella of the Islamist government led by the Tunisian branch of the Muslim Brotherhood known as Hizb an-Nahda

[21] Abu Anas al-Libi was captured in Tripoli in October 2013 by the American special forces and transported to the USA. He died in hospital while waiting for a trial.

(Renaissance Party). Some Salafi groups tried to establish political parties, most of which rejected democracy from the start. Ansar al-Sharia was blamed for the 2012 ransacking and burning the American embassy in Tunis in response to releasing American film *Innocence of Muslims* regarded as an insult to Islam. During the mob riots four people were dead and many others were wounded. The group was designated as a terrorist organization and outlawed by the Tunisian government after mass demonstrations following the assassination of the two opposition politicians by the organization in February and July 2013. The decision damaged the organization, its members started to act in a conspiracy but it had not been able to recover entirely. It was replaced by the Katibat Uqba Ibn Nafi[22] established in December 2012 on the initiative of the AQIM leader Abdel Malekdrukdel. Khaled Chaieb alias Abou Sakhr Lokman became its leader, who took over the leadership of the outlawed Ansar al-Sharia in January 2014. In September 2014, one of the Uqba Ibn Nafi Brigade fractions pledged allegiance to the IS (again under the leadership of Abu Sakhr), while other militants remained loyal to AQIM acting in Libya and Tunisia. In July 2014 Abu Sakhr met Mokhtar Belmokhtar to carry out common attacks on tourism infrastructure and governmental facilities in Tunisia. At the beginning of March 2015 Tunisian extremists announced establishing a new organization – Jund al-Kilafah fi Tunis, which pledged allegiance to the Islamic State. It was just after the IS appeal to Tunisians for joining caliphate troops. On 29 July 2013, militants of the Uqba Ibn Nafi Brigade and AQIM laid siege to a military post in Chambi Massife, west Tunisia, killing 8 soldiers. One year later (16 July) fifteen other soldiers were killed there, and twenty others were wounded. Tunisian and Algerian security forces carried out antiterrorist operations on both sides of the border. Jihadists had been attacking soldiers, police officers, and security forces in different regions of Tunisia until March 2016.[23] Nevertheless, the most bloody attacks were carried out in the country in 2015. Western tourists were their target. On 18 March 2015, in Bardo Museum 24 people were killed and ca. fifty others were wounded. On 24 June 2015, in Sousse, 36 people died, and 39 others were wounded. On 24 November a suicide bomber linked to the IS blew himself up while trying to get on a bus together with the president's security guards. Thirteen people were killed and twenty others were wounded.

Since 2013, when the Egyptian forces under the leadership of gen. Abd al-Fattah as-Sissi (the incumbent president of Egypt) overthrew the President Muhammad Mursi linked to the Muslim Brotherhood, extremist groups in Egypt have escalated attacks on the military and police forces, especially in Sinai. So far dozens of soldiers and policemen have died in Sinai. It was there the Islamic State managed

[22] The name of the group refers to a legendary Tunisia conqueror, who established in 672 AD the oldest Arab building in North Africa – The Great Mosque of Kairouan. Kairouan is regarded by the Arabs as a fourth sacred place after Mecca, Medina, and Jerusalem. Uqba ibn Nafi died in 683AD in the territory of present Algeria in a battle with united Berber forces under the leadership of Kusail; E. Szymański, *Tradycje i legendy ludów Afryki Północnej*, Kraków 1994, pp. 63–66.

[23] https://fr.wikipedia.org/wiki/Bataille_de_Chaambi [access: 12 May 2017].

to establish a strong cell. In November 2014, Ansar Bait al-Maqdis (Supporters of the Holy House) organization established in 2011, took an oath of allegiance to Abu Bakr al-Baghdadi. It formed an official branch of the IS, known as Wilayat Sinai. The group called Agnat Misr (Soldiers of Egypt) established in 2013, also took the side of the IS. Although the groups do not have control over any territory, they are very active to date, often carrying out bloody attacks on different targets, but mainly in Sinai. Their targets are mostly soldiers and public officials of Egypt, the Copts, and tourists. The IS militants had a strong presence in the area of Rafah city, in the suburbs of Sheikh Zuweid city, and in the area of the biggest Sinai city, Al Arish. On 31 October 2015, they led to the catastrophe of an aircraft operated by Metrojet Russian Airlines, killing all 224 passengers and crew on board flying back home from the city of Sharm el-Sheikh. On Good Friday 2017, they attacked Coptic churches in the city of Tanta, the Nile Delta, and in Alexandria, where at least 45 people died. On 27 May 2017, the IS claimed responsibility for shelling one day earlier a bus with Coptic pilgrims in Al Minja province, killing 26 and wounding 25 people. Nevertheless, the most tragic attack took place on 24 November 2017. The group of 25-30 terrorists opened fire on worshippers in a mosque in the town of Ar Rawda near Al Arish. In the attack 305 people died. That was the worst massacre in the modern history of Egypt.

Somali Harakat al-Shabaab al-Mujahideen (Mujahideen Youth Movement), linked to Al Qaeda, managed to overrun the most territory of Somalia together with its capital city of Mogadishu between 2007 and 2010. After the intervention of Kenyan forces in 2011, Al-Shabaab was ousted from the major territories and it is currently dispersed. Nevertheless, it has not been shorn of operational capabilities as far as terrorist attacks in Somalia and neighboring Kenya are concerned.[24] Al-Shabaab pledged loyalty to Al Qaeda only in 2012. In 2014, faction of Abdul Kader Muhammad Abdul Kader, leader of foreign operations, and Muhammad Sandher expressed their support for the rapprochement with the IS. In September 2014, the leader of the organization Ahmed Abdi Godane was killed in an American drone strike. After his death Ahmed Umar alias Abu Ubaidah alias Ahmed Dirije took over the leadership, with his deputies Mukhtar Robow alias Abu Mansur and Mahad Karate alias Mahad Warsame Kalej. An Advisory Board consisting of 10 experienced jihadists was established as assistance. Its main goal was the supervision of different activities of the group: operational, political, propaganda, and religious. There are units responsible for internal security, carrying out attacks abroad (mainly in Kenya), responsible for militants abroad (Muhajirun),

[24] Before Kenyan military troops intervened in Somalia, Al Shabaab had split up into a nationalist faction with Hasan Dahir Awys opting exclusively for a power struggle in Somalia, and the faction with Ahmed Abdi Godane, claiming for establishing caliphate in eastern Africa. After Godane's death in 2014 national factions with Ahmed Imar and Mukhtar Robow at the helm gained an advantage in the organization: https://ctc.usma.edu/posts/the-life-and-death-of-al-shabab-leader-ahmed-godane [access: 3 X 2014]; Y. Olomojobi, *Frontiers of Jihad. Radical islam in Africa*, 2015, pp. 161–165.

mainly from Kenya, Tanzania, Sudan and Somalis from Western countries. For the last few years, radicals outside Somalia have shown decreased interest in entering the organization. The main reason is the popularity of other, more accessible frontiers of the struggle, especially in Iraq and Syria. On 13 December 2017 Robow was granted amnesty, and at the beginning of December in the same year Mahad Karate died due to an American drone strike.

The organization is known for its bloody attacks in Kenya, where its members had carried out ca. 140 attacks since the Kenyan military troops entered Somalia in October 2011 until the end of 2014. On 21 September 2013 a group of masked and armed attackers entered Westgate shopping mall in Nairobi, taking many hostages and killing non-Muslims. Until the facility was recaptured on 24 September, 71 people died and 175 were wounded. The attack was a retaliation for the Kenyan troops' activities in Somalia. On 21 November 2014, the bus with 60 passengers was hijacked about 50 kilometers from the town of Mandera near the border with Somalia and Ethiopia. They separated Muslims from non-Muslims. The non-Muslims were ordered to get on the bus where they were shot dead and the assassins managed to defect to Somalia. In the attack 28 people were killed. A similar attack took place in December 2015 in the rural area of El Wak, on the Somali border, but this time Muslims protected Christian passengers by refusing to be split into groups. In the attack two people were killed. On 2 April 2015, four armed Al-Shabaab gunmen stormed Garissa University, killing the guards at the entrance gate. Initially the attackers were shooting indiscriminately on students, then started the selection releasing Muslim students and executing the rest, mainly Christians. In the attack 148 people were killed. After ca. a 20-hour siege, terrorists were killed. On 6 and 25 October 2016, terrorists attacked twice the town of Mandera. In those two attacks 18 people died, and many others were wounded. Muslim Youth Center Al Hijra is the Kenyan branch of Al Shabaab.

Al-Shaabab has still control over some areas in the south and middle Somalia. In Mogadishu the associates of the organization collect a revolutionary tax from entrepreneurs and businessmen. There are at least 2 explosions each month. Al-Shabaab carries out attacks on politicians, businessmen, kidnaps workers of humanitarian missions, deploys mines, attacks hotels, and soldiers of the AMNISOM (African Union Mission in Somalia). For example, on 30 July 2017, 24 soldiers were killed in an ambush by Al-Shabaab. The attack took place a few hours after a car bomb had exploded in the capital of Mogadishu killing five people and leaving thirteen others wounded. On 14 December 2017, a bomber dressed in a police uniform blew himself up at the Police Academy in Mogadishu. At least 18 policemen were killed and 15 civilians were wounded. It is said that the death toll could have been much worse if the attacker had detonated his explosives in the crowd of policemen preparing themselves for their early morning parade on the square. Nevertheless, the deadliest attack by Al Shabaab and one of the most bloody attacks ever took place on 14 October 2017. The group carried out an attack on a hotel and a market place in the capital city with large trucks filled with explosives. The second explosion turned out to be

especially tragic, because the truck blew up next to an oil tanker, which intensified the blast. In both attacks 512 people were killed and 295 others were wounded. Since 165 people could not be identified, they were buried in a common grave. From that moment on, the US increased the frequency of airstrikes on Al Shabaab positions. On 13 November 2017, Pentagon confirmed killing more than 40 jihadists of Al-Shabaab and the Islamic State within 4 days. In a subsequent operation against Al-Shabaab, on 21 November 2017, the American troops killed more than 100 jihadists. According to the UN report, since 2017 the activity of jihadists in Somalia has increased significantly.

The Nigerian organization Jamā'at Ahl as-Sunnah lid-Da'wah wa'l-Jihad (Group of the People of Sunnah for Preaching and Jihad), better known as Boko Haram is equally vicious. In September 2014 it announced establishing its own caliphate. At the beginning of 2015, its leader Abubakar Shekau and his group was aligned with the Islamic State, establishing officially in April 2015 the West-African Province of the Islamic State or the Province of the Western Sudan (Wilayat Gharbi Ifriqiyyah). The IS wanted to take control over Boko Haram and to weaken Abubakar Shakau's position within the organization. The reason was Shakau's objection to Abu Bakr al-Baghdadi's plans to expand Boko Haram's activities outside Niger and Cameroon, and to delegate the leadership in the organization to a collegial body (Majlis al-Shura), composed of, among others pointed by the IS leader, Mamman Nur and Abubakar Adam Kambar. This way Shekau would be deprived of a one-man leadership in Boko Haram. To diminish Shakau's influences, Al-Baghdadi ordered to divide Boko Haram troops into 3 groupings and to dislocate them to the northern Cameroon, the Lake Chad area and eastern Niger. Shekau's task was to coordinate activities mainly in the northern Nigeria. The onflicts between the leaders concerning the scope of activities in different regions and the sphere of competence caused that Jama'atu Ansarul Muslimina fi Biladis Sudan (Vanguards for the Protection of Muslims in Black Africa) left Boko Haram. Its leader Khalid al-Barnawi established cooperation with Al Qaeda in Islamic Maghreb.

Until 2015 Boko Haram took control over almost three states in north-east Nigeria: Borno, Jobe and Adamawa. After the Islamic State it is the most murderous organization which had already killed more than 20,000 people and caused migration of ca. 2 million people from the area. According to different sources, military capability of the organization was estimated at from 4,000 to 30,000 jihadists in 2015. The group became famous for kidnapping 276 schoolgirls from their school in Chibok on the night of 14-15 April 2014. That case was the best known case in the media, but not the only one. A few months later, jihadists were to kidnap 300 school children and other 100 kids and women from the town of Damasak. The media was silent on this point. Admittedly, it's true that kidnapping the girls in Chibok made public opinion look at Nigeria with great concern. There was even a social media campaign #BringBackOurGirls, supported by the US First Lady Michelle Obama, which aimed to put pressure on the Nigerian forces to find the children. Despite the promises of African politicians and the passage of time, many girls form Chibok are still in captivity. Those

who managed to escape on their own are free. In May 2017, as a result of an agreement with the authorities of Nigeria, 82 girls were set free in exchange for some Boko Haram prisoners. According to Amnesty International, between 2014 and April 2015, Boko Haram kidnapped at least 2,000 women and children. They are used as sexual slaves and kitchen aids, as bargaining chips in negotiations to release prisoners and for suicide bombings. In Nigeria, Cameroon and Chad 44 children were forced into suicide attacks in 2015, compared with only four in 2014. Some of the children were only eight years old. The total number of suicide attacks in those three countries and in Niger, carried out by Boko Haram and its sister organization from northern Cameroon, Jama'atu Ansaru Muslimina fi Biladis Sudan, increased from 32 in 2014 to 151 in 2015. The number of girls and women taking part in these attacks has also increased. Between 1 January and 16 August 2017, 83 children were used as bombers, of these 55 were girls, and one was a baby strapped to a girl. Most of the girls were under 15 years old. Usually terrorists attach explosives to children and leave them in any crowded public place. Then, the bomb is detonated remotely. In a few cases children managed to get to the local services, which then removed and secured the explosives properly. In March 2014 a teenage girl, who managed to thwart an attack, said that he was one of the 276 schoolgirls from Chibok school kidnapped by Boko Haram in 2014. It is the first organization in the world, in which children and women represent a higher percentage of bombers.[25] The authorities of Nigeria informed several times about its leader's death, Abubakr Shekau. Abu Musab al Barnawi was to become its new leader. The decision was announced and published in a jihadist weekly *Al-Naba* on 2 August 2016. Two days later Shekau confirmed he was still the leader of the organization. On 27 June 2017 a video was released online, on which he claimed responsibility for a Nigerian policewoman kidnapping and criticized Nigerian authorities for spreading false news on the end of his organization.

Terrorist activities of Boko Haram led to a total destruction of 900 schools, some of them were burnt, and to closing twice as many establishments. More than 600 teachers and school workers were killed and 19,000 were forced to flee.[26] Hundreds of murdered or kidnapped schoolchildren and thousands of wounded people should also be mentioned. Since the Islamists in Nigeria were forced onto the defensive by the coalition forces of Nigeria, Chad, Niger, and Cameroon, they target civilians in their own attacks. Children with explosives strapped to them are sent to crowded market places and stations. On the other hand, thanks to military successes, the Nigerian army has released hundreds of kidnapped people in recent months. According to the report of the UNICEF and International Alert, London based foundation, women and teenagers returning to their villages are treated with suspicion or are even rejected. Victims of rapes quite often bear jihadists' children. Local societies are also afraid that kidnappers have inculcated

[25] https://kobieta.wp.pl/horror-ktorego-swiat-nie-chce-dostrzec-w-2017-roku-boko-haram-wysadzilo-w-powietrze-55-dziewczynek-6158590054090881a [access: 24 VIII 2017]; https://wiadomosci.wp.pl/zamach-w-maiduguri-zabitych-10-osob-wielu-rannych-6188198088788097a [access: 16 XI 2017].

[26] https://wiadomosci.wp.pl/pala-szkoly-porywaja-dzieci-morduja-nauczycieli-krwawa-kampania-fanatykow-boko-haram-6025269939212929a [access: 22 IV 2016].

radical ideas into them. In April 2016, it was rumored that members or sympathizers of Boko Haram from Senegal were able to carry out attacks on the beaches of Italy, France and Spain. In October 2017, the first in a series of trials of 2,300 people accused of terrorist activity in Boko Haram started. Khalid Barnawi is one of the persons accused of kidnapping and killing 10 foreigners.

At the end of 2015 and the beginning of 2016 Tanzim Al Qaeda fi Jazirat al-Arab (Al Qaeda Organization in the Arabian Peninsula, AQAP) established its own emirate. AQAP, regarded as the most dangerous branch of al Qaeda, has been present in Yemen fora long time, nevertheless, during the presidency of Abd Rabbuh Mansur Hadi and hispredecessor Ali Abd Allah Salih, its operational capabilities were limited because American airstrikes and attacks by soldiers of the government in Sana put the organization on the defensive. That situation lasted until January 2015, when Shia rebels from Husi movement forced Hadi to escape from Sana, and following that the retreat of American troops from the country. As a resultof Saudi Arabia intervention in March 2015, the conflict became very soon the next competition arena between Saudi Arabia and Iran in the region, which led to the escalation of the conflict and the humanitarian catastrophe. While the clashes between Husi and governmental forces focused in the south-western, the most populated part of the country, AQPA took advantage of the situation in the east taking over other areas, very often left by governmental forces. It built its structures, very often with the silent approval of the local people, who thought that the situation was more stable than in other regions liberated by Yemeni forces, and the alternative to Al Qaeda might have been even worse. AQPA, in fact, ever since its creation in this part of the Middle East, has been using the same tactics as the Islamic State, i.e. taking over and controlling a territory with its population and the whole social and economic potential. Furthermore, AQPA as distinct from other Al Qaeda's branches, was shifting its activities to Europe. It should also be noted that creating quasi state structures in the hot spots by Islamic terrorist organizations constitutes an increasingly widespread phenomenon.

In 2016 AQPA had control over 10 cities. Despite the fact that it exercises power through local supporters, and not under the name of Al Qaeda, rule by extremists are ruthless and are not that much different than their ideological rivals from the IS. Just as the IS in Syria and Iraq, AQPA collected taxes and made profits from the oil fields and oil facilities. The organization's assets, in the poorest country in the Middle East, was assessed at 100 mln USD. For a long time the successes of Al Qaeda remained in the shadow of struggles between Husi and the regime, and the war in Syria. A few months after terrorists from AQPA, brothers Said and Cherif Kouachi carried out a terrorist attack on the Paris headquarters of the satirical magazine Charlie Hebdo in January 2015[27], American drone airstrike killed some of the most important figures of the organization, including its leader and number two in the whole Al Qaida, Nasir Al-Wuhayshi in Mukali, Hadramaut province (12 June 2015). This seaside town was captured by

[27] G. Kepel, *Terror we Francji. Geneza francuskiego dżihadu*, Warszawa 2017, pp. 239–265.

Al Qaida militants in April 2015 after two weeks of struggles. From the beginning of 2016, the US intensified their campaign of airstrikes. In one of such airstrikes on an AQPA facility in Mukalli, 50 jihadists were killed. Although comparing to struggles with the IS, the number of attacks in Yemen was rather small. AQPA took advantage of the void left by the authorities and became stronger than ever. Nevertheless, it is not the first time when jihadists from Yemen have got a chance to widen its influences. Every time the US and Yemeni forces were able to take from terrorists their prizes, but they were not able to defeat them completely.[28] In April 2017, the AQPA leader, Qasim AL-Raymi announced that its organization was going to fight with Shia movement Husi, and is ready to start, under some conditions, negotiations with the President Mansur Hadi. At the beginning of August 2017 Yemeni soldiers supported by advisers from the UAE started an operation against AQPA in Shabwa province.

From the second half of 2014 the Islamic State had been trying to build its outposts in Afghanistan. The Islamic Movement of Uzbekistan, acting on the border of Afghanistan and Pakistan, pledged allegiance to caliph Ibrahim. In Talib movement there was a cleavage and competition as far as effectiveness of attacks was concerned. Emir Hafiz Said Khan became the leader of the Afghan and Pakistani troops of the IS. His goal was to establish Wilayat Khorasan in the territories of Afghanistan, Pakistan and Central Asia.[29] Khan was killed on 26 July 2016. Abdul Hasib was appointed his successor, but he was killed in May 2017. Most fighters were recruited from the Tehrik-e Taliban Pakistan. It is the most active in provinces of Badakhshan, Kunduz, Farah, Raryab, and in the east, in provinces of Logar, Paktika, and particularly in Nangarhar. It was observed that more and more young people and the Taliban were recruited into the IS. Local IS commanders gave larger pay to their soldiers than the Taliban, which attracted recruits. In 2015 the organization Hezb-e Islami Gulbuddin Heekmatiar joined the IS. At the beginning of June 2015 its leader declared the common fight with the IS against the Taliban in Afghanistan. Nevertheless, it were the Taliban who won the competition in the end. They seem to control ca. 40% of the territory of the country nowadays and carry out terrorist attacks on governmental facilities, market places and shopping malls, the seats of foreign institutions, Shia cultural institutions, police forces, military and security forces at least once a week.

Superior authority of the Islamic State was also acknowledged by the Philippine Abu Sayyaf organization and Al-Jama'a al Islamiyya and Jimat Anshorut Twhid from Indonesia. Because of that there was a cleavage in the last-mentioned organization followed by the establishment of Jama'at Anshorut Sharia. In the Philippines, Abu Sayyaf militants under the IS name captured the city of Marawi in the Mindanao island on 22 May 2017.

[28] A. Wejkszner, *Globalna sieć…* , pp.146–148; the same, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010, pp. 249–252.

[29] The Khorasan Group aka Battalion of Wolves was active in Syria with Muhsin al-Fadhli as the operational leader. The group cooperated with an Yemeni bomb constructor Ibrahim al-Asiri, a member of AQPA. Terrorist attacks in the West were the goal of the group; B. Hall, *ISIS. Państwo Islamskie*, Warszawa 2015, pp. 201–204.

It was just after the governmental forces tried to arrest the leader of the organization Isnilon Hapilon who had come to the city for medical treatment. Abu Sayyaf fighters under Mahmud Ahmad alias Abu Handzalah and supported by Maute group (estimated at over 300 persons) threw the military out, killed Christians and took 200 people hostage. Fighting for the city lasted 5 months. On 23 October 2017, defense minister of the Philippines announced the end of military action, claiming that Islamists were eliminated. Mahmud Ahmad and Hapilon were killed. Almost 500,000 people fled protecting themselves from struggles in Marawi and in the whole region, and more than 800 people died, including jihadists, civilians and military men. The near future will show whether jihadists are defeated because Abu Sayyaf organization, active since 1991, has remarkable ability to revive, recruit new members and fighters and pose a new threat.

The popularity of the IS ideas and the decline of Al Qaeda caused that the IS gained great importance among Muslim terrorist organizations. It took over human resources, finances and military resources of Al Qaeda, becoming the biggest, the richest and the most dangerous terrorist organization in the world. The restitution of caliphate had a deep political, ideological and religious message because of its significance in Muslim tradition. Therefore, it will be very difficult for the current generation of jihadists fighting for development and maintaining the caliphate to deal with its collapse caused by the significant participation of the western forces hated by extremists. Anyway, the memory of colonial period and the UK and France dominance in the Middle East has again revived. Apart from those countries and the US, a new aggressor, Russia has appeared. Syrian and Iraqi authorities, Shiites and Kurds remain traitors and enemies, and as such they have to reckon with the possibility of terrorist attacks against them. The IS as a global hybrid terrorist structure is going to be a particular challenge for the police and security services in many countries. Their officers must expect implacable hostility, fanaticism, disdain for death, and cruelty. Further confrontation between the IS and Al Qaeda will remain in doubt. No scenario can be precluded that the conflict will be replaced by some kind of agreement, or even cooperation, for example common terrorist attacks. One such example took place in January 2015 in Paris, when Kouachi brothers, linked to Al Qaeda, carried out a terrorist attack on Charlie Hebdo publishing house and Amedy Coulibaly, their accomplice declaring his affiliation to the IS, carried out an attack on a Jewish supermarket.

Abu Bakr al-Baghdadi's death can lead to ease tensions between the IS and Al Qaeda. Changes in the Al Qaeda leadership can also lead to the improvement of relations between the two organizations. It seems that Hamza bin Laden, the 28-year-old son of Osama Bin Laden and his third Saudi wife, Hajrija Sabar, known as the 'Prince of Jihad', will take the lead in Al Qaeda in the near future. In August 2015 video footage of Hamza bin Laden and Ayman Al Zawahiri calling on jihadis to attack Washington, London, Paris, and in Tel Aviv was released. After that, the other three video footage of Hamza bin Laden appeared, on which he eagerly encouraged lone wolf attacks to be carried out in the West, and to revenge his father. In August 2016, his video footage appeared online, on which he called for regime change in Saudi Arabia, ruled by *large criminals*

and thieves, and American agents. The power in the country must be taken over by a new government that would distribute revenue from oil more fairly and encourage its citizens to jihad. Nevertheless, the real sin of Saudis is their stance in Yemen, where since March 2015 they have been waging a vicious war against Shiite rebels from Husi movement. Hamza accused Riyadhof favoring Shiites and fighting Al Qaeda affiliated jihadists, which is *a double betrayal against Muslims in Yemen.*[30] Hamza bin Laden has his own concept of jihad regardless of his charismatic name which calls to mind the mastermind behind the worst terrorist attack in recorded history. He is against any spectacular long prepared attacks, which can be disrupted by special services. Like the IS, he calls for attacks on Americans, Europeans, and pro-Western Muslims, wherever they are, with any accessible weapon. Apart from that, unlike al-Zawahiri, he did not criticize the caliphate, which may – after the collapse of the IS – win him support and renew Al Qaeda or any other organization founded on it possibly in the future.[31] Being aware of that new threat, the end of September and the beginning of October 2017, 40 operatives from the British SAS came to Syria with the aim of tracking him down and killing.[32] Their attempts have so far been unsuccessful. However, this piece of information publicly available can win the young bin Laden new followers.

Abstract

Military victory over the Islamic State does not mean defeating this terrorist organization, members of which will move into conspiracy, and will continue terrorist attacks. Organizations allied to the Islamic State operating in the foreign wilayats (provinces) of the caliphate: in Sinai, Libya, Nigeria, or Afghanistan are still active. There are also other groups active, linked to Al Qaeda or formed its franchises before, leaders of which pledged allegiance to caliph Ibrahim (Abu Bakr Al Baghdadi) between 2014 and 2015. There are more than 40 such organizations altogether. Some of them split following internal arguments over which side to be on: Al Qaeda or the IS, involved in the conflict since 2013. Apart from the Middle East, North Africa has become the main arena for activity and competition between jihadist organizations, especially the regions of Sahara and Sahel, where the IS has increased its influences since the second half of 2014. As long asthe IS has been defeated in Syria and Iraq, in Africa its operational capabilities to carry out terrorist attacks have remained although its position has also weakened. The consequences of the IS activities and its other affiliates were tragic. The year 2014 was the most violent when 32,858 people were killed in the whole world. In 2016 terrorists killed 25,673 people around the world. It is almost 22% less than in 2014. The list of countries with the highest terror risk has not changed at all.

[30] https://wiadomosci.wp.pl/syn-osamy-bin-ladena-nowym-liderem-al-kaidy-hamza-wzywa-do-walki-6029048256705665a [access: 23 VIII 2017].

[31] M. Urzędowska, *Powrót Al-Kaidy i Ben Ladena*, „Gazeta Wyborcza" of 2 November 2017.

[32] http://www.dailymail.co.uk/news/article-4938874/SAS-begin-mission-kill-capture-Osama-Bin-Laden-s-son.html [access: 6 X 2017].

The first five countries are Iraq, Nigeria, Afghanistan, Syria, and Pakistan. According to statistics, 75% of all victims came from those countries.

The security situation in Europe may deteriorate in the near future. Jihadist propaganda still meets with a favorable response, and it is going to be more and more effective, if the reality fails to meet the immigrants' expectations, and demanding attitudes turn into anger. Deportations of those who lost their right of residence, also because of the committed offences, or tightening asylum law and conditions of granting state benefits will encourage such behaviors. Denmark, Austria, Germany, and France have already announced the above-mentioned limitations because the line between refugees and economic migrants tends to blur.

Easing tensions between the IS and Al Qaeda, for example, after Abu Bakr al-Baghdadi's death can cause increased risk. Changes in the leadership of Al Qaeda can also contribute to the improvement of relations between the two organizations. It seems that Hamza bin Laden, the 28-year-old son of Osama Bin Laden, known as the 'Prince of Jihad', will take the lead in the organization in the near future. Unlike the current leader of Al Qaeda, Ayman al - Zawahiri, he did not criticize the caliphate, which may – after the collapse of the IS – win him support and renew Al Qaeda or any other organization founded on it possibly in the future.

Keywords: Al Qaeda, terrorist attacks, security, the Middle East, jihad, jihadists, fanaticism, Islam, caliphate, conflicts, Kurds, mujahedeen, Muslims, Islamic State, salafists, Syrian Democratic Forces, the Taliban, terrorists, terrorism, Wahhabism, threat, attempts.

Danuta Gibas-Krzak

Terrorism in the Balkans. Genesis – types – prognoses

Introduction

Although there are more than two hundred definitions of terrorism it is very hard to choose the most appropriate one which reflects the subject in the most precise way and which properly explains the nature of international order in the globalisation era. It does not change the fact that modern terrorism is political and social phenomenon which roots lie in the complicated processes occurring in the society. Many researchers claim that it is better to establish different kinds of terrorism than to give one definition. In the framework of this paradigm one can speak of a state terrorism, ethnic terrorism and international terrorism. In science there is also a notion of asymmetric threat which refers to the studies on war and conflicts.[1] It is hard to deny that terrorism, often perceived as non-selective and senseless, is in fact conscious and planned act of the use of violence.[2] Lack of one, reflecting the nature of the phenomenon typology causes that researchers attempt to systematize terrorism which involves with its division into doctrine objectives and ideological goals. International terrorism is commonly used term and it is understood as the use of force or the threat of the use of force by individuals or groups of people against other people, places or objects, violating international law with the intent to intimidate social (ethnic) group, society, nation or international society. The attention is also drawn to the fact that after the Cold War the cooperation between individual terrorist organisations is particularly dangerous as far as training, giving the shelter to terrorist commandos, joint actions and using terrorist methods by political, ethnic groups, religious movements and nations fighting for independence are concerned. Carrying out actions of terrorist nature by special services as well as cooperation between terrorist groups and organised crime and their joint actions with special services can cause some concern.[3]

It is worth noting that terrorist activities have been used for ages as an effective tool for fighting both the stronger opponent and the society because it is the intimidation of the terrorized subject that lies behind.

As every social and political phenomenon, terrorism has evolved over the centuries taking various forms until it became the real curse of our times. In an era of globalization it is known of brutal acts – actions and operations carried out by organizations linked ideologically and religiously to Islam. In spite of the complicated typology of the phenomenon, the following terrorism types can be specified with regard to historical perspective:

– anarchic terrorism of the 19th century and the beginning of the 20th century,

[1] R. Borkowski, *Terroryzm ponowoczesny. Studium z antropologii polityki*, Toruń 2007, p. 43.
[2] B. Hoffman, *Oblicza terroryzmu*, Warszawa 1999, p. 175.
[3] *Encyklopedia Politologii*, ed. M. Żmigrodzki, vol. 5, Zakamycze 2002, p. 365.

- leftist terrorism of the 1960s and 1980s,
- right-wing terrorism of the end of the 20th and the beginning of the 21st century,
- postmodern, religious, global terrorism.[4]

However, there are other less known aspects of terrorist activities particularly referring to south-eastern part of The Old Continent. It should be noticed here that in no other European region one can encounter such wide spectrum of terrorism forms what undoubtedly makes this area unique for historians, political scientists and representatives of other fields of science. Over the last hundred years the Balkans have been a theatre of different subversive actions and numerous terrorist acts which influenced the world history. It was because of Gavrilo Princip and his comrades from the Young Bosnia, small terrorist organisation, responsible for an attack in Sarajevo and the assassination of Archduke Franz Ferdinand, what would lead to the outbreak of the First World War (1914-1918). Macedonian revolutionaries from the Internal Macedonian Revolutionary Organization (VMRO) started their operations in the Balkans several years earlier. Initially, they were determined to fight with the Ottoman Empire but over the years they turned against Yugoslavia. The phenomenon of post-Ustashe and post-Chetnik terror remains practically unexplored in Polish and global historiography. The link between the terrorism of Balkan origin and the Islamic terror organisations of modern type has been much better described; even though, it seems that this problem with regard to the Balkans is not imperceptible and that it is marginalised by political decision makers, from the Western Europe in particular.[5]

In this context it seems important to submit this specific Balkan terrorism to separate studies; heuristic studies mainly, with the use of the methods of analysis, synthesis and comparative analysis. Analysis method allows the research material to be processed. The usage of the method helps to divide described events into a set of individual, specific features and elements of events. Synthesis method, on the other hand, allows to formulate general statements.It also enables a generalisation of detailed data from the researched material. Using this research method is crucial while closing every stage of research and process of opinions justification. Frequent usage of synthesis is involved with the use of inductive methodology which enables the so-called generalising deduction (inductive inference). This method requires studying on the basis of the facts that form the basis for scientific deduction. However, comparative method enables to follow both the way and the forms of terrorist activities in different periods of time, countries and regions. Then it is possible to conclude what was specific and what was typical for the examined fact or event. They usually relate to comparing data from different countries, areas or regions. The comparative method is used to justify the validity of a certain thesis. Thanks to its usage, the important generalisations are made, which results in comparative deduction. Taking the above

[4] R. Borkowski, *Terroryzm ponowoczesny…*, p. 49.

[5] Vide: *Terrorism in the Balkans in the 20th and 21st century*, ed. Danuta Gibas-Krzak, Toruń 2018.

methods under consideration, the aim of this article is to identify types of terrorism in the Balkans, placing its origins in time, presenting its development and considering the present nature of this terrorism. Some research questions were considered helpful:

- What is the genesis of terrorism in the Balkans?
- What is the evolution of terrorism in the Balkans?
- What factors decided on the developments of terrorist activities in that part of Europe?
- To what extent the disintegration of communist Yugoslavia influenced the polarization of national relations and shaping radical religious movements linked to Islamic terrorism?
- Are the Balkans really a home to people of religious fundamentalist motivated terrorism?

The main hypothesis is: the Balkans open a great possibility for development of bases and training camps for terrorists linked to global jihad because of geographical conditions (natural conditions). This fact poses a threat to Europe's security and its democratic societies because of the probability of a conflict not only on a local scale, but also on an international scale.

Types of terrorism in the Balkans in the 19th and 20th centuries

The history of terrorism in the Balkans is connected to national and liberation movements in this part of Europe. They used terrorist methods as a tool for Balkan nations to regain independence, lost during the Turkish invasion. One of terrorism precursors in the region was the Internal Macedonian Revolutionary Organization (VMRO) established in 1893, which used terrorist methods aiming at the liberation of the people living in the Slavic lands. During that time, the activity of Macedonian death squads was truly appalling; they were carrying out cold-blooded murders and spectacular attacks on wealthy members of Turkish families. It needs to be pointed out that in 1903 VMRO organized the biggest uprising in Macedonian history called the Ilinden Uprising.[6] It should also be mentioned that Macedonian separatists were actively engaged in the process of disintegration of the Kingdom of Yugoslavia in the interwar period and their allies became members of the Croatian Ustasha – Croatian Revolutionary Movement (known as Ustashe). Alexander I Karađorđević, King of Yugoslavia and Louis Barthou, French Foreign Minister were assassinated in 1934 in Marseilles (France) by Macedonian and Croatian extremists. Ustashe, presented often as a movement which was using terrorist methods[7], was also known for terrorist attacks in Belgrade and Zagreb, and in the 1930s they tried to begin an uprising in the area of Zadar, Banja and Kordun aiming to split Croatia and

[6] T. Wasilewski, *Historia Bułgarii*, Wrocław-Warszawa-Kraków-Gdańsk-Łódź 1988, p. 207; Klejn, *Bułgaria. Szkice z dziejów najnowszych*, Pułtusk 2005, p. 54 et passim.

[7] D. Trifunović, *Threat to international security – terrorism in South East Europe*, [in:] *Służby specjalne w systemie bezpieczeństwa państwa. Przeszłość – teraźniejszość – przyszłość. Materiały i studia*, ed. A. Krzak and D. Gibas-Krzak, Szczecin 2012, vol. II, p. 279.

the Kingdom of Yugoslavia.[8] In the interwar Romania there was a political organization called The Iron Guard and its activity was described as terrorist. The organization was established in July 1927 as the Legion of the Archangel Michael.[9] In the moment of the establishment it was only a secessionist group from the National-Christian Defense League (Liga Apărări National Crestine, LANC), which was active in Moldova from the beginning of 1920s. Nonetheless, terror and direct actions became crucial elements of the fight soon. LANC death squads attacked prominent state officials (they assassinated a prime minister for instance) and damaged public facilities.[10] It cannot be forgotten that the Balkans were the arena of different mainstreams and forms of terrorism. Political assassinations, which can be classified as acts of political terror, were also quite popular in the interwar period in Yugoslavia and Bulgaria. Also Soviet special services which exercised control over the Comintern and communist parties in Balkan countries used terrorist methods. Their members used individual terror on a large scale particularly in the first years following the Great War, which was supposed to be the first stage of the proletarian revolution. Numerous attacks were often unsuccessful, like an attack on the Bulgarian tsar, Boris III at the Arabakonak Pass. It was neither the first nor the last failure of both Comintern and Bolshevik special services. Nevertheless, it resulted in the fact that Cremlin authorities were forced to abandon, at least partially, the idea of spreading revolution over other countries and regions.[11]

During World War II, in a complicated situation in the occupied back then Yugoslavia, terror was institutionalized as a form of genocide with the main involvement of The Independent State of Croatia (Nezavisna Hrvatska Drzava, NDH) and its allies. Establishing in 1941 puppet NDH, led by the Ustashe, represented the idea of a Croatian state, which it had been fight for with terrorist methods. The activity of the state terror structures was aimed not only against Serbs, Jews or Roma, but also against those Croats who were opponents of Ante Pavelić. It should also be noticed that the Second World War was the time of a common state terror used by occupation authorities and regimes collaborating with the Axis powers. For the next several years after the end of World War II, communist authorities of Yugoslavia, Albania, Bulgaria and Greece were carrying out intensive actions using terrorist attacks in order to eliminate their political opponents. Yugoslavia chose the "out-of-the-block" option but it did not prevent it from the attacks of the general public that criticized the country for the support given to the international terrorism The country indeed made considerable profits from arms trade which were provided to the Third World countries and earned approximately 700 million

[8] J. Wilamowski, K. Szczepanik, *Ustasze i separatyzm chorwacki*, „Przegląd Historyczny" 1983, vol. LXXIV, pp. 82–90.

[9] N.M. Nagy Talavera, *The Green Shirts and the Others. A history of fascism in Hungary and Romania*, Iasi 2001, p. 370.

[10] A. Dubicki, *Terror as a method of fighting of the Iron Guard*, [in:] *Terrorism in the Balkans in the 20th...*, pp. 52–60.

[11] A. Krzak, *Active intelligence service (terrorism) of the Comintern and Soviet secret service in Bulgaria in the 1920s – case study*, [in:] *Terrorism in the Balkans in the 20th...*, pp. 36–48.

annually that way.[12] Another example was offering a shelter by communist authorities to famous terrorist, Carlos, members of Baader-Meinhof organization and Abu Abbas from the Palestinian Liberation Front, known for hijacking the Italian cruiser „MS Achille Lauro" in 1985. It cannot also be forgotten that in 1980s there were training camps of Palestinian and Libyan terrorists in Yugoslavia. Until the end of 1984 in Voivodina, there were more than 800 individuals trained in intelligence courses including the members of national and liberation movements and terrorist organizations from Third World countries.[13] Between 1945 and 1990 special services of Yugoslavia carried out attacks on representatives of anti-Yugoslavian emigration killing 73 people.[14] Serbian sources report that Josip Broz-Tito and German Chancellor Willy Brand reached a secret agreement which enabled killing Yugoslav dissidents in Germany. One of the contract killers was supposed to be Željko Ražnatović, aka Arkan, future commander of Serb paramilitary troops which were known for the war crimes committed during the disintegration of communist Yugoslavia and the ensuing civil war.[15] In 1981 in Western Germany there was a trial of three Yugoslav agents of secret police who were sentenced to years in prison for planning and preparing acts of murder on Yugoslav (Croatian) migrants.[16] Also some Serbian politicians, including the late former president Slobodan Miloševic, are suspected of terrorist involvement. Under his government it came to a close cooperation between police and special services and criminal community, the most dramatic example of which was the assassination of the Serb Prime Minister Zoran Đinđić in 2003.[17]

Croatian dissident environment paid back the communist authority by using various forms of terrorist attacks. Factions of the Yugoslav emigration had prepared more than 400 terrorist attacks in and outside the country between 1946–1985 as a result of which 102 people died and 330 were wounded. The Croatian Revolutionary Brotherhood (CRB) which was established in 1961 aiming to prepare uprising in Yugoslavia and to gain independence for Croatia, carried out 120 attacks during which 53 people were killed and 118 were wounded. Terrorists prepared also an attack on Josip Broz-Tito (1976), an attack on Yugoslavian club in Paris (1966), an attack on Embassy of Yugoslavia in Germany (1966), and an attack on a vice-consul of Yugoslavia in Lyon (1969). Some members of CBR joined terrorist group linked to the Ustashe movement. The group was preparing a military uprising to liberate Croatia during the meetings of the conspirators in Austria in 1972.[18]

---

[12] I. Lučić, *Bosnia and Herzegovina and terrorism*, "National security and the future" 2001, no. 3–4, p. 117.

[13] Ibidem, p. 115.

[14] *Emigrant Croats who were victims of federal terror after 1945*, "Slobodna Dalmacija", 15.08.2000, p. 10.

[15] M. Lopušina, *Tajne srpske policije i zloupotrebe*, [in:] *Służby specjalne w systemie bezpieczeństwa*…, p. 213.

[16] I. Lučić, *Bosnia and Herzegovina*…, p. 117. Vide: M. Doder, *Jugoslavenska neprijateljska emigracja*, Zagreb 1989.

[17] M. Lopušina, *Tajne srpske policije*…, pp. 214–220.

[18] D. Trifunović, *Threat to international security*…, p. 279.

Islamic terrorism in the Balkans

The origins of Muslim terrorism are usually associated with the medieval sect of Nizari which used assassins' methods and terror to a large extent. After the First World War in Egypt, there was a national and religious organisation called Al-Ichwan al-Muslimin (Muslim Brotherhood) established, aim of which was to return to traditions of the real, i.e. early Islam and liberation of the Muslim world from the Western civilisation which stands for depravity and decay for a true believer. Its followers introduced the rule of Islamic fundamentalism into international usage giving it some institutional frames. They preached the rule of jihad initially understood as a method of peaceful spreading of the religious rules. Nevertheless, it became an aggressive terrorist activity which influenced almost all fundamentalist, extremist and terrorist organisations over time.[19]

Terrorism related to extreme currents of Islam in the Balkans emerged and rooted during the disintegration of Yugoslavia and the fight between conflicted nations during the civil war (1992–1995). At present, this kind of terrorism is related to the presence and increase of Muslim fundamentalists' impacts in the region. It should be remarked that during the Cold War the society of Yugoslavia was not influenced by the radical Islam rules. In 1971 Muslims got a status of a separate nationality in Yugoslavia, but their rather superficial religiousness was of a more secular nature. The victory of the Khomeini revolution was a direct impetus for revival of local Islam believers.[20] In the 1970s Alija Izetbegović, future President of Bosnia and Herzegovina, called for application of the Islamic Declaration, and started the development of an organized Islamist movement that way.[21]

A participation of Muslim mercenaries in the civil war, which has generated several controversies, has become an important aspect of Islam believers' dominance. It is presumed that there were 1,500 to 3,000 volunteers taking part in fights in Bosnia and Herzegovina, called "warriors of God" (Allah). According to some statistics, at the beginning of 1995 there could have been even 20 000 of them. The first were recruited in 1992 by Muhamed Čengić, the vice Prime Minister of the government in Sarajevo, who went to Turkey with a task to collect weapon, munitions and mercenaries."The warriors of God" came from Muslim countries: Saudi Arabia, Pakistan, Turkey, Algeria, Afghanistan, Egypt, Sudan, Iran and Syria. Many of them were veterans of the Afghanistan war and belonged to Al Qaeda, the Armed Islamic Group (GIA), Hezbollah, Hamas or Jamaat al-Islamiyya. They were fighting in the name of Allah launching jihad, and their goal was to spread the idea of Panislamism in Bosnia and Herzegovina, although some of them earned substantial sums of money

[19] K. Izak, *Leksykon organizacji i ruchów islamistycznych*, Warszawa 2014, p. 7. Vide: J. Hauziński, *Asasyni. Legendarni zabójcy w czasach krucjat*, Poznań 2016.

[20] N. Beloff, *Tito's flawed legacy. Yugoslavia and the West: 1939-84*, London 1985, p. 216.

[21] In the Islamic Declaration published in 1970 A. Izetbegović enclosed ideas of the Balkan Muslim state. I. Aralica, *Što sam rekao o Bosni*, Zagreb 1995, p. 88.

as mercenaries.[22] Islamic fundamentalists in the Bosnian army ranks committed numerous war crimes. According to the report of 1993 by a special UN envoy, Tadeusz Mazowiecki, mujahedeen fighters in the region of Jablanica – Nonjic and Radesnie had deported and murdered non-Muslim inhabitants. The 7th Brigade of the 3rd Corps ("El Jihad"), which members boasted about their war crimes, was particularly brutal. Zelena Legija and Gerila Battalions as well as a Muslim unit from the town of Tešanj, „Al Mujahedeen", were known for killing taken hostage adversaries particularly Serbs who were decapitated.[23] There were charges of committing the war crimes against the commanders of the 3. Corps, Enver Hadžihasanović and Mehmed Alagić brought into the International Criminal Tribunal for the former Yugoslavia (ICTY).[24] They attempted to impose strict religious rules in the occupied territories, forcing the inhabitants to live in accordance with Sharia law; for instance, girls were obliged to wear long dresses under penalty of law and older women were obliged to wear hijabs.[25]

Muslim countries were very supportive to the Balkan jihad. In the years 1992-1995 Iran supported the authorities in Sarajevo financially and logistically.[26] In the report of the US Congress of January 1997 it was stressed that Iranian Revolutionary Guards had been integrating with Bosnian military structures quickly. Iranian intelligence VEVAK (Vezarat-e Ettela'at va Amniyat-e Keshvar) organized its nets all over the country and Iranians controlled significant part of the security apparatus there. Special services became a tool of Islamisation (for example Muslimanska obavještajna služba, MOS), which stayed in contact with bin Laden and Al Qaeda during the civil war as well as with other Arab organizations supporting jihad like Tvaik Group, which was a cover for Saudi intelligence according to the German Intelligence Service BND. Nevertheless, it was a net of car rental companies in Europe officially. MOS was issuing Bosnian passports for members of terrorist organizations who were fighting in the Balkans. Bosnian diplomats were selling passports even to common criminals and their prices were up to 500 US dollars for one document.[27] In May 1992 „Ševe" team was established and it was comprising former officers of the Yugoslav intelligence fighting the so-called internal opponent. It was led by Nedžad Ugljen who was responsible for the personal security of Izetbegović since the spring of 1994.[28] Former major of the Yugoslav counterintelligence, Enver Mujezinović was

[22] D. Džamić, *Psi rata na Balkanu. Strani plaćenici u ratnim sukobima na prostorima bivše Jugoslavije*, Beograd 2001, pp. 204–207.

[23] Ibidem, p. 209.

[24] Contrary to a standard opinion that war criminals in the civil war in Yugoslavia in the late 20th century were mostly Serbs, it is also individuals of Muslim nationality and religion (and Croatians) who were charged for crimes and barbaric acts during the long and brutal conflict.

[25] D. Džamić, *Psi rata na Balkanu…*, pp. 208–209.

[26] Ibidem, p. 81.

[27] Džon P. Šindler, *Nesveti teror. Bosna, Al Kaida i uspon globalnog džihada*, Beograd 2009, pp. 145–147.

[28] J. Elsässer, *Jak dżihad przybył do Europy. Wojownicy Boga i tajne służby na Bałkanach*,

also involved in the team's work. Terrorist attacks on Serbian and Croatian people were the tasks of the group, and they were preceded by special services' snipers recruitment in Sarajevo. Their aim was to kill Serbs and Croats in order to make them leave the city.[29] The Ševe team dealt also with eliminating political opponents.[30] In summer 1993 Muslim special forces sent two groups to kill Fikret Abdić who turned out to be inconvenient. He was against the presidency of Izetbegović claiming that he ought to take the post according to the result of the election. He advocated development of economic cooperation and agreements with Serbs and Croats, strongly criticised religious fanaticism and continuation of the civil war, which in his opinion could have been ended earlier. The attacks prepared with the knowledge of Izetbegović were a failure and five assassins, trained by Iranian intelligence, were arrested by the Croatian police.[31]

After the Dayton Agreement was signed (1995) Izetbegović publicly paid tribute to mujahedeen fighters, praising them for their commitment and bravery. It is worth noting that the politician did not take any actions to prevent the formation of the Wahhabi sects which were frequently offering shelters for terrorist groups linked to Al Qaeda in the country. After the end of civil war political elites helped mujahedeen fighters to find employment, mostly in the police and in the army.[32] There were also some Wahhabis among them who proclaimed slogans of Islam reforms in more radical way. After the civil war, there were numerous incidents regarding Islamisation of the society and closing mosques which imams did not agree to preach fundamentalist ideas. The incidents started to turn into terrorist attacks over time. According to experts, Al Qaeda had at least two training bases in Bosnia and Herzegovina where terrorists had been trained. An Algerian, commander of the El Mujahid, Abu Al Mali was the head of one of the training groups. He was arrested while going to Istanbul and using a Bosnian passport. One cannot omit the fact that four out of seven terrorists responsible for 9/11 attacks had been fighting in Bosnia and Herzegovina and had a citizenship of the country. There are theories that there was also Muhammed Atta, the best known terrorist, who was recruited by the German citizen and Al Qaeda member, Muhammed Hadar Zammar who had also been a participant of a Bosnian jihad.[33]

The police and security forces continue to take many actions to counter terrorism and Islamic extremists. One of the biggest operations was carried out on 1 and 2 February 2010 in the village of Gornja Maoča[34] between Tuzla and Brčko,

Warszawa 2007, pp. 130–131.

[29] D.P. Šindler, *Nesveti terror...*, pp. 158–159.

[30] Ibidem.

[31] Ibidem, pp. 203–204.

[32] A. Wejkszner, *Ewolucja terroryzmu motywowanego ideologią religijną na przykładzie salafickiego ruchu globalnego dżihadu*, Poznań 2010, pp. 215–216 et passim.

[33] A. Krzak, *Niebezpieczeństwo terroryzmu dla państw narodowych na Bałkanach*, [in:] *Problemy bezpieczeństwa wewnętrznego i bezpieczeństwa międzynarodowego*, ed. Krzysztof M. Księżopolski, Warszawa 2009, p. 439 et passim.

[34] *Długie brody i krótkie spodnie*, 4.02.2010, http://mojesarajevo.blogspot.com/, [access: 12.04. 2018].

where mujahedeen community established by members of El Mujahidin was active. In the action some members of Wahhabi sect with its leader Nusret Imamović were arrested. Imamović, having been instructed by Osama bin Laden, presented his radical, justifying terrorist attacks views on the Internet. In the premises of the sect there were weapon and propaganda materials in Arabic found.[35] The investigation revealed that Bosnian Wahhabis cooperated with a similar sect from Novi Pazar. According to Serbian authorities, the arrested took part in planning terrorist attacks in Western Europe and one of the attacks was supposed to take place during the burial ceremony of the Pope John Paul II.[36]

Although after 1995 mujahedeen activities in the Balkans have been weakened, the phenomenon cannot be underestimated because in the 21st century terrorist nets related to Muslim fundamentalism started to recover. A new strike team of terrorist suicide bombers started to act in 1996, and it was comprising young nationals of Bosnia and Herzegovina with fair hair and bright eyes. They were imitating terrorists from the Middle East, and were trained in explosives and suicide operations. Al Qaeda leaders decided to recruit new terrorists from among Slavs creating the "White Al Qaeda", more difficult to identify and to trace because of the European look of its members.[37] In the middle of 2013 radical Islamist leaders accepted a plan called The Balkans 2020 by Ayman az-Zawahiri[38], in which the Balkans are one of the centres of the Islamic terrorism, playing at the same time a key role in Al Qaeda's strategy accepted to 2020. In the Balkans, and most of all in Bosnia and Herzegovina, Kosovo, Sandžak and Croatia there are still new terrorist recruitment centres established. Financial means for their activities come mostly from drug trafficking.[39] Enhancing actions in Western Europe is mainly based on collecting the White Al Qaeda and preparing its members for terrorist strikes. Until the end of 2014 about 200 terrorists in the age of 20-25 had been prepared for the attacks. They were trained in Islamic countries and it was financed by Al Qaeda's branch responsible for the Balkans and Europe. Then, the terrorists were placed mainly in Macedonia and Kosovo. In 2005 the training of suicide bombers was continued in the northern Albania and in Kosovo. There were women recruited from among widows who lost their relatives in the war, so they became the victims of the manipulation easily.

Many experts think that orthodox Islam believers started to settle down in the regions and countries, where they had not been before: so in Bosnia and Herzegovina, Kosovo, Serbia and Croatia and lately in Bulgaria. The League of Muslim World is responsible for spreading Wahhabism idea, and particularly its branch the World Council of Mosques, which finances the building of Muslim

[35] D. Halimović, *Vehabije u BiH: Od Bočinje do Maoče*, 6 February 2010, http://www.slobodnaevropa.org/, [access: 12 IV 2018].

[36] Ibidem.

[37] M. Drecun, *Alahovi ratnici*, Beograd 2008, pp. 305–310.

[38] Y. Bodansky, *Osama bin Laden człowiek, który wypowiedział wojnę Ameryce*, Warszawa 2001, p. 95.

[39] M. Drecun, *Alahovi ratnici*…, pp. 6–9, 304–305.

places of worship in the Balkans. In Kosovo they are built in the places of burned Orthodox churches. Moreover, new religious centres of Islamic cult were opened in the capital of this quasi state[40] every month in 2008. It should also be pointed out that the problem of the disputed province has its broader dimension, both of ethnic and religious nature as it is involved with Muslim community in the Old Continent.[41] Young Albanian elites living in Kosovo regard Serbs as their enemies and chant the slogans calling for the elimination of that "foreign" nation. The strong ties of this quasi state with Islamic terrorism go back to the times of the Kosovo Liberation Army (Ushtria Çlivimtare e Kosovës – UÇK), the Albanian organisation aimed at gaining the independence of Kosovo and the creation of the so-called Great Albania. Since 1995 UÇK has intensified fights using terrorist methods. During the next four years its members repeatedly took many actions of physical elimination of people of Serbian nationality (administration employees, security services officers mainly), as well as the so-called Albanian collaborators who were in favor of the coexistence with other nations living in Kosovo and those who were in favor of resolving the conflict with the peaceful methods.[42] The UÇK raids on the towns inhabited by Serbs were supported by the volunteer units of fighters from Bosnia and Herzegovina, which resulted in the escalation of ethnical tensions and it also increased the number of military conflicts and terrorist acts.[43] Murders and assaults were aimed to force Serbian minority to leave Kosovo and to provoke Yugoslavian army and militia maintaining the order in the province. Since 1997 UÇK had started regular fights with Serbs taking 30% of the Drenica region in Kosovo. Western countries regarded UÇK as a terrorist organisation until 1998; nevertheless, they changed their attitude because of the support given to the organization by the USA. Due to the growing involvement of the USA in the Kosovo conflict, in February 1998 the US State Department removed The Liberation Army of Kosovo from the list of terrorist organisations. The reason was that it became a desirable ally in fight with Slobodan Milošević's rule.[44] Growing animosities between Serbs and Albanians caused an outbreak of an open armed fight. The escalation of that fight resulted in the NATO military intervention in 1999 and in establishing the UN international protectorate in the province. Actions taken by international community

[40] On 17 February 2008 Kosovo formally annovnced its independence. The act was not recognized by Serbia. Independence of Kosovo is not recognizedby for exemple Russia, Spain, Cyprus, Romania, Greece and Slovania standing for affiliation of the disputed territory to Serbia. E. Bujwid-Kurek *Serbia w nowej przestrzeni ustrojowej. Dzieje, Ustrój, Konstytucja*, Kraków 2012, p. 94.

[41] K. Izak, *Leksykon organizacji i ruchów*..., p. 522.

[42] S. Schwartz, *Kosovo: Background to a War*, London 2000, pp. 137–143.

[43] T. Arbuckle, *Unhealthy climate in Kosovo as guerillas gear up for a summer confrontation*, „Jane's International Defense Review" 1999, no. 2, p. 60. Serbian and Russian special services reported many times on links between UÇK and Al Qaeda, and Osama Ben Laden was involved in financing the Liberation Army of Kosovo. He passed Albanian terrorists 500 to 700 million US dollars. Paul L. Williams, *Al-Kaida. Międzynarodowy terroryzm, zorganizowana przestępczość i nadciągająca apokalipsa*, Poznań 2007, p. 88.

[44] D. Gibas-Krzak, *Serbsko-albański konflikt o Kosowo. Uwarunkowania – przebieg – Konsekwencje*, Toruń 2009, pp. 178–183.

did not solve the conflict. During the fights UÇK became a conglomerate of various military groups, aim of which was to establish the so-called Great Albania. There were units financed by intelligence services from the USA, Germany, the UK and Croatia. Police actions aimed at Muslim radicals were often followed by arrests, seizure of the rifles and ammunition. According to special services, Kosovo (like Bosnia and Herzegovina) has become an area where terrorists fighting in the Islamic State ranks and on different fields of jihad are recruited. There are theories that they also take part in attacks on civilians in Western Europe.[45] Recruitment of the White Al Qaeda was a success, as police investigations and special services reports confirmed. According to the American intelligence assessments, in 2004 there were about 6,000 people from Albania, Bulgaria, Macedonia, Kosovo and Bosnia and Herzegovina who had direct or indirect links to Al Qaeda. British antiterrorist units stationing in Sarajevo detected links between terrorists responsible for London attacks of 7 July 2005 and members of Bosnian cells. In 2005 members of the Sarajevo group equipped in explosives were arrested. Also a terrorist group Maximus, Al Qaeda's cell for Northern Europe, active in Sarajevo canton was dismantled. Its leader was 19-year-old citizen of Sweden Mirsad Bektašević. He was responsible for recruitment of young Muslims for bin Laden's net. Terrorists planned to carry out an attack on the EUFOR in Sarajevo. In March 2005 next five suspects were arrested for contacts with Muhammad Porča, a radical imam from Vienna.[46]

The base in the Balkans has been established to enable terrorists to get to Western Europe quicker. Another alarming phenomenon is its radicalisation, building of paramilitary structures, establishing close cooperation with Al Qaeda and other extremist or terrorist organisations. It does not remain a mystery that the Balkans are one of the regions which inhabitants joined terrorist networks of the Islamic State to a large extent. According to the CIA data, as well as other special services from different countries, even hundreds of people could have left the Balkans for Syria and Iraq.[47] According to the analyses of Israeli special services, Islamic humanitarian organisations are constantly sending funds for Muslims of Bosnian and Albanian origin laying the financial foundations for the future actions of terrorist nature.[48] Bosnian security services assessed that there can be about 3,000 armed Islamists in the country.[49]

---

[45] *Džihadisti iz BiH. Ako BiH uđe u EU, mnoga vrata će nam biti otvorena* (2016), http://www.nezavisne.com/novosti/bih/Dzihadisti-iz-BiH-Ako-BiH-udje-u-EU-mnoga-vrata-ce-nam-biti-otvorena/353577, [access: 25 III 2018].

[46] K. Izak*, Radykalny islam na Bałkanach źródłem konfliktów społecznych i terrorystycznego zagrożenia dla Europy*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, no. 9, p. 54.

[47] K. Karnowski*, ISIS pokonane. Upadł ostatni bastion Państwa Islamskiego w Syrii*, 4.11.2017, https://wiadomosci.wp.pl/isis-pokonane-upadl-ostatni-bastion-panstwa-islamskiego-w-syrii-6184061996299905a, [access: 12 IV 2018].

[48] *Lieberman: Balkans the next target of Worldwide Jihad*, 6.01.2010*,* http://serbianna.com/news/archives/3788, [access: 12 IV 2018].

[49] *Bosnia: 3,000 militants pose grave security threat'*, 13.07.2010, http://www.adnkronos.com/AKI/English/Security/?id=3.1.677269022, [access: 12 IV 2018].

Radical Islamists actions still pose a serious threat to security, the example of which is the attack on the American Embassy in Sarajevo perpetrated by Mevlid Jašarević on 28 October 2011 under the slogan of revenge for Gaddafi.[50] In January 2015 during the Charlie Hebdo attack in Paris there was weapon and ammunition from Bosnia and Herzegovina used. In November 2015 in the suburbs of Sarajevo two Bosnian soldiers were killed by a member of Wahhabi sect. The same year near Mostar, there was a car bomb attack in which the head of corps staff in Military Forces of Bosnia and Herzegovina, General Anto Jeleč travelled. In 2016 Bakir Izetbegović, a former member of the Presidium of the Republic of Bosnia and Herzegovina assessed during the Organisation of the Islamic Cooperation summit in Istanbul that his country suffers from a syndrome of religious extremism development combined with the instances of terrorist acts.[51] One could make a hypothesis that other terrorists are likely to prepare next attacks aimed against US diplomatic missions, against NATO bases or military forces of Bosnia and Herzegovina sent in order to take part in operations abroad. One should not be astonished by the popularity of fundamentalist movements and increase in the number of their supporters in Bosnia and Herzegovina. There are approximately 100 000 believers and followers of radical Islam movements in the country who are waiting for the chance to prove that they are true Muslims. And they are able to do it in very drastic and radical way.[52] Bosnian sources claim that nowadays Muslim extremists take part in the military trainings in the town of Mahnjača on the border of Teslić commune in the republic of Serbia and Zenica commune in the Federation of Bosnia and Herzegovina.[53] New studies also indicate that new training camps for fundamentalists are being established. The most important ones located in Bosnia and Herzegovina are in the town of Ošve, 250 km from Belgrade, Dubnica (as the centre of jihadists) and Jezera which was bought by Wahhabi sect. In Serbia there is also Furkan centre in Novi Pazar where volunteers for fights in Syria and other jihad battlefields are recruited.[54]

Impacts of Islamic terrorists in Bulgaria, Albania, Macedonia and Greece

Not only the countries of the so-called Western Balkans have experienced this dangerous phenomenon of Islamic terrorism linked to radical Islam movements. In Bulgaria almost one sixth out of the total number of 7,1 million inhabitants are Muslims who are Sunni believers. For the last 20 years the country was able to keep ethnical

[50] S. Mišljenović, *Vehabija iz Novog Pazara pucao na ambasadu SAD*, 28 X 2011, http://www.novosti.rs/vesti/planeta.70.htm, [access: 12 IV 2018].

[51] F. Alispahić F., *Posrbljavanje bošnjačkog liderstva*, „Preporodov Journal" 2016, p. 40.

[52] *Egipćanin okuplja vehabije u* BiH, 21 V 2011, http://www.rtv.rs/sr_lat/region/egipcanin-okuplja-vehabije-u-bih_254995.html, [access: 12 IV 2018].

[53] Ibidem.

[54] *Ako nas Srbija ne spasi terorizma, onda smo načisto propali*, 24.08.2015, https://www.fokus.ba/vijesti/globus/ako-nas-srbija-ne-spasi-terorizma-onda-smo-nacisto-propali/100222/, [access: 12 IV 2018].

balance although the expansion of Wahhabism is also seen there. Since the mid-'1990s significant amounts of money were allocated for more than 150 new mosques and the so-called "educational centres", aimed at spreading Wahhabi ideas.[55] There are 1050 mosques in the country and new ones are built mostly with the money from Saudi charity organisations. They also finance scholarships of Bulgarian students in religious schools in Saudi Arabia and Jordan.[56] The authorities try to suppress fundamentalist tendencies and in many cases these activities are successful. In 2003 a few Islamic centres, financed mainly by Saudis, were closed. Nevertheless, the researchers claim that the number of fundamentalist centres and madrassas teaching Wahhabi rules is increasing, particularly in the south and north-eastern Bulgaria (Plovdiv, Kazanlak, Velingrad, Bilka, Razgrad). At the same time the most dangerous is that some schools controlled by Islamic radicals are not subjected to any state control.[57]

Only some Balkan countries are able to take effective counter-terrorist measures. Albania remains an exception; its authorities have been effectively cooperating with Western European and American institutions fighting Islamic terrorism for a long time. And it seems that their effectiveness can be a good example for other countries of the region. One of the most spectacular examples of such policy was an action carried out by special services and the police between 2004 and 2006. It was to suppress a sedition of a Saudi businessman Yasin Abdullah al Khadi, who had been cooperating with Al Qaeda and other terrorist organizations. He was running his business in Tirana and he was a leader of a charity organization and that made it easier for him to support terrorists as well as to assist in establishing local Islamist centres. At the same time a group of fundamentalists suspected of financing terrorism and taking part in Egyptian Islamic Jihad was removed from Albania.[58]

Nevertheless, there is an alarming situation in Macedonia nowadays where growing radical Islam currents contribute to the split in Muslim societies. In an officially running Islamic Religious Community one can perceive a struggle for power between moderate representatives of the main stream and a branch of Wahhabis, who fight for the influence and money among themselves. In this case religious divisions are related to ethnic divisions, which are not beneficial to the state stability but they only generate further tensions and threat to security.[59] It should be stressed that the radicalisation of Muslim society took place along with the collapse of communist Yugoslavia in this territory. In January 1992 Albanians from Macedonia voted in favour of setting up an autonomous republic of Illiryda. Following the separatists from Kosovo they started to create illegal organisational structures including schools and universities. After

[55] *Bałkany coraz bardziej islamskie*, https://euroislam.pl/balkany-coraz-bardziej-islamskie/?print=print, [access: 12 IV 2018].

[56] K. Izak, *Leksykon organizacji i ruchów*.., p. 525.

[57] *Bałkany coraz bardziej*... https://euroislam.pl/balkany-coraz-bardziej-islamskie/?print=print, [access: 12 IV 2018]. *Terrorism in the Balkans*..., pp. 8–9.

[58] K. Izak, *Leksykon organizacji i ruchów*.., p. 521.

[59] I. Stawowy-Kawka, *Miejsce ludności muzułmańskiej w Macedonii – przemiany i perspektywy*, „Prace Komisji Środkowoeuropejskiej PAU" 2014, vol. XXII, p. 135.

the Kosovo War in 1999 political aspirations of Albanians increased. They started to demand the status of equivalent nation in Macedonia and annexation of border regions to Albania. In 2000 a Macedonian branch of the Liberation Army of Kosovo triggered incidents on the borders of Macedonia and Kosovo. There was a rebellion of the Liberation Army of Kosovo in spring 2001. On 15 march 2001 Albanians attacked Tetovo. Islamic fundamentalists also took part in the rebellion and they were supported by Kosovars, who had not been disarmed by international forces. The offensive of Macedonian troops led to the withdrawal of the separatists to the border areas but fights were ceased after the diplomatic intervention of the West.[60]

Macedonian authorities unwillingly admit to the threat posed by the radical Islam although facts seem to confirm the threat. In 2007 three Albanian brothers from Macedonia together with a Jordanian, Turk and Albanian from Kosovo, all living in the USA, were supposed to take part in preparations of the attack on Fort Dix, American military base in New Jersey. In May 2010 four extremists transporting weapon were killed in a police action near Skopje.[61] Although Macedonia belongs to international coalition of countries fighting with terrorism, it cannot be dispensed from tracing and responding to any possible terrorist activity. Moderate Muslims admit that at present five mosques in Skopje are under control of Wahhabis, despite the fact that the Islamic Religious Society banned Ramadan Ramadani (alleged leader of the movement) from organizing services and serving as imam in Isa Beg mosque in Skopje. While seeking followers to overthrow present authorities of the Islamic Religious Society, Ramadani rejected accusations of radicalism and denied the reports of any threats from Islamic political and religious movements.[62]

According to Ioannis Michaletos, Greece lying in the Balkans between Turkey and Northern Africa, located in the Mediterranean, not distant from the Black Sea and the Middle East is an important transit zone for international terrorism and it serves as a corridor for jihadists. Greece is also a convenient place for the attacks of lone wolves who can act immediately and in a spontaneous way without any need of tight links to terrorist nets. Lone wolves seem to constitute the next mainstream in modern terrorism, particularly dangerous for Greece which is vitally important from a tourist's perspective.[63] Between 2015 and 2016 a huge wave of immigrants flooded Greece and went further to Europe. At the same time a new group of non-governmental organization emerged in order to help refugees. However, among them there were many organisations connected to different fractions of political Islam such as Islamic Relief Worldwide, which closely cooperated with terrorist net established by the Muslim Brotherhood. It rooted in Greece as an organization helping migrants, although in November 2014 it was officially recognized as terrorist

[60] A. Koseski, *Główne problemy transformacji w Republice Macedonii (1991–2000)*, [in:] *Transformacja systemowa w krajach Europy Środkowej, Wschodniej i Południowej 1989–2002*, ed. T. Godlewski, A. Koseski, K.A. Wojtaszczyk, Bydgoszcz – Pułtusk 2003, p. 160.

[61] K. Izak, *Leksykon organizacji i ruchów…*, p. 525.

[62] *Bałkany coraz bardziej islamskie…*, https://euroislam.pl/balkany-cora-bardziej-islamskie/?print=print, [access: 12 IV 2018].

[63] The so called *lone wolves* can be dangerous for other Balkan countries as well.

organization by the United Arab Emirates. The organization financed for example Hamas and in July 2014 authorities of the US Missouri State stated that the local, American branch of the organisation transferred 1,4 million US dollars to terrorists in Iraq and Afghanistan. Furthermore, Russian special services indicated that Islamic Relief tends to sponsor Caucasian jihadists. The Greek analyst identified also other linked to Islamic terrorism organisations, which are active on a Greek island of Lesbos, i.e. Al Muntada Trust and One Nation NGO. The first finances Nigerian extremists, the second provides weapons to Syria and is linked to Turkish organisations known for supplying the ISIS with weaponry. It also maintains contacts with Al Qaeda.[64]

Conclusions

According to different intelligence assessments in the so-called Western Balkans there are about a few thousand people linked to Al Qaeda and other terrorist organisations. The leaders are identified and to a large extent the same also applies to the names of the members of such organisations for example Sahid Emir Musa Aiza (veteran of the Afghan war) who are responsible for the recruitment of Slavic people of Islamic faith. Such young people are found mainly in Bosnia and Herzegovina, Bulgaria, Macedonia, Kosovo and Sandžak. Ayman az-Zawahiri is regarded as the main leader of terrorist underground in the Balkans. The number of mujahideen fighters, who had come there during the war, undoubtedly decreased. But their followers were left there which contributed to the fact that the Balkans became popular among many terrorist organisations and they also became an arena of struggles for power and influences of different Muslim countries. International situation was also favourable because many Balkan countries has not been able to cope with numerous internal problems of social and economic nature since the Cold War. There is high unemployment, economic stagnation, local politicians focused more on struggle for power and fuelling ethnic and religious conflicts rather than on necessary reforms. It all generates frustration in the young generation that do not see any perspectives. Therefore, its representatives are "an easy prey" for recruiters from terrorist organisations.[65]

One cannot ignore the aspect of natural environment, which is beneficial to terrorists. Training camps and bases can be inaccessible for special services and the police because of topography. In distant parts of the Balkans, particularly in the mountainous part of the region, there are convenient conditions for the development of modern and global terrorist organisations. This is even more dangerous because the Balkans are one of the most important interfaces between organisations from the Middle East and their goal is the expansion to the Northern and Eastern Europe. One of the most dangerous aspects of this proximity is the development of terrorist net and recruitment

[64] I. Michaletos, *Contemporary risk assessment of extremism and terrorism in Greece. The case of Islamist-driven security risks in Greece*, [in:] *Terrorism in the Balkans...*, pp. 187–195.

[65] Vide: *Paradoxes of stabilization. Bosnia and Herzegovina from the perspective of Central Europe*, ed. M. Szpala, OSW Report 2016, no. 2.

of future terrorists, particularly in the form of a "white jihad". Muslim countries after the civil war in Yugoslavia did not stop financing actions which goal was the promotion of Islam in the region. The financial means come from not only governmental institutions but also from private charity organisations.[66] There are frequent examples of religious indoctrination in educational institutions in post-Yugoslavian countries, where those children who worship religion other than Islam are discriminated because of that.[67] Also social networking sites spreading rules of the radical Islam and harsh criticism of Western culture and way of living are becoming more and more popular in the Balkans. These include official websites of radical organisations for instance "Young Muslims" or the websites of Islamic communities. All of these cause that radicalising Islam and its terrorist cells can contribute to the a new conflict in the Balkan powder keg.

Abstract

The author of the article presents a phenomenon of terrorism in the Balkans throughout the 19th, 20th an 21st centuries. She highlights a thesis that specific phenomenon of terrorism in the region requires additional studies, mostly of heuristic nature. Among the types of Balkan terrorism there is terrorism connected to national and liberation movements and political terrorism. Furthermore, terrorist actions in Romania and Bulgaria, terrorism of the Ustashe and terrorism of the anti-Yugoslav emigration and other its forms have been indicated. A particular attention has been paid to terrorism connected to extreme streams of Islam, which appeared in the Balkans as the aftermath of the civil war (1992–1995). In the post-Cold War era Islamic terrorism in the Balkans is linked to a growth of influences of Muslim fundamentalists. The author proves a thesis that due to their topography the Balkans create a great possibility for the development of training camps and bases for terrorists linked to a global jihad. It poses a threat to the security of Europe and its democratic societies because of the probability of inciting a conflict, not only on a local but also broader, even non-European scale.

Keywords: international terrorism, Balkans, political terror, Islamic fundamentalism, Wahhabi sects, net of a global jihad.

[66] V. Janková, *Wahhabism in the Balkans. The case study of Bosnia and Herzegovina*, Praha 2014, p. 72.
[67] Ibidem.

Tomasz Safjański

Exposing terrorist activity by Europol – legal and practical considerations

Introduction

Europol is a platform of multilateral cooperation between law enforcement agencies, made up of police forces, border guards, customs, financial, migration, military police, and occasionally special services of the EU Member States. Established under the Maastricht Treaty. Europol started its operational activity on 3 January 1994 as the Europol Drugs Unit, "Eurodrug". The Convention on the establishment of the European Police Office (Europol Convention) was ratified and came into force.[1] The European Police Office (Europol) became fully operational on 1 July 1999.[2]

Artur Gruszczak distinguishes Europol as the key element of the European intelligence community, the position of which within the community results from its close relations with the EU institutions, agencies and organs (European Border and Coast Guard Agency - Frontex, EU Intelligence Centre – UE IntCen) and law enforcement agencies of the Member States.[3]

Europol's competences with regard to criminal intelligence

Europol's competences in exposing terrorist activities result directly from the Treaty on the Functioning on the European Union (TFUE).[4] According to Article 88.1 of the TFUE: *Europol's mission shall be to support and strengthen action by the Member States' police authorities and other law enforcement services and their mutual cooperation in preventing and combating serious crime affecting two or more Member States, terrorism and forms of crime which affect a common interest covered by a Union policy.* According to the Treaty (...): *Any operational action by Europol must be carried out in liaison and in agreement with the authorities of the Member State or States whose territory is concerned. The application of coercive measures shall be the exclusive responsibility of the competent national authorities.*[5] Pit transpires from the above quoted treaty provisions that the procedure of exposing terrorist activities

[1] Council Act of 26 July 1995 drawing up the Convention based on Article K.3 of the Treaty on European Union, on the establishment of a European Police Office (Europol Convention), signed in Brussels on 26 July 1995 (Journal of Laws 2005, no. 29, item 243, as amended).

[2] See more in T. Safjański, *Europejskie Biuro Policji Europol. Geneza. Główne aspekty działania. Perspektywy rozwoju*, Warszawa 2009.

[3] See more in A. Gruszczak, *Europejska wspólnota wywiadowcza. Prawo – instytucje – mechanizmy*, Kraków 2014.

[4] Consolidated version of the Treaty on European Union (OJ EU C 115 of 9 V 2008), p. 49.

[5] Ibidem, Article 88.3.

provided for within the framework of Europol's activity is fully legitimate and proceeds pursuant to international agreements. The cooperation, however, may be initiated once certain specified prerequisites are met. Understandably so, the operational potential of Europol cannot be exploited and taken advantage of on anybody's whim.

First and foremost, Europol's representatives are not even vested in the elementary competences enjoyed by the national services, neither e.g. operational and intelligence (surveillance, wiretaps), nor investigative (detaining and arresting people, searches, interrogation, securing forensic traces) powers, or general police empowerment (id check, body and luggage search, ship or air consignments check, coercive measures or the use of weapon).

The procedure of exposing terrorist activities by Europol is a multifaceted phenomenon. Under the explicit provisions of the treaty Europol is responsible for supervising a direct cooperation between all EU Member States with regard to combating, among others, the criminal activity of terrorism. Each Member State appoints competent national bodies – all of them authorised under the national legislation to prevent and combat transborder threats to cooperate within the framework of Europol's operations. The vast spectrum of forces available, including: police forces, border guards, customs, financial, migration, military police, and occasionally special services of the EU Member States has a decisive impact on the model of actions undertaken.

The Europol's counterterrorist-related activity is aimed at supporting and complementing actions taken by the Member States, contributing thus to their increased effectiveness. It is premised on the assumption that the relevant domestic services of the Member States are primarily weighed down with the obligation to combat any manifestations of terrorist activity. Europol initiates its terrorism countering activities only when the scale, extent or the nature of such threat exceeds the counteracting capabilities available at a national level.

Europol seeks to ensure adequate direction, cohesion and consistency of the actions undertaken by individual national services. In practice, the supportive counterterrorist function of Europol comes to the force, when coordination of national services activities within Europol is more effective than realized separately by individual member countries. The role of Europol is to support rather than substitute police services of the respective Member States.

The Regulation (EU) 2016/794 of the European Parliament and the Council of 2016 on the European Union Agency for Law Enforcement Cooperation (Europol)[6] details the scope of the tasks under consideration. In light of the Regulation Europol is obligated to:

– collect, store, process, analyse and exchange information, including criminal intelligence/operational data;

[6] The Regulation (EU) 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (JL UE L 135 of 24 V 2016, p. 53).

- notify immediately the Member States, through their national units established or designated, of any information and connections between criminal offences of their interest/within their concern;
- coordinate, organise and implement investigative and operational actions to support and strengthen actions by the competent authorities of the Member States;
- provide information and analytical support to Member States in connection with major international events;
- prepare threat assessments, strategic and operational analyses and general situation reports;
- support Member States' cross-border information exchange activities, operations and investigations, as well as joint investigation teams by providing operational, technical and financial support.[7]

Dismantling and operational exposing

Dismantling is an act originating from forensic study/tactics comprising **recognition** (acquiring maximum information on the place, object, adversary and the tactics of the future and current forensic activities); **detecting** (exposing a perpetrator, their tools and the manner the offence was perpetrated by collecting, assessing and analysing the information; **preventive role** (preventing criminal activities).[8]

Operational dismantling involves tactical and forensic activities by means of which criminal activity may be exposed. It comprises a set of planned and systematically executed operational activities aimed at individuals, legal persons, body corporate, or groups of people base on the presumption or acknowledgement of preparation, attempt or commission of a specified offence, or unidentified kind of criminal activity.[9]

Europol's actions are focused on:

- disclosing and identifying the location of security threats to the EU which bear the hallmarks of a terrorist activity,
- obtaining information sufficient to make hypothesis regarding an individual or terrorist organization having causal relationship to the threat,
- establishing further data to neutralize the threat (for example making an individual arrest, dismantling terrorist organization, foiling the attack).[10]

Information remains a prerequisite, which triggers the process of operational exposing of criminal (terrorist) activity. Its absence or poor quality puts the legitimacy of such undertaking into question.

[7] Ibidem, article 4.1.

[8] See. S. Pikulski, *Podstawowe zagadnienia taktyki kryminalistycznej*, Białystok 1997, p. 96 et seq.

[9] Parliamentary project of an act on operational actions, http://orka.sejm. gov.pl/proc6.nsf/projekty/353_p.htm, article 2 paragraph 4 [access: 24 V 2013].

[10] See. T. Hanausek, *Zarys kryminalistycznej teorii wykrywania*, part 2, Warszawa 1987, p. 3 et seq.

Analytical capability

Based on the inherent *sui generis* status of Europol exposing of criminal activities takes predominantly the form of an analytical study comprising special procedure of acquiring, verifying, gathering and distribution of criminal information and intelligence data. In the tactical and forensic dimension it involves engaging criminal analysis and information and intelligence data swapping to support operational cases or investigations of the overall similar nature occurring in the Member States. Actions taken within analysis work referred to as the Analysis Project, AP concentrate on a specific subject (person, environment) or an object (place, phenomenon).

From a technical and criminology perspective the analytical work makes use of special IT tools of database parameters, *the so called* "analytical databases", analysis work files (AWF), work files, work files for analysis, analytical files. To avoid misunderstanding, it should be pointed out that the "AWF" acronym refers in practical terms to a tactical as well as a technical aspect of the exposing procedure.

The AWF is used mostly in the cases of threats of the most difficult detection rate, with the detection and arrest of the most serious crimes (for example terrorist acts).[11] The underlying assumption is that the operational cases or inquiries conducted within the framework of different domestic jurisdictions are likely to reveal numerous links (whether subjective, objective or both). These links are indicative of a natural tendency displayed by terrorist organizations (international criminal groups) to get involved in cross-border criminality and the interpenetration of criminal markets. The starting point for the AWF is the identification of links between the cases run by the respective Member States. Under the preliminary data processing stage Europol's analysts seek similarities, relaying even on the most fundamental details like overlapping identification data, the address details, the bank account number. The AWF is launched once Europol determines that cases conducted by law enforcement agencies of a few Member States are related operationally, and the interested states recognize the need to launch integrated investigation. The relevance of information is analysed for the purposes of specific analytical study and individual national inquiry.

Information and data submitted by the Member States, gathered in the operational cases or domestic investigations are used for the purpose of analytical study. At the request of Europol or on their own initiative, national police units communicate to Europol all the necessary information for the purposes of analyzing a particular case and in a specific AWF. The Member States communicate such data only where processing thereof for the purposes of preventing, analyzing or combating offences is also authorized by the national law. From the analytical point of view it requires indicating a range of data to communicate concerning criminal investigations or operational cases in every Member State.[12] The data for analysis are transferred by

[11] See more: T. Safjański, *Działania operacyjne Europolu*, Szczytno 2013.

[12] Regulation (EU) 2016/794 of the European Parliament and of the Council of 11 May 2016 on the European Union Agency For Law Enforcement Cooperation (Europol) and replacing and

the national units of the Europol liaison offices to Europol in the form of contribution notes. They are verified by a project manager in terms of formal requirements. Further on, the information and data are entered into an analysis work file.

Methodology of the AWF relies mostly on criminal intelligence (mainly analysis and the exchange of information), and individual activities undertaken by the Member States (joint investigation teams). Within analysis work files there are general (strategic) analyses and detailed (operational) analyses.[13] **General analyses** are drawn up for the purpose of processing vital information on a defined, more extensive issue and enhancing initiatives launched by competent domestic organs. Detailed analyses are prepared to get specific information on criminal activities under Europol's competence. In the case of analysis of a general nature, all Member States learn about its findings in the reports developed by Europol and transmitted via liaison officers or experts.

The process of analytical study carried out by Europol involves also operational meetings. The cooperation between Europol's analysts and law enforcement officers is multifaceted. Apart from intelligence analysis Europol provides also expert support to the member states. It can be effected from the Europol headquarters or directly on site (the so-called mobile offices). The AWF, member states should ultimately create joint investigation teams directed to a particular criminal proceeding.

The goal of an analysis work file overlaps with the main goal of the detection process, i.e. it leads to gather complex intelligence data on terrorist activities and other information vital in the evidentiary proceedings. It is the analysis work file's task to indicate detection directions, loopholes in the case files and the need for information and data. The analysis work files allow to compare and check offences-related information from different sources and from scores of states. Analysts may search for information in all systems and data bases in Europol. This is how the system of information circulation and exchange is created. The system, in which information and data are exchanged between Europol preparing the analytical projects and domestic services running operational cases or investigations. The operational and analytical projects hold a central position in the system and facilitate conducting the cases or investigation by providing conditions for using information from other jurisdictions. Europol's analysis work files can be a direct basis for operational actions in the Member States. These projects enable Member States to supplement gaps in their operational recognition.

The Member States supply frequently analytical files containing solely fragmented pieces of information, which, upon merging operational analysis and the information from other Member States allow to identify international criminal structures and their dismantling. Participation in a project enables a dynamic exchange of information on groups and whole criminal structures. Information provided constitutes an analytical input providing the basis for further joint actions of the interested parties. Participants of an analytical project receive reports and evaluation of the case, which allows

repealing Council Decision 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ UE L 135 z 24 V 2016, p. 53).

[13] Ibidem, article 10.

constant monitoring of risks in the EU. Possible links are thoroughly checked to take preventive actions or detect actions possible. The operational analysis work files enhance detecting processes in the scope of international organized crime group.[14]

Each **operational analysis work file** requires the establishment of analytical analysis group, consisting of:

- Europol's analysts,
- other Europol staff designated by the Director,
- liaison officers from the Member States,
- experts from the Member States supplying the information or interested in the analysis.

Analysts are exclusively entitled to enter data to an analysis work file or make any changes therein. All participants of the analysis group may retrieve data from such file. Under the participation rules, the participants – according to their tasks – can be attributed a leading or supporting status. The leading role means collecting, processing and supplying information to the national unit, and the supporting role means the analysis of data from the police data systems in order to make the leading entity aware of the information for the purpose of analysis, as well as transferring information to Europol.

In practice an analytical group within a working file consists of Europol's employees, one of whom is the project manager, the others being analysts (with proper specific training[15]) and specialists. Furthermore, non-Europol employees usually law enforcement or governmental organisations staff or agents are additionally hired to resolve the issue. The same applies to the non-Europol employees who are law enforcement or other governmental organisations workers or agents of the so called third countries, exchanging information with Europol under relevant agreements. Europol's analysts, allocated to a particular project, cooperate directly with representatives of national operational or investigative teams. Their role is to show the need for source information necessary for the analysis and taking part in the evaluation of database contents. Europol is entitled to invite experts from the third countries to cooperate within an analytical group under the following conditions:

- there is an agreement between Europol and this particular entity or working arrangements regarding exchange of information, including personal data exchange, confidentiality of exchanged data,[16]

[14] See. P. Chlebowicz, W. Filipkowski, *Analiza kryminalna. Aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2011.

[15] Such trainings are performed in accordance with certain standards to give the possibilities of further cooperation between criminal analysts from different countries. Such trainings in Poland are performed in one educational center, the Police Academy in Szczytno. To prepare a criminal analyst specialized psychological test and job interview are needed as well as four-week training according to the ANACAPA program. During the training period participants get to know analytical techniques of information visualization and handling analytical program called *Analyst Notebook.*

[16] Countries covered only by a strategic agreement cannot be invited (Russia, Turkey). Danish Protocol allowed the possibility of passing data to a third country, which does not have any agreement on the operational cooperation with Europol in exceptional cases and in urgent situations on

- association of the experts from the entity is in the interest of the Member States,
- the entity is directly interested in the analytical works,
- all participants unanimously agree to include experts of the entity in the works of the analytical group.[17]

Analysis work files are a unique and most effective form of Europol's operational work offering many opportunities in the detection. The goal of analysis work files is to identify links between cases carried out in Member States. The procedure of analysis work files initiation is relatively complicated and embraces several stages. The most important are: proposing an initiative of opening an analysis work file, feasibility study of the analytical project, preparing documentation required to open the AWF and planning paperwork, introducing and opening the analytical project. The examples of analysis work file directed to detecting terrorist threats done by Europol for the past few years are shown in the table below.

Table. Europol's analytical work files regarding terrorist threats.

Name of the AWF	Subject of the analytical work file
Hydra	countering Islamic extremists groups or terrorist organisations. It also comprises financing terrorist groups by Islamic charity organizations, couriers with great amounts of money to finance terrorist acts, using forged credit cards, bank frauds, falsifying ID for terrorist purposes.
Dolphin	Countering terrorist groups indicated by the EU Council as posing serious threat to the EU Member States.

Source: private study.

AWF employs following tactical and criminalist modus operandi:

- criminal information gathering,
- operational criminal analysis,
- strategic criminal analysis,
- exchanging criminal information.

Gathering criminal information

The above mentioned AWFs are used for storing criminal information. They contain comprehensive intelligence gathered for criminal analysis purposes (both operational

the basis of the decision of Europol's Director.

[17] The Regulation (EU) 2016/794 of the European Parliament and the Council of 11 May 2016 on the European Union Agency for Law Enforcement Cooperation (Europol) and replacing and repealing Council Decisions 2009/371/JHA, 2009/934/JHA, 2009/935/JHA, 2009/936/JHA and 2009/968/JHA (OJ UE L 135 of 24 V 2016, pp. 53–114).

and strategic). The information is supplied by the Member State police forces (materials concerning operational cases as well as investigations). Groups of persons on whom data are stored:

- the file shall include data on persons, who, in accordance with the national law of the Member State concerned, are suspected of having committed or having taken part in a criminal offence in respect of which Europol is competent or who have been convicted of such an offence,
- persons regarding whom there are factual indications or reasonable grounds under the national law of the Member State concerned to believe that they will commit criminal offences in respect of which Europol is competent,
- persons who might be called upon to testify in investigations in connection with the offences under consideration or in subsequent criminal proceedings,
- person who have been the victims of one of the offences under consideration or with regards to whom certain facts give reason to believe that they could be the victims of such an offence,
- contacts and associates,
- persons who can provide information on the criminal offences under consideration.

The collection, storage and processing of the personal data such as racial origin, political opinions, religious beliefs and data concerning health or sex life is subject to a specific regime. Data are submitted by the Member States in their national languages or in English.

Exchange of criminal data within AWFs

It is a method of passing, making accessible collecting or receiving information by law enforcement agencies or other entitled entities. Europol is responsible for the exchange of information in accordance with the law. The provisions of the Decision on the Europol regarding exchange of information and intelligence provide framework for the action, making this exchange possible. They regulate the framework of information in Europol making analytical tasks possible by supplementing its data bases and information system. The legislation provides that Europol communicates information to relevant Member States authorities because the institution is obliged to notify the competent authorities without delay of information concerning them and of any connection identified between criminal offences. Within analysis work files there is information on criminals, offences and premises attached thereto, subjects, events, modi operandi, criminal phenomena and general threats.

The pattern of information exchange within an AWF has been worked out in cooperation with the Member States and agreed by the Heads of national units of Europol. It shall ensure that data security is complied with. This model provides for cooperation, both bilateral and multilateral. In practice the framework of information is as follow:

– Europol national unit – national liaison office – Europol,
– Competent national authority – national liaison office – Europol.

Operational criminal analysis

It shall be understood as a detecting instrument. It is used mainly in a multidimensional cases with numerous criminal leads, with complicated criminal links, vast information, the processing of which using traditional methods and techniques would be difficult or purely impossible. Operational criminal analysis is used first and foremost to gain investigative aim.

Methods which shall allow to establish modus operandi of a certain criminal activity, to identify links between different analytical objects (person, thing, place) and to establish structures of organized criminal groups are used within operational analysis. They are as follow:

- analysis of modus operandi,
- comparative analysis of crimes,
- analysis of criminal organizations,
- analysis of data stored in a file,
- financial analysis,
- analysis of methods used in a file.

The analyses generated in Europol can serve to start or support or facilitate investigations in Member States or accompany such investigations. It regards particularly proceedings which can be pursued only in accordance with provisions of the national law and by the competent national authority, which, however, have international links and international aspects that require tight cooperation via liaison officers of certain countries within Europol.[18]

Strategic criminal analysis

The basic role of strategic criminal analysis is supporting decision-making processes. The goal of its application is to submit to the Police decision makers more versatile material including diagnosis of potential areas of threats, their evaluated scale and the feasibility of their occurrence. Ultimately the material shall constitute a basis for coordinated and pre-emptive actions and thereby limit the number of unexpected or critical incidents. The above indicated approach is compatible with modern standards of the EU Member States law enforcement agencies, the so called *intelligence-led policing*. From the institutional perspective it is Europol that plays a leading role in strategic analysis in combating organised criminality.

Strategic analysis is focused on predicting direction and the volume of threats development, risk assessment as well as establishing priorities, mechanisms and strategy of counteracting. The substance of analysis concerns sources and resources of a criminal potential and targets of criminal activities. It also embraces some data research not connected to a particular investigation or proceeding, and therefore it does

[18] See. P. Chlebowicz, J. Kamińska, *Operacyjna analiza kryminalna w służbach policyjnych*, Warszawa 2015.

not apply to personal data. Nevertheless, in practical terms, this kind of analysis – next to operational (tactical) analysis – is perceived as an integral part of criminal analysis.

Strategic analysis is also a response to the needs in the scope of security policy and combating offence. Its consequence is that decision-makers receive an exhaustive material allowing the diagnosis of potential threats, their scale and prediction of its occurrence.

As part of strategic analyses Europol develops general reports concerning threat assessment and risk assessment, prepares recommendations concerning combating organized crime, phenomenology and structural analyses on the basis of intelligence submitted by the Member States or from other sources, which allows to recognize modi operandi, areas and structures of the criminal activities. Europol's criminal intelligence (including criminal analysis) unravels the picture of transnational criminality in the European Union.

Levels of AWFs

As far as AWF shortcomings are concerned, national police services had been pointing out their insufficient scope or too narrow focus. Some countries opted for opening analysis work files using only regional approach. Having the above under consideration, in 2013 analytical work files were divided into 3 levels:

1. Strategic,
2. Operational,
3. Targeted.

Strategic files

Aimed at processing data and information on organised crime and terrorism at the highest possible spatial and time scope. The analytical work files on a strategic level enable Europol to notify the Member States of the scale and threats development directions and provide them with data required to take pre-emptive actions (political decisions, changes in law). At present Europol leads two analytical work files on a strategic level: AWF Serious Organized Crime and AWF Counter Terrorism.[19]

Operational files

Aimed at gathering information on a particular sort of organised crime and terrorist activity or on a structure of organised crime threats in a particular region of the EU. These analytical files on operational level are called Focal Points.[20] They can focus on a particular geographical area (Balkans, Baltic Sea region), theme (Russian-language organised crime, Alban criminal groups), the area of criminal activity (human trafficking, VAT Fraud) or any particular commodity based (drugs, Euro counterfeiting).

[19] *Europol, New AWF Concept Guide for MS and Third Parties*, Haga 31.05.2012, p. 10, http://www.statewatch.org/news/2013/jan/europol-awf-new-concept.pdf [access: 15 II 2018]

[20] Ibidem, p. 5.

Target files

Dedicated to the detection of specific criminal organised groups or terrorist organisations, offences and their perpetrators. According to the vocabulary used by Europol, such analytical files on a target level are called Target Groups.[21] Intelligence gathered within target files is passed to the police services of the Member States. Police services have huge detection potential, which enables specific operational actions (for example surveillance, operational control) or investigative acts (arrests, search) to be taken on further by the national police force. For instance, in 2010 within a target group Europol supported anti-terrorist unit of the British Police in Greater Manchester county in their anti-terrorist operation. The British police submitted ca. 6,000 electronic documents, mainly in Arabic, which were subsequently adequately studied to identify people who might have posed a threat to security of the UK. Verification of those electronic files in Europol's systems revealed also existing other terrorist materials, which had already been used in a court as evidence. The result of Europol's work consisted of revealing of an extremist preacher, who was a subject of interest in other investigations in the EU. Europol used the materials passed by the Greater Manchester county police to analyse and assess ideology promoted by the suspect. The results of the analysis were a report and assessment of the threat from the suspect and his followers in Europe. The documents presented information on links to investigations conducted in Member States. The main suspect was sentenced to 2 years in jail after he was found guilty for charges under section 58 of *the Terrorism Act* in conjunction with possessing materials for terrorist purposes.[22]

The effectiveness of the above actions was possible as the outcome of intelligence being passed on by Europol to the Member States police services. The value of intelligence from analytical files is determined by the amount and the quality of criminal information submitted previously to Europol. It is the EU Member States which provide the information. This way there is a sui generis feedback loop between intelligence work done in the Member States and the work of Europol.

Conclusion

Based on the analysis of Europol provisions the following assumptions important for dismantling terrorist activities can be made:

- counterterrorist competences of Europol are strictly defined by the rules (it is precisely known what kind of activities Europol can take and what kind of activities cannot). Forms and methods of realizing the competences come from a solid practice of international cooperation;
- dismantling terrorist activities by Europol is mainly based on criminal intelligence, i.e. gathering, processing (analysis, assessment and interpretation), or exchange

[21] Ibidem, p. 7.

[22] *Europol's Review. Europol Annual Report 2010*, Europol, Haga 2011, p. 28.

of information and intelligence data. Using information and intelligence data submitted within the frame of investigations and joint investigation teams via Europol is subject to the same rules of data security as if it was obtained in the Member State which received the data;

- counterterrorist support shall be provided usually at the request of the Member State (with the exception of the so called spontaneous transmission of information);
- dismantling terrorist activities within Europol requires necessary professional standard of its officers. They have to have a specific professional knowledge, analytical capabilities and proficiency in English but also general, legal and cultural knowledge. Furthermore, they should have a good command of information tools. Cooperation within Europol is always associated with representing one's own country. Unprofessional actions cause damage to the image of the delegating country. They can also lead to legal accountability for the damages incurred.

To date Poland took part in a dozen of analytical work files, including AWF Islamic Terrorism (regarding terrorist activities of Islamic extremists) and AWF Hydra regarding terrorist activities of Islamic extremists). The system of processing information for the purposes of Europol's analytical work files in the Polish Police involves designating officers responsible for the coordination of passing information on each organizational level of the Police, designating officers to perform tasks within an analysis group established by Europol in support of a specific work file (national experts), development of procedures entailing processing this type of information and general AWFs functionality training. These assumptions were worked out more than 10 years ago in the Police HQ.[23]

National experts' tasks are:

- providing specific work files with information from preliminary proceedings or operational and intelligence activities;
- forwarding information from the work files to the national Police units and other law enforcement agencies;
- coordinating the Police cooperation with national and international partners as regards work files;
- taking part in meetings within particular work files that results from membership of Europol;
- initiating and performing information activities to boost the knowledge on work files within the Police as well as making information on activities

[23] They are the result of works of the teams established by the Decision No. 211 of the Police HQ of 21 March 2007 on establishing a team to develop a concept of quantitative and qualitative Polish contribution to Europol's Analytical Work Files and the Decision No. 47 of the Police HQ on establishing a team to assess capabilities of enhancing Polish engagement in international initiatives on countering Eastern European organized crime (not published) and *the Decision No. 60 of the Police Commissioner of 3 March 2010 on national experts performing their tasks within Europol's analytical work files* (Official Journal of the Police 2010, no. 3, item 11).

from the concrete work files available to law enforcement and public order institutions;
– forwarding information on their activities to a national coordinator during their meetings.[24]

National experts perform their duties in certain units of the Police HQ concerning tasks within analytical group established for the purpose of a certain AWF. They are obliged to give their support to police officers from the Police units.[25] National experts' tasks are as follow: obtaining relevant information and preparing contributions for AWFs, coordinating the Police cooperation with national and international partners as regards work files, taking part in meetings within particular work files that results from membership of Europol, initiating and performing information activities to boost the knowledge on work files within the Police as well as making information on activities from the concrete work files available to law enforcement and public order institutions. While performing their tasks national experts can request particular data from the Police organisational units. Upon the requests the Police units pass information concerning working files to national experts unless their passage would jeopardise the success of a current investigation or other operational and intelligence activities, or the safety of individuals involved.[26] National experts are seconded and supervised by the chiefs of organisation units from the criminal and investigation service of the Police HQ.[27] The chief of the unit competent in matters of international cooperation of the Police is responsible for coordination of national experts' activities. He organises meetings with national experts in order to give them assistance in fulfilling their tasks. He also designates a national coordinator to supervise national experts' work.[28]

Exposing terrorist activities is one of the most difficult tasks and requires some support actions (exchange of information, criminal analysis). Europol is engaged in operational criminal analyses in cases, where there is a strong need to establish links between separate elements of events in different countries, because of some signs (perpetrator, aggrieved) or aspects (place, time, modus operandi, subject of implementation). Obtaining intelligence data which increases the likelihood of detecting terrorist threats is possible due to international exchange of information and criminal analysis (for example combined analysis of telecommunication data from several Member States). In such cases the role of Europol is to build an information advantage of the national police forces taking up operational or investigative actions. Europol offers possibilities to obtain in-depth information on organised crime and terrorist threats for the purpose of national police services. Intelligence materials passed by Europol

[24] *The Decision No. 60 of the Police Commissioner of 3 March 2010 on national experts…*, section 4.
[25] Ibidem, paragraph 5, item 3.
[26] Ibidem, paragraph 5, item 1 and 2.
[27] Ibidem, paragraph 6 and 8.
[28] Ibidem, paragraph 7.

to Member States often contribute to detecting offences, organisational structures of criminal groups or terrorist nets. Gathering such materials by national police services in any other way than via Europol would be much more difficult. Europol's activities often allow to find additional threads or even to indicate potential evidence sources.

Basic role of Europol in detecting threats is based on the possibility of enhancing effectiveness of investigation actions on a national level. Most activities by Europol run parallel to national investigation proceedings. As the experience shows the analytical work files of Europol were often a starting point and a focus of detecting processes in numerous cases of international character. The assessment given does not diminish the value and basic significance of activities performed by competent services in Member States in the detecting processes. Detecting result of Europol's operational actions must comply with legal rules in Member States.

The main obstacle in Europol's effectiveness is still a diminished trust of practitioners (officers) to international cooperation formula while providing information to Europol's work files unwillingly (it refers mostly to sensitive criminal information on planned terrorist attacks). As a result Europol is not capable to prepare pre-emptive intelligence (that could prevent a terrorist attack). It can only trace financial flows connected to terrorism and indicate links between terrorism suspects, sources of illegal weapon or forged documents, but after a terrorist attack takes place.[29]

But sensitive criminal information is exchanged between liaison offices of the Member States in Europol. Copies of the information very rarely end up in work files. A direct cooperation between liaison offices is in reality a practice of avoiding central intelligence systems of Europol.[30]

Sharing criminal information within international cooperation is usually limited and sub-optima.[31] It results in the fact that Europol does not have sufficient capacities to dismantle terrorist activities. Because of the costs of obtaining criminal information concerning terrorist threats and their sensitivity, dismantling these threats will still be based on direct relationships between antiterrorist services of the EU Member States. Unfortunately, it is inconsistent with multilateral cooperation idea within Europol.

It is worth noticing that the interaction at the interface between antiterrorist intelligence services is a strategic situation that requires taking up decisions on whether to launch cooperation or not. From a political point of view taking up a cooperation is often contrary to operational interest of a particular intelligence service. In such a situation a conflict of interests can occur between the intelligence services. This relationship of interdependence between them can cause a situation that a conduct of one service tends to limit or make the other to act in a particular way as far as recognition, detection or prevention in countering terrorism is concerned.[32]

---

[29] T. Safjański, *Barriers to the Operational Effectiveness of Europol*, „Internal Security" 2013, no. 1.

[30] A. James, *Understanding police intelligence work*, vol. 2. Bristol 2016, p. 45.

[31] A. James, *Examining intelligence-led policing: developments in research, policy and practice*, Palgrave MacMillan 2013, p. 100.

[32] A. James, T. Safjański, *Europol's Crime Analysis System – Practical Determinants of Its*

Abstract

The article discusses the role of Europol in dismantling terrorist activity. Dismantling is a key step in the materializing by law enforcement forensics' functions: reconnoitring, detecting and preventing. The legal power of Europol to detect terrorism threats arise directly from the Treaty on the Functioning of the European Union. From the forensics point of view, Europol dismantling potential on terrorist activity is based on special analytical databases called analysis working files (AWFs). In this model, information and intelligence are collected, processed and exchanged with respect to strictly defined threats (persons, criminal groups, terrorist organizations) to support operational cases or penal proceedings conducted by EU Member States national police authorities.

Keywords: detection, international cooperation, Europol, special analytical searches, AWF's, EU security, forensics tactic.

Success, Policing: A Journal of Policy and Practice, Oxford University Press, Vol. 12, Issue 2 Published: 11 April 2018.

Dariusz Gradzi

Third Party Providers (TPP)[1] – new payment service providers in the Internet and mobile environment. Review of legal regulations and analysis of possible threats to cybersecurity of the paying critical infrastructure

Introductory remarks

Payment Services Directive (PSD I)[2] has introduced the notion of payment services to the European legal order and the closed catalogue of those services, as well as providers of payment services (so-called suppliers). Since its entry into force on the market, new paying electronic services based on Internet infrastructure have developed, including in particular services based on access to payment accounts (including banking) by third parties, which such permission is granted to the holder (user) of the account (e.g. bank client).

Electronic payments distinguishes between Internet payments[3] (made via the Internet) and mobile payments[4]. They may be carried out, inter alia, by means of payment using a payment card and by transfer orders [traditional bank transfer or the so-called Pay-By-Link[5] (PBL). The development of trade in the Internet environment

[1] The so-called Third Party Payment Service Provider – Supplier of payment services being a third party. Cf. M. Mostowik, *Legal Protection of payment account information in the light of account information services (AIS)*, Monitor of Banking Law, July – August 2017, p. 32.

[2] *Directive of the European Parliament and of the Council of 13 November 2007 on payment services in the internal market amending Directives 97/7/EC, 2002/65/EC, 2005/60/EC and 2006/48 EC and repealing Directive 97/5/EC,* Unit EU L 319/1 of 5 December 2007.

[3] B. Chinowski, *Electronic Payment methods. Essence, development, projections,* Electronic version: https://www.knf.gov.pl/knf/pl/komponenty/img/Elektroniczne%20metody%20platnosci.pdf P. 5 [access: 20 X 2017].

[4] These are payments made using the mobile equipped in the operating system, with a multimedia interface using radio technology, telecommunications networks WI-Fi(GSM, GPRS, UMTS, Wi-Fi, Nfc, Rfid, Bluetooth), Final Recommendations for the Security of Payment Account Access Services Following the Public Consultation, the European Central Bank https://www.ecb.europa.eu/pub/pdf/other/pubconsultationoutcome201405securitypaymentaccountaccessservicesen.pdf. [access: 25 X 2017].

[5] This is an Internet payment method that involves the fact that when shopping online, during the payment through the "payment gateway" the customer a special link that directs it to bank who runs his account and after logging in to the electronic banking system there is a supplemented format the transfer with the recipient's data (usually the billing agent) and the amount. After authorization the recipient gets a message about execution and can proceed to fulfill the contract, which significantly speeds up online transactions. The condition of the payer's use of this service is its sharing by the bank in which the payer has an account. Cf. M. Grabowski, *Payment Instruments in Polish law*, Warszawa 2013, https://depotuw.ceon.pl/bitstream/handle/item/327/Instrumenty%20Płatnicze%20w%20prawie%20polskim.pdf?sequence=1, p. 211 [access: 4 X 2017].

and the need to accelerate the execution of the payment process has led to the evolution of the initiating services by introducing an interface (so-called "Payment gateway", "Payment Gate") linking the merchant website (e.g. with the payment service provider's website (e.g. bank).[6] In addition to the payment services traditionally designed to make payments between the payer and the recipient of the funds (or the entity acting on the basis of the contract,e.g. a clearing agent), new complementary services have emerged, referred to in this article and which introduces the second directive on payment services (PSD II)[7]:

- third party payment initiation service,
- third party access to account information service,
- confirmation of availability of funds on payment account.[8]

The above services provide the user with the opportunity to expedite the payment transaction and aggregated[9] online information about the payment account, provided through the interface of the payment account provider. With this last service, you have the ability to quickly orient yourself to your financial situation.[10]

The object of this study will be the presentation of new payment services introduced to the European and the same Polish legal order by the PSD II Directive and micro and macro threats which may involve the functioning of new Payment services. The cornerstone of these rules in the PSD II directive is the granting of rights to the payers to use third party providers (TPP) and the need to respect this right by the payment account provider (including bank) – the so-called Account Servicing Payment Service Provider (ASPSP), as appropriate mechanisms are provided for the[11] legal which break with possible lack of willingness to cooperate by ASPSP of TPP.[12] For this reason, ASPSP were forced to work legally to cooperate with TPP. In current market realities ASPSP often prevent the development of TPP by: blocking specific IP addresses[13] or blocking the payer's bank account[14] and preventing the so-called Screen Scraping.[15]

---

[6] Cf. Recital 27 of the preamble to the PSD directive.

[7] *Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC, 2013/36/EU and Regulation (EU) 1093/2010 and repealing Directive 2007/64/EC*, Dz. Unit. EU L 337/35 of 23 December 2015.

[8] Unlike the Payment Initiation service and account information services, the process of confirming the availability of cash is not a separate payment service. Cf. K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 85.

[9] It refers to all kinds of information regarding multiple-element sets of unitary objects or multiple-element sets of features of those objects. Cf. J. Oleński Ekonomika informacji. Podstawy, Warszawa 2011, p. 209.

[10] Theme 28 Recital Directive PSD II.

[11] Sanctions of the supervisory Authority – the KNF, the obligation to notify of Art. 68 paragraph 6 PSD II.

[12] Should be noted that the business terms of TPP are direct competition for ASPSP.

[13] Internet Protocol (IP), Cf. http://munitus.pl/co-to-jest-ip.html [access: 4 X 2017].

[14] Cf. M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 33.

[15] Screen Scraping – The method of access to the user's online banking, whereby the client

Statistical and hazard data

The feature of common services TPP is the fact that in order to perform them is necessary to gain access by a third party (TPP) to a payment account (banking). The development of non-cash payments, including electronic due to continuous technological progress, has led to the emergence of new payment services in the form of services based on access by third parties to payment accounts (including banking). PSD II is not creating these services in the factual context, but merely trying to capture them in a regulatory aspect, because until now, although they have been operating on the financial market for many years, they have not been in a legal regulation. Services of this type have hitherto remained outside the regulatory area, because in their case there is no entry by TPP in possession of cash[16], which allowed them to benefit from the exclusion of the application of the PSD and the Payment Services Act (UUP)[17] in the wording before implementation to the Polish legal order PSD II.[18] PSD II has brought changes in the form of necessity – in principle – to obtain the authorization of the supervisory authority (in Poland – the Financial Supervision Commission) to provide these services.

The services of TPP are designed to facilitate and expedite the making of payments in the Internet environment. However, attention should be paid to the possible dangers that will entailed the emergence of new services and new suppliers in the context of the following statistics. Statistics show that the number of detected cyber attacks in Poland in 2015 in comparison with 2014 was increased by 46 percent. The biggest risk factor for the financial sector is the threat of attacks on IT systems.[19] In 2014, in Poland, approximately 230,000 computers had malicious software installed, of which 50,000 of cases were malicious software in the form Trojan Bank.[20] The number of mobile banking users over the last 4 years has risen to about 8.2 million (an increase of 680 percent).[21] In the same

authorizes the bank (e.g. in which the credit is applied) to log in to his payment account at another bank (where the user has the payment history) by means of log the first bank login data. Logging in by analysis banking interface content by the IT system First Bank, which automatically enter the Customer's login and password in the specified fields and login to the online banking system. Cf. The warning issued by the KNF 14.07.2014, "*Risks associated with giving another bank login data"*, https://www.knf.gov.pl/?articleId=53072&p_id=18 [access 23 X 2017].

[16] Art. 6 paragraph 10 UUP from ZW. with article 3. 3 (a) 1 PSD I.

[17] *Payment Services Act of 19 August 2011* (OJ no 199, item 1175, Subsequent. D.).

[18] *The act of financial service law of 10 May 2018 Amending the Payment Services Act and certain other provisions of the (OJ 2018, item 1075).*

[19] Information Technology, http://zasoby.open.agh.edu.pl/~08pdiakow/indexb0c5.html?q=node/37 [access: 4 X 2017].

[20] Cf. A. Marciniak, bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, pp. 181–182 [access: 2 X 2017].

[21] Cf. Research reports conducted by the PRNews.pl portal In the fourth quarter of 2012 and I Quarter 2017, https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-i-kw-2017-360755

way, the number of owners of mobile banking smartphones in 2013 was 12 percent, whereas in 2015 already 43 percent.[22]

The number of non-cash transactions is increasing on average 15 percent year-to-year. The number of transfer orders increased from PLN 31 trillion in the year 2010 to 47.5 trillion ZL in the year 2015. The share of transfer orders in the year 2015 in general non-cash transactions amounted to 45 percent. In all non-cash transactions, the number of transactions with a credit card amounted to 54 percent in the year 2015, while in 2010 it was 36 percent. Card transactions in the years 2009-2015 reached on average a year increase of 24 per cent.[23] The number of payment cards issued in Poland in the year 2014 more than 36 million.[24] In 2013, the share of fraudulent card transactions in the value of all card transactions amounted to 0.005 percent.[25]

In parallel between 2005–2015, there has been a dynamic increase in the acceptability of payment cards (networks constituting the so-called POS points of sale – where payment by credit card is accepted) from 55 thousand POS points in 2005 to 184,000 in 2015. The number of single POS terminals to accept payment cards has increased during this period from 129,000 to 463,000. The percentage of Poles actively using the bank account over the Internet is also growing. In 2009 it was 46 percent, while in 2016, 69% percent.[26] Number of bank accounts held for private individuals by banks, branches of institutions and credit unions increased from 44 million in 2010 to 58 million in 2015.[27]

In the first quarter of 2017, more than 15,000 merchants were seen on the Internet[28] and 11.5 million payment transactions. The value of these transactions amounted to 1.78 billion. On average, more than 128 000 transactions were recorded.[29]

These statistics show the enormous and irreversible trend of the growth of non-cash payments and electronic payment transactions.[30]

[access: 23 X 2017]; https://prnews.pl/raport-prnews-pl-rynek-bankowosci-mobilnej-iv-kw-2013-16158 [access: 23 X 2017].

[22] Cf. A. Marciniak, Bank CERT – New weapon in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of banking Informatics 2016*, Gdansk 2016, http://www. Efcongress. com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 181-182 [access: 2 X 2017].

[23] *Status of cashless trading in Poland*, https://www.mr.gov.pl/media/30118/Rozwoj_obrotu_bezgotowkowego_112016.pdf [access: 10 X 2017].

[24] Comparison of selected elements of the Polish payment system with the systems of other European Union countries in 2015 https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_2014.pdf, p. 18 [access: 10 X 2017].

[25] Ibid p. 31.

[26] D. Maison, *Attitude of boxes towards non-cash trading. Test report 2016 and comparative analysis with data from 2009 and 2013,* https://www.nbp.pl/badania/seminaria/8v2017.pdf [access: 10 X 2017].

[27] *Comparison of selected elements of the Polish payment system with the systems of other countries of the European Union for 2015*, https://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/porownanie_UE_2014.pdf, p. 6 [access: 10 X 2017].

[28] E.g. online store is which accepts.

[29] *Information on payment cards and quarter 2017*, https://www.nbp.pl/systemplatniczy/karty/q_01_2017.pdf, p. 36 [access: 10 X 2017].

[30] *Status of cashless trading in Poland*, https://www.mr.gov.pl/media/30118/Rozwoj_obrotu_

This data leads to the conclusion that the activities of TPP especially in the initial period should be particularly supervised and verified, given the potential risks to the financial ecosystem, which is based on the mutual trust of its participants and caring for the safety of end users.

Payment services and their suppliers-legal characteristics

Before further analysis, it is necessary to present deadlines which will help to understand the process of electronic payment and its participants. According to the Polish Payment Services Act (UUP):

- *Provider* – is a payment service provider. UUP contains a closed catalogue of suppliers, which may include national banks, credit institutions, electronic money institutions, payment institutions, credit unions or payment service bureaus, which means that other companies are not allowed to provide these services under penalty of criminal[31],
- *Merchant* – It is a recipient other than the consumer for whom the accounting agent provides a payment service (e.g. a shop or an online store). This is the entity that accepts the payment in a non-cash form[32],
- *Payment service* – It is a service whose essence is the change of ownership of funds, e.g. a bank transfer where funds from an account in one bank are credited to a user's account in another bank. This service therefore aims to allow the payer to transfer funds to the payee. UUP introduces a closed payment service catalogue,
- *User* – It is a natural person, legal entity or an organizational unit not being a legal person, which the law confers legal capacity, using payment services as payer or consignee,
- *Payer* – It is a natural person, legal entity or an organizational unit which is not a legal person, which the law confers a legal capacity to make a payment order leading to the debiting of its payment account or the payment of funds (the entity making payments),
- *Recipient* – it is a natural or legal person, or an organizational unit which is not a legal person, which the law confers the legal capacity of the recipient of the funds constituting the subject of the payment transaction (the entity receiving the payment),
- *Payment order* – This is a statement by the payer or payee to the supplier containing the command to execute the payment transaction.[33] It initiates a payment transaction. The payment instrument may be used for its assembly. The order must have data enabling the transaction to be carried

bezgotowkowego_112016.pdf [access: 10 X 2017].

[31] Art. 150 and N. UUP.

[32] M. Pacak, *Payment Services. Comment*, Warszawa 2014, LexisNexis p. 181.

[33] Ibidem, p. 182.

out, such as: payer and payee data, transaction amount, unique customer ID – e.g. IBAN-International Bank account number Account Number[34],

– *Payment transaction* – This is initiated by the payer or recipient of the deposit, transfer or withdrawal of funds. A payment transaction may be:
  • *Initiated by the payer* e.g. transfer order (traditional bank transfer), where the transaction order of the payer sends to his payment service provider[35],
  • *Initiated by the customer* – where the payer has previously given consent to initiate a transaction. In this case, the payee initiates a payment transaction without the payer's participation (e.g. direct debit[36]),
– *Payment Instrument* – this is the device or user-agreed and provider-set of procedures used by the user to place payment orders. These are the title of the example:
  • Technical procedures, such as electronic banking[37],
  • Material objects such as Payment cards – the so-called trading instruments[38],
– *Payment Card*[39] – This is a cash withdrawal card (ATM) or for making a payment order via merchant or a billing agent,
– *Debit Card* – A payment card enabling the execution of payment transactions, except for transactions in the weight of cash made available to the user for credit,
– *Credit card* – This is a payment card allowing the execution of payment transactions into the weight of the funds provided to the user for credit.

In the light of the UUP in the Polish legal order there are among others the following payment services:

- Payment Account maintenance (it should be noted that the payment account holder is not only banks), making cash withdrawals,
- Accepting cash deposits,
- Execution of payment transactions by means of a payment card or similar payment instrument,
- Execution of direct debit,
- Transfer command (traditional bank transfer),
- Issuance of payment instruments (e.g. payment cards), so-called Issuing,
- *Acquiring* execution of payment transactions initiated by the merchant or through the payer's payment instrument, in particular their authorization, sending to

[34] M. Grabowski, *Payment Services Act. Comment*, Warszawa 2012, C.H. Beck, p. 28.
[35] Ibidem, p. 27.
[36] Art. 63d Law of 29 August 1997 (OJ no 140, item 939).
[37] M. Grabowski, *Payment Services Act. Comment*, Warszawa 2012, C.H. Beck, p. 19.
[38] K. Korus, *Concept of payment service in the payment Services ACT*, Monitor of Banking Law, July-August 2012, p. 37.
[39] It should be noted that the subjects of payment cards are regulated particular by Regulation (EU) 2015/751 of the European Parliament and of the Council of 29 April 2015 on levies on interchange with respect to card-based payment transactions.

the issuer of the payment card or payment systems for payment orders having to transfer to acceptor the funds owed to it.[40] Except for the settlement operations of the payment system within the meaning of *The Law on settlement finality in payment and securities settlement systems and the rules for the supervision of these systems*.[41] These are transactions in which, for example, a payment by credit card is made in the store (merchant), which authorizes and settles the transaction on the services acquiring provided by the paying agents, transmitting a payment order to the bank – the publisher of the card belonging to the person making the payment and then, after receiving from that bank the cash, settling with the acceptor,

- The provision of money remittance (transfer to the payee of the cash received from the payer without the payment account being carried out – e.g. the receipt of fees for small bills in the purpose of their transmission to service providers or the receipt of payments for their make),
- provision of a payment transaction initiation service,
- provision of account information Access Service.[42]

Areas of payment infrastructure exposed to risk

The following places must be distinguished.[43] In the area of electronic payment infrastructures exposed to threats. These are:

– Payment Systems[44], entities accounting for payment transactions (e.g. National Clearing House) and payment card systems infrastructure – payment schemes (card organizations)[45],
– IT banking systems[46] (and) the infrastructure of entities involved in the processing of payment transactions (suppliers, including clearing agents),
– Merchants infrastructure, i.e. recipients of an electronic payment[47],

[40] R. Kashubian, Ł. Obzejta, *Payment cards in Poland*, Warszawa 2012, Wolters Kluwer, p. 107.

[41] *The Act on settlement finality in payment and securities settlement systems and the rules for the supervision of these systems of 24 August 2001* (OJ no 123, item 1351, Subsequent D.).

[42] *Provision of services and initiation of payments and service access to account information has been added to UUP based on PSD II Act of 10 May 2018 amended the law on payment services and certain other acts (OJ 2018, item 1075).*

[43] D. Gradzi, *Electronic payment security as part of Cybersecurity States – Review of legal regulations*, Internal Security Review No. 16 (9) 2017, p. 38.

[44] SORBNET2, TARGET2-NBP, for large payment, ELIXIR, EXPRESS Elixir, National settlement system, payment system BlueCash, the BLIK mobile payment system, the card payment system for retail payments, http://www.nbp.pl/home.aspx?f=/systemplatniczy/nadzor_syst_platn/systEmy_platnosci. HTML [access: 15 X 2017].

[45] Article 2 (1) 19b *Payment Services Act of 19 August 2011* (OJ no 199, item 1175, Subsequent. D.), define a card organization as: an entity that defines the issuant and acceptance rules of a payment card, which includes contracts with publishers (banks) or billing agents (e.g. VISA or Mastercard).

[46] K. Radziejewski, *Cybersecurity Governmental administration in Republic of Poland*, Internal Security Review, No. 16 (9) 2017, p. 313.

[47] Article 2 (1) 1b *UUP* define merchant as a customer other than the consumer to whom the payment agent provides the paying service (including, for example, an online store that accepts

– Applications and infrastructure for end users, both online and mobile, including mobile devices and computers.

Part of the above elements is a critical infrastructure[48], which is covered by the National Programme for the Protection of Critical Infrastructure.[49] These elements should be classified as financial systems, the operation of which is possible on the basis of communication systems and ICT systems.

"Critical State Infrastructure" includes, inter alia, banking and financial systems and telecommunication.[50] It consists of real (objects, servers) and cyber systems which, in case of coexistence, allow the provision of payment services. Due to the specificity of the payment services (remote access) and the open nature of the banking systems that can be accessed using public networks, they are exposed to cybercrime. Cybercrime is understood as a *"The use of telecommunications networks to violate any legal good protected by criminal law"*.[51] Government Programme for the Protection of Cyberspace Republic of Poland for the period 2011–2016[52] defines "cybercrime" as "criminal offences committed in "cyberspace". „Cyberspace" is defined in the above document as "a digital space for the processing and exchange of information created by ICT systems and networks, together with their associated relationships and user relations". Statistics of incidents in cyberspace coordinated by CERT[53] show an increase in the number of incidents compared to previous years. In 2014, more than 12,000 entries were registered, of which 7.4 thousand qualified as actual incidents. In 2015, more than 16,000 entries were registered, and as actual incidents qualified 8.9 thousand cases.[54]

In addition, it should be given that the occurrence of a threat in the above areas of critical infrastructure may be classified as a terrorist event[55] imply introduction

---

both card payments and the so-called payment services. Pay-By-Links – Instant transfers, where the amount of the payment transaction is dealt with By an intermediate settlement agent).

[48] Within the meaning of art. 3 point 2 Point. b), c) and D) *The Crisis Management Act of 26 April 2007* (OJ no 89, item 590, Subsequent. D.).

[49] Within the meaning of art. 5b *The Crisis Management Act of 26 April 2007* (OJ no 89, item 590, Subsequent. D.).

[50] Cf. Art. 3 paragraph 2 *Act of 26 April 2007 on crisis management* (OJ no 89, item 590, Subsequent. D.) and R. Kośla, *Protection of critical infrastructure in Poland – Current state of work*, HTTP://WWW.CERT.PL/pdf/Kosla_p. PDF [access: 2 X 2017].

[51] M. Staszczyk, *Unauthorized banking transactions as a manifestation of cybercrime*, electronic version, http://www.finanseiprawofinansowe.uni.lodz.pl/Publikacje/5/4_Staszczyk.pdf, p. 46 [access: 2 X 2017].

[52] *The Government Programme for the Protection of cyberspace RP*, https://bip.mswia.gov.pl/bip/programy/19057,Rzadowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html [access: 17 VIII 2018].

[53] Government Incident Response Team, http://www.cert.gov.pl/cer/o-nas/15,O-nas.html [access: 10 X 2017).

[54] http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/910,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2015-roku.html [access: 3 X 2017].

[55] In the meaning of article 2, point 7 *Act of 10 June 2016 on anti-terrorist activities* (OJ 2016, item 904).

of CRP alarm steps[56] where there is a suspicion that the offence is caused by a terrorist offence or the threat of such a crime.[57] A terrorist offence is, inter alia, an offence which is punishable by a custodial sentence whose upper game is at least 5 years, committed in order to cause serious disturbance to the regime or economy of Republic of Poland the threat of committing such a prohibited act, which in particular concerns critical infrastructure. It is possible to use the banking critical infrastructure by TPP and cause damage to the banks, as well as their clients, whose height can not be predicted.

Third Party Providers (TPP) – legal regulations

The legal acts governing access by third parties (TPPs) for payment accounts are[58]:

- PSD II directive,
- Regulatory Technical Standard (RTS)[59] – Concerning the strong authentication of the client and universal and secure communication, regulating the way of communication between TPP, and ASPSP[60], issued pursuant to art. 98 paragraph. 4 ph. 2 PSD II in connection with article 3. 10-14 of Regulation (EU) No 1093/2010 of 24 November 2010 establishing a European supervisory authority (European Banking Authority). RTS does not require implementation in national legal order[61] and EU member states are to ensure that it is forcibly applied by TPP and ASPSP from the first day after 18 months from the date of entry into force of the RTS,
- UUP and the Act amending the Payment Services Act and certain other acts.[62]

[56] According to Article 15 (1) 2 *Act of 10 June 2016 on anti-terrorist activities* (OJ 2016, item 904).

[57] For the purposes of Article 115 Par. 20 of the Penal Code of 6 June 1997 (OJ no 88, item 553).

[58] Included in the elaboration of both legal acts enacted and the legislative phase.

[59] RTS are issued based on Art. 290 of the Treaty on Functioning of the EU (OJ C 202 (2016), and are called. Level in the system of EU legislation. They shall be drawn up by the European Banking Authority (EBA) – The European Banking Authority and as a project are submitted to the European Commission. The European Commission has the power to adopt the so-called Act Non-Legislative which complements the legislative act (in this example, the PSD II directive). The RTS is therefore binding on Member States or supervised institutions (e.g. banks). RTS the European Commission submits to the Council of the European Union and the European Parliament, which may reject the act, cf. *The structure and status of European Union legislation with a particular focus on RTS, ITS and the so-called. Guidelines*, http://mifid.pl/wp-content/uploads/2015/11/Struktura-aktów-Unii-Europejskiej-ze-szczególnym-uwzględnieniem-RTS-ITS-i-tzw.-Guidelines.pdf, p. 4 [access: 4 X 2017].

[60] https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/regulatory-technical-standards-on-strong-customer-authentication-and-secure-communication-under-psd2 [access: 14 X 2017].

[61] K. Korus, access-based services to the account in the PSD II directive, Monitor Banking Law, July-August 2017, p. 82.

[62] Cf. Act Amending the Payment Services Act and certain other provisions of 10 May 2017., http://prawo.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20180001075 [access: 19 VI 2018].

The common scope of the PSD II directive to TPP

TPP are currently operating in the payment service market and are active participants carrying a huge volume of payment transactions both in terms of amount and quantity[63] (in 2014 of the services of one only provider of TPP used 8 million people in 11 countries, which supplier since 2005 has conducted over 100 million transactions). For this reason, PSD II introduced the requirement not to discriminate against these entities until the implementation of its provisions.[64] It is worth noting that the Financial Supervision Commission has in the past issued warnings before the activities of TPP.[65]

The PSD II introduces three types of services for TPP, also referred to as services XS2A.[66] They are:

- Payment Initiation Service (Payment Initiation Service-PIS): It means a service which consists in initiating a payment order from a user at the request of a payment account held with another payment service provider.[67] The PIS may not at any time be in possession of cash, which distinguishes this form of payment from the so-called Instant Transfers (Pay-by-Link), where the "broker" – the clearing agent shall be in possession of these resources,
- Account Information Access Service (Account Information Service – AIS): means an online service that consists of providing consolidated information about a payment account held by a payment service user[68],
- Confirmation of the availability of funds on the payment account (Confirmation of the Availability Of Funds -CAF). The CAF does not constitute a separate payment service and is not listed in annex 1 of the PSD II directive.

ASPSP is obliged to allow PIS and AIS to rely on user authentication procedures provided by ASPSP.[69] This regulation leads to the conclusion that TPP has the right to use its own authentication of the user, independent of ASPSP authentication, but may also rely solely on the authentication of the user used by ASPSP.

---

[63] https://www.sofort.com/pol-PL/newsroom/prasowe/SOFORT-Banking-utrzmuje-szybie-teo-wzrotu[access23X2017].https://retailnet.pl/2015/06/22/13453-dagmara-kruszewska-sofort-3-ml-tra-mieieczie/, http://prnews.pl/wiadomosci/sofort-wyniki-za-1-polowe-2016-50-sklepow-dzieie-chce-rozac-wspolrae-6553123.html [access: 14 X 2017].

[64] Recitals 29 and 33 to the PSD II directive.

[65] *A warning of the KNF by admission of intermediaries to a bank account in Internet payments of 18.11.2013, the risk of giving another bank login data for the 14.07.2014*, Cit. For: "*Recommendations concerning the security of payment transactions performed in the Internet by banks, national payment institutions, national e-money institutions and credit unions* Issued by the KNF in November 2015, p. 2, https://www.knf.gov.pl/dla_rynku/regulacje_i_praktyka/rekomendacje_i_wytyczne/Rekomendacja_dot_bezpieczenstwa_transakcji_platniczych [access: 25 X 2017].

[66] So-called. Access This Account (Account Access), Cf. M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 32.

[67] Art. 4 paragraph 15 of PSD II.

[68] Art. 4 point 16 PSD II.

[69] Art. 97 paragraph. 5 PSD II.

All the legal obligations imposed by PSD II on ASPSP apply only if they lead a payment account for the user. The bank account is then a payment account when it is used for the execution of payment transactions.[70] Access to information and functionality other than a payment account (e.g. credits, deposits, deposits, investments) is not regulated by the PSD II directive.[71]

The scope of the applicability directive PSD II applies only to payment services provided within the European Union (EU). A shortcoming of this applicability directive is that where the service provider is not in connection with the territory of the EU the service TPP can be provided without any restrictions with the PSD II Directive, but also without the possibility of seeking by TPP from ASPSP particular behavior to which the entity is obliged by PSD II.[72]

The obligations imposed on ASPSP relating to access to payment accounts by TPP Concern only the case where these accounts are carried out by ASPSP online. The PSD II directive does not define what is meant by the availability of an online payment account. It is aptly assumed that this term should be understood broadly and encompasses cases of any form of communication of information systems of the parties in real time.[73]

Guarantee the ability to provide services to TPP, which are competitive and stand in opposition to the interests of the so-called. Payment service providers is art. 36 of the PSD II directive, which provides that each payment institution should have access to services provided under payment accounts. These services should be provided by ASPSP based on objective, non-discriminatory and proportionate rules. Any refusal to provide such services to TPP should be duly substantiated and notified to the supervisory authority – the Financial Supervision Commission.

TPP are not obligated to establish any contractual relationship with ASPSP. The requirement to cooperate ASPSP with TPP derives directly from directive PSD II.[74]

TPP in the case of provision of payment initiation services does not enter into any stage of payment transaction in the possession of cash. Where the TPP intends to do so shall be obliged to request the Financial Supervision Commission and obtain full authorization for the provision of payment services.

---

[70] Cf. K. Korus, *The notion of payment service in the payment services Act,* Monitor of Banking Law, July-August 2012, p. 33.

[71] Rightly K. Korus indicates that accounts linked to credits may be payment accounts. K. Korus, access-based services to the directive account PSD II, Monitor Banking Law, July-August 2017, p. 86; *Recommendation Council of banking Law and the Regulating the payment of the Union of Polish Banks on selected problems of interpretation of the Payment Services Act,* http://zbp.pl/public/repozytorium/dla_bankow/prawo/rada_prawa_bankowego/dzialalnosc/rekomendacja_grupa_robocza.doc [access: 25 X 2017*];* M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 33.

[72] K. Korus, access-based services to the account in the PSD II directive, Monitor Banking Law, July-August 2017, p. 87.

[73] Ibid, pp. 87–88.

[74] Cf. Recital 30 to the preamble and Article 66 paragraph. 5 of the PSD II directive.

Payment Initiation Service (PIS) – general remarks

The PIS service is intended to expedite the performance of the contract by merchant (e.g. the shipment of goods through the online shop), because it gives him the guarantee of payment for goods or services-through PIS is initiated a specified electronic payment Merchant Payment Account as if you were doing it personally. Consent to the execution of a payment transaction granted by the payer through PIS is equivalent to the execution of a payment transaction expressed by the payer directly to the supplier.[75]

A model payment transaction scheme with the participation of PiS is such that the payment order of the payer (e.g. the person making the purchase in an online environment) is transferred to the ASPSP via the online banking provided to the user by ASPSP using the identification data agreed by the user of ASPSP, which is made available by the payer of PIS to initiate the payment transaction. The recipient of the cash is usually the seller of the goods, which is the contract with the PIS to handle such payments.[76] The PIS service allows you to make payments in an online environment without having to have a different payment instrument – e.g. Payment Card.[77]

Individual credentials used to secure user authentication (proof of identity by the provider), which the user or PIS use, are issued by the payment account provider (ASPSP).[78]

The PIS service was standardized in art. Article 4 (15) of the PSD II Directive and 66 of that directive. Essentially this service consists in placing the order by PIS on the command and on behalf of the user of a payment request to ASPSP to transfer funds to the account of the payee indicated by the user.[79] The main payment service which is the object of PIS is the transfer command.[80] The leading suppliers of these services are brands such as: Sofort[81] Whether Trustly.[82]

Payment Initiation Service (PIS) – regulatory issues

The Payment Initiation Payment service provider (PIS) may only be the payment service provider with such status according to the provisions of the Payment Services Act. In the case of a supplier having the status of a payment institution, it is necessary

[75] Article 64 paragraph. 2 of PSD Directive II.

[76] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 84.

[77] Recitals 28 and 29 to the preamble to the PSD Directive II.

[78] Recitals 30 to the preamble to the PSD Directive II.

[79] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 84.

[80] In the meaning of art. Article 3 (1) 4 UUP.

[81] https://www.sofort.com/pol-PL/kupujacy/sb/zakupy-online-z-sofort-banking/.

[82] https://trustly.com/pl/.

to extend the payment service authorization in respect of PIS and AIS.[83] Must have initial capital of 50 thousand euro.[84] The initial capital of such entities shall consist of one or more of the following elements:

- Equity instruments,
- Agio emissions related to capital instruments,
- Retained profits,
- Cumulated other total income,
- Reserve Capital.[85]

This is intended to constitute a guarantee element in case of adverse events related to the activity of TPP.

The payment service provider providing the PIS service should have a liability insurance or other comparable guarantee in order to be able to meet its obligations.[86] This regulation and the appropriate level of protection are of particular importance for the stability and security of the Bank (or other payment account holder), since in the event of an unauthorized payment transaction initiated by PIS, the ASPSP (e.g. the Bank) shall return without delay and in any event no later than the end of the following working day, the payer (customer) and the amount of the unauthorized transaction.[87] The subsequent order of the PIS, where he is responsible for the unauthorized transaction, shall compensate the ASPSP losses incurred or sums paid as a result of a refund to the payer, including the amount of the unauthorized payment transaction.[88]

Art. 66 PSD2 introduces the assumptions and regulatory framework of the PIS to the European legal order. The following are fundamental issues concerning the regulatory requirements imposed on the PIS and the ASPSP.

Duties of PIS:[89]

- The PSD II directive stipulates that the use of PIS is the right of the payer (the user) and ASPSP must respect this entitlement,
- PIS must obtain the payer's consent to initiate a payment order,
- The right to use the PIS is only available if the ASPSP leads to the user's online payment account,
- PIS does not at any time enter into possession of the payer's cash for the provision of the payment initiation service,

[83] Credit institutions within the meaning of Article 4 (1) 1, point 1 *Regulation (EU) No 575/2013 of the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms, amending Regulation (EU) No 648/2012* do not need dry authorization, in accordance with Article 11 (1) 1 of PSD Directive II.

[84] Article 7 point B PSD2

[85] Article 7 Directive II in ZW with Article 3. Article 26 (1) 1 point. A) to E) *Council Regulation (EU) no 575/2013 of 26 June 2013 on prudential requirements for credit institutions and investment firms, amending Regulation (EU) no. 648/2012.*

[86] Article 5 (1) 2 of PSD Directive II.

[87] Article 73 paragraph. 2 of PSD Directive II.

[88] Article 73 paragraph. 2 ph. 2 PSD Directive II.

[89] Article 66 paragraph. 1 and 3 of the PSD Directive II.

- PIS cannot change the amount of the payment order,
- PIS cannot change the payee of a payment order,
- PIS cannot alter any other features of the payment transaction,
- PIS must ensure that individual credentials of the user are not available to others (than the user and publisher of such data) of the parties,
- PIS must ensure that individual user credentials are transmitted through safe and efficient channels,
- PIS must ensure that all information about the payment service user is provided only to the payee and only to the expressly agreed payment service user,
- PIS is obliged each time a payment is initiated to identify itself to the payment service provider who holds the payer's payment account (ASPSP),
- The PIS is obliged to initiate payment, to communicate securely with the ASPSP, the payer and the consignee, in accordance with the provisions of article 5. 98 paragraph. 1 point. (d) PSD II directives[90],
- PIS may not store sensitive payment data,
- PIS may not require the payment service user of data other than the data necessary for the performance of the Payment initiation service,
- PIS may not use, obtain, or store any data for purposes other than for the provision of a payment initiation service expressly requested by the payer.

ASPSP obligations[91]:

- The ASPSP is obliged to communicate with the PIS in a secure manner, in accordance with the provisions of Article 98 paragraph. 1 point. (d) PSD II directives,
- ASPSP is obliged without delay after receiving a payment order from PiS to pass or make available all information about the initiation of the payment transaction and all information available to the ASPSP provider in relation to the execution of the transaction payment,
- The ASPSP must treat the payment orders transferred through the PIS, in a non-discriminatory manner, in relation to payment orders transferred directly ASPSP by the payer himself-in particular in terms of execution time, priority the nature of the levy, which, however, does not apply where

[90] EBA (European Banking Authority), in cooperation with the ECB (European Central Bank) and after consultation with all relevant stakeholders, including in the payment service market, develop draft regulatory technical standards RTS addressed to payment service providers specifying:

1. Requirements for strong client authentication,
2. Exclusions from the use of strong client authentication,
3. The requirements which security measures must fulfill to protect the confidentiality and integrity of the individual credentials of the payment service users,
4. Requirements for common and secure open standards of communication for the purpose of identifying, authentication, notification and information, as well as for the implementation of security measures, between ASPSP, the payer, the payee and the other payment service providers.

[91] Article 66 paragraph. 4 PSD Directive II.

discriminatory proceedings are justified by objective reasons,
– The performance of the PIS‘ services must not depend on the existence of a contractual relationship between the PiS and the ASPSP.

AIS – general remarks

The AIS service is regulated by Article 4 (16) and 67 of the PSD Directive II. This service consists of AIS access to the user's payment account (bank). Access to the account is based on the identifying data you have agreed with ASPSP. The user's data is provided by AIS. AIS logs in to the user's online banking system, and then collects and transmits aggregated data to the operator on-line communications. AIS thus obtains access to account data and for all payment transactions in that account.[92]

AIS – regulatory issues

Article 67 of the PSD Directive II introduces the AIS regulatory framework to the European legal order. The provision of AIS services does not require the authorization of the National Competent Authority (FSC), but only the registration.[93] The payment institution providing the AIS services should hold a liability insurance or other comparable guarantee in order to be able to meet its obligations.[94]
AIS responsibilities:
– The PSD II directive stipulates that the use of AIS is the payer's right (user) and ASPSP must respect this entitlement,
– AIS must obtain the user's consent to provide its services to him,
– The right to use the AIS services is granted to you only if the ASPSP leads you to a payment account available online,
– AIS must ensure that individual user credentials are not available to other parties, except for the user and the publisher of the user's personal authentication data,
– AIS must ensure that individual user credentials are transmitted by the AIS service provider through safe and efficient channels,
– AIS must identify themselves to ASPSP for each communication session,
– AIS must communicate with the ASPSP and the user in a safe manner and in accordance with the provisions of art. 98 paragraph. 1 point. (d) PSD II directives,
– AIS may only access information relating to payment accounts and related payment transactions,
– AIS may not request sensitive payment data relating to payment accounts,
– AIS may not use, obtain, store any data for purposes other than for the performance of the account information service explicitly requ-

[92] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 85, Article 67 paragraph 2 (a) (d) PSD Directive II.
[93] Article 33 and 5 (2). 3 PSD Directive II.
[94] Article 5 (1) 3 PSD PSD Directive II.

ested by the payment service user in accordance with the data protection regulations.

ASPSP obligations:

- ASPSP must communicate with AIS in a safe manner and in accordance with the provisions of Article 98 paragraph. 1 point. (d) PSD II directives,
- ASPSP must treat requests for data provided through AIS in a non-discriminatory manner, unless discriminatory treatment is justified by objective reasons,
- The supply of AIS services must not depend on the existence of a contractual relationship between AIS and ASPSP,
- As stated in the preamble of the PSD II directive, ASPSP provides all the information concerning the payment account, in particular the IBAN or NRB number, the amount of the balance, the transaction history (amount, title, date of execution, data of the other party[95]).

The leading suppliers of these services are: Kontomierz[96], AFAS[97], Tink[98], Money Dashboard[99], Quontis.[100]

CAF (Confirmation of the Availability of Funds) – General Comments

The PSD II directive introduces in addition to the aforementioned services TPP, also the process of confirming the availability of funds on the payer's payment account. However, this process is not a regulatory separate payment service.

This process enables the publisher of a payment instrument based on a credit card[101], previously designated ASPSP by the user (whose payment account provides the ASPSP) demand from ASPSP in real time, using online communication, information or on the user's account there is a certain amount. This process is therefore governed by the obligations of the ASPSP to the issuer of a payment instrument based on a credit card. It is your responsibility to inform ASPSP about your intention to use the CAF.[102]

---

[95] M. Mostowik, *Legal Protection of payment account information in the light of account information Services (AIS)*, Monitor of Banking Law, July – August 2017, p. 34.

[96] http://kontomierz.pl.

[97] https://www.afas.nl.

[98] https://www.tinkapp.com/en/.

[99] https://www.moneydashboard.com.

[100] http://www.qontis.ch.

[101] Instrument-based on payment card is a any payment instrument (among others card, mobile phone, computer) enabling initiation payment transaction they using the payment card system infrastructure – cf. Article 2, point 20 of the regulation of the European Parliament Council Regulation (EU) 2015/751 of 29 April 2015 on the fees interchange with respect to card-based payment transactions.

[102] K. Korus, *Access-based services in the PSD II directive*, Monitor Banking Law, July-August 2017, p. 85.

CAF – regulatory issues

It is ASPSP to confirm at the request of the supplier issuing payment instruments based on the card – availability on the payer's payment account the amount necessary for the execution of a card-based payment transaction.[103] (CAF service – Confirmation of the Availability Of Funds).

Legal requirements to applicability a CAF service:[104]

- the payment account of the payer must be accessible via the Internet at the time of the request for confirmation of availability of funds
- the payer has given ASPSP permission to respond to requests from a particular payment service provider to confirm that the amount corresponding to the specific payment transaction on the basis of the card is available on the payer's payment account,
- the consent for the ASPSP from the user to the story of the request must be given before the first request for confirmation.

Legal requirements imposed on the applicant supplier:

- the payer has granted this entity explicit permission to request the availability of cash,
- the payer has initiated a payment transaction executed using a card-based payment instrument,
- the CAF supplier must authenticate himself to the ASPSP provider,
- The CAF supplier must communicate with the ASPSP in a safe manner in accordance with the provisions of art. 98 paragraph. 1 point. (d) PSD II directives.

The confirmation of the availability of funds on a payment account by ASPSP is to answer "yes or no". Balance status is not fed. The CAF supplier may not store or use a response obtained from ASPSP for any purpose other than the execution of a card-based payment transaction.[105] Confirmation of availability of funds does not permit ASPSP to block a certain amount in the payer's account until the payment is settled.[106] For the implementation of the CAF service it is necessary to permit the issuance of card-based payment instruments.

Activities of TPP and cybersecurity

The prevention and countering of cybercrime in the area of payment infrastructure should be addressed, in addition to the eligible public entities, by industry financial organizations[107] (in cooperation with the relevant public services), as directly exposed

[103] Article 65 paragraph. PSD directive II.
[104] Ibidem.
[105] Article 65 paragraph. 3 PSD directive II.
[106] Article 65 paragraph. 4 PSD directive II.
[107] Cf. A. Marciniak, Bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński,

to threats and interested in the cybersecurity. An example of such an organization is FinansCERT from Norway.[108] This organization is CERT[109] in the Norwegian financial sector: banking and insurance. Its main tasks are:

- Tracing external threats,
- Support to combat attack and reduce losses,
- Coordination of cooperation with public institutions and order services (Interpol, police).

Other industry organizations whose activity is information security threats are among others established in the United States, but the global reach of non-governmental organizations: National Cyber-Forensics & Training Alliance (NCFTA), Financial Services Information Sharing and Analysis Center (FS-ISAC), SoltraWhether working in the European Union European Financial Institutes – Information Sharing and Analysis Centre (FI-ISAC).[110]

Bank Centre Cybersecurity

In September 2015, a recommendation on security and prevention of online banking inaccessibility was issued at the initiative of the Electronic Banking Council (PSV). The recommendation recommends that affiliated banks PSV established cooperation on:

- counteracting attacks on banks‘ e-banking platforms and their customers,
- responding to attacks.

The result of this recommendation was the establishment of the banking centre Cybersecurity BCC.[111] BCC is now one of the key platforms of the National Center Cybersecurity (NC Cyber).[112] BCC cooperates with the police and the National Clearing House S.A.,

A. Sieradz (ed.), *Challenges of Banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 187, [access: 2 X 2017].

[108] FinansCERT as an organization was established on 23 April 2013 in the Norwegian Industry organization umbrella Financial Institutions, http://www.finanscert.no [access: 15 X 2017].

[109] Computer Emergency Response Team – *Computer Incident Response Team.*

[110] A. Marciniak, Bank CERT– New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of Banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 187, [access: 25 X 2017]

[111] See the BCC open information on the PSV website. https://zbp.pl/wydarzenia/archiwum/wydarzenia/2016/lipiec/otwarcie-bankowego-centrum-cyberbezpieczenstwa [access: 25 X 2017]; Until Streżyńska, reply to interpellation, BM-WOP. 072.69.2017, Warsaw 22.06.2017, http://www.sejm.gov.pl/Sejm8.nsf/InterpelacjaTresc.xsp?key=75AD31FB, [access 25 X 2017], A. Marciniak, Bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of Banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 191, [access: 25 X 2017]. 191 [access: 3 X 2017].

[112] NCC was established on 4 July 2016 and operated in the NASK structure (scientific and academic computer network), which is a state research institute within the meaning *Act of 30 April 2010 on research Institutes*. According to paragraph 3 (a) of 2 (1 Point D *of the Council of Ministers of 7 June 2017 on the giving of the scientific and academic network of the statutes of Status of State Research Institute* (Journal of laws 2017, item 1193). DNASK tasks should be to ensure cybersecurity public entities through the development of the National Cybersecurity.

telecommunications operators, quick payment operators, exchanges bitcoin.[113] In the event of a risk to cybersecurity BCC becomes the crisis staff, which manages the crisis situation in the banking sector. Currently, the focus of BCC is in particular:

- Monitoring of the banking sector in terms of Cybersecurity and to respond to hazards,
- Communication management in particular by:
  a) Developing a coherent information policy for customers and media in the banking sector, the main objective of which is to inform immediately of any risks Cybersecurity or failure of electronic banking systems,
  b) Develop communication procedures between participants,
  c) The elaboration of cooperation and communication channels with law enforcement agencies, other CERT, software producers and security systems,
- Defining and monitoring the implementation of preventive measures in the sector.[114]

We can easily imagine situations in which TPP in the initial phase of the activity, building its reputation in the market and user confidence, after a while having already had the data to log into the accounts of the clients ' bank, leads to mass to a number of unauthorized transactions. These transactions against clients allegedly using the PIS service are, in the first instance, legally and financially responsible for the bank. The Bank has a claim to TPP for reimbursement of amounts that are the subject of unauthorized transactions, which can however be satisfied only if the TPP is solvent. Another example is possible when AIS has a database of sensitive credentials to log in to bank accounts and intentionally leads to loss of such a database. Costs, not only financial (due to very large volume and volume of payment transactions), but social (caused by loss of customer confidence in the payment ecosystem) can be difficult to quantify. Even if the caused damage is covered in full, the significant resulting cost will be the loss of confidence in the financial sector by customers.

Taking the above into account, the activities of TPP can also cause significant legal problems on the plane:

- Banking secrecy[115],
- Payment secrecy[116],
- Rights to the protection of personal data,
- Rights of privacy, such as the holder of the account and third parties whose personal data appear in the electronic banking application, as paying or recipients.[117]

---

[113] A. Marciniak, Bank CERT – New weapons in the fight against cybercrime [in:] A. Kawiński, A. Sieradz (ed.), *Challenges of banking Informatics 2016*, Gdansk 2016, http://www.efcongress.com/sites/default/files/wyzwania_informatyki_bankowej_0.pdf, p. 193, [access: 25 X 2017].

[114] Ibid., p. 193.

[115] See. Article 104 paragrapf 1 *Act of 29 August 1997 Banking Law* (OJ no 140, item 939, Subsequent. D.).

[116] See. Article 11 (3) 1 UUP.

[117] To the extent indicated risks Cf. M. Mostowik, *Legal Protection of payment account information*

Summary

The services of TPP are currently and will continue to be present in the electronic payments segment, and their even greater growth will occur when they are permanently aggregated with providers of social networks and mass services such as: Facebook, Apple, Amazon, NetflixGoogle[118], Uber Spotify.

Both the payment initiation service providers (PIS) and the payment account service provider (AIS) on one side and the traditional payment service providers on the other should respect the data protection requirements and PSD II and the RTS directive. The RTS should ensure the interoperability of[119] different communication solutions from a technological point of view. The RTS should also allow the payment account provider (ASPSP) to know that the payment transaction is in contact with the PIS and not the client directly.[120]

It should be noted that the provisions of the PSD II directive on the activities of TPP are very general. All the important technical issues to ensure the security of these services and the entities using them and providing them have been settled by the RTS. In view of the fact that the services of TPP are provided inter alia in an Internet environment, malfunctions in their operation may pose a threat to cybersecurity of the paying critical infrastructure. The Association of Polish Banks constantly monitors the factual and legal situation, noting the risks associated with the activity of TPP.[121]

The legal architecture contained in the PSD II directive in the field of TPP, is an example of effective regulatory lobbying of entities providing these services for years. Players who are TPP, due to potential risks at the micro-scale (loss of funds by the user) and macro (threat to the payment operation of critical infrastructure) should meet with the prudential approach of the regulator – Supervisory Committee and users in the early stages of operation.

Abstract

Online and mobile payments due to their non-cash character and speed are characterized by very high development potential. As their volume and quota increase, the risks associated with their processing are increasing, as they do not involve the physical participation of the parties and the Internet environment. New payment methods

in the light of account information Services (AIS), Monitor of Banking Law, July – August 2017, pp. 35–42.

[118] Specified in short FAANG (Facebook, Apple, Amazon, NetflixGoogle).

[119] A feature of the product or system whose interfaces enable it to work with other products or systems.

[120] Recital 93 to the preamble to Directive PSD II.

[121] Based on note Restrictions Services based on third party access (PISP, AISP) to payment accounts in the light of the PSD2 of the Banking Council of the Polish Bank Association, https://zbp.pl/public/repozytorium/wydarzenia/images/luty_2017/Polish_Bank_Association_Notatka_PL_Third_Party_Services_PSD2_January_2017_fin.pdf [access: 10 X 2017].

have led to the emergence of new suppliers – the so-called Third Party Payment Service providers-payment service providers which are third parties whose activities may involve specific threats. At the micro scale, you can indicate the security risks of your financial resources. On a macro scale, you should indicate the potential risks to the so-called of paying critical infrastructure and more broadly - cybersecurity.

Keywords: PSD, cybercrime, Third Party Providers, critical infrastructure, Financial Supervision Commission, electronic payment transactions, mobile payments, online payments, Account Servicing Payment Service Provider, Account Information Service, Payment Initiation Service.

Konrad Hennig

National ownership of power generation technology as an element of the energy security of Poland

Energy security of every single state is contingent on shaping the energy balance ensuring the utmost resilience against the following factors: 1. external attacks (achieved by the dispersion of generator installations); 2. system crush (by mastering technologies); 3. disruptions in energy sources supply (by achieving self-sufficiency or diversification of sources and transporting channels). In the politicians' perception the notion of energy security boils down merely to energy independence to be achieved via the maximising the energy sources derived from their own territory. The reliance of the domestic energy balance on available original energy sources in a given country is definitely the first step towards a responsible energy policy. No less important, however, though often overlooked, is the exploitation of one's own technologies of sources acquisition and power production. Given the continually growing challenge of rapid technological advancement constituting the object of competition between super-powers (with cyber security and economic security taking the lead) the issue of energy security becomes an overriding element of a public debate. The energy security comprises four component parts i.e.: 1. independence in obtaining energy sources; 2. the stability of electricity networks and the transport of fuels; 3. diversification of sources of foreign energy resources supplies and of the sources of energy production within the state; 4. technological independence, i.e. the state ownership of energy production technologies, to be discussed further in the present article.

The level of energy independence, calculated as a share of energy produced from domestic sources in the total energy consumed for the five selected EU countries:

Table 1. Degree of energy independence.

2014 data in thousands of tonnes	Germany	Spain	France	UK	Poland
General consumption of energy	306 753	114 559	242 642	179 421	94 018
General acquisition of energy	120 713	35 101	137 128	108 236	67 326
Degree of energy independence	**0,393519**	**0,306401**	**0,565145**	**0,603252**	**0,716097**

Source: „Energy Balances of OECD Countries", IEA.

As the above data show, Poland has a relatively high degree of energy independence, due to a proportionate exploitation of hard coal and brown coal, covering ca. 30% of the domestic need, to the needs of our economy, as well as extraction of natural gas.

"*The most important energy carrier is hard coal (60,6% in 2015). The second carrier in terms of volume of extraction was brown coal with the share of 17,9%. The share of natural gas in the whole extraction was 5,4%, crude oil 1,4% and the rest, mostly renewable energy carriers 14,7%".* In turn *"the most important consumed carrier was hard coal with its share of 39,5%. The share of crude oil was 25,1% and natural gas 14,0%. Brown coal was 11,6% of the consumed energy and other carriers were 9,8%.*[1]" Can we therefore acknowledge with satisfaction that as a country we enjoy a basic level of energy security?

In terms of statistics the above question could get a positive answer. However, we have to bear in mind that security cannot be perceived as a state but a set of diachronic processes. Variability of phenomena in time, particularly in view of their complexity and mutual correlation makes us see challenges and threats as a highly dynamic phenomenon. Minor processes unfolding today on a small scale may grow geometrically in a short term perspective, threatening the stability of electricity system or fuel system. In view of this, we need to be very cautious in deriving optimism from the extrapolation of past experiences concerning electric system based on coal-burning.

The government policy in recent years has put much emphasis on a diversification of liquid fuel supplies (gas in particular), while at the same time the Polish power generation system fails significantly in terms of flexibility in 5 basic categories: 1. administering of deliveries; 2. demand shaping; 3. storing; 4. obsolete networks, and 5. the structure of the wholesale, balancing and retail market.[2] It is therefore exposed to the loss of dynamic stability (the risk of lowering voltage: *brown-out*, the risk of cutting voltage: *block–out*) as a result of energy imbalance between energy produced at a certain time and the volume of energy transformed in appliances and energy lost during the transmission. To provide the system with more flexibility, we need more international connections, power depots, and the domestic available reserve power. The coal facilities providing a base in producing power are partially flexible but their phasing out entails the high risk of damages and accidents, and the work on full capacity is dependent on cooling water availability. The gas installations available only in heating segments, municipal and industrial cogeneration show the highest flexibility. The wind and PV installations are dependent only on weather conditions and cannot be disposed as per the requirements of the National Electrical System (Krajowy System Elektroenergetyczny). The increase of their share in the electric mix leads to a further exacerbation of a poor flexibility of the system. Only a few of pomp-storages in Poland feature higher flexibility (response in 2–3 minutes) and are capable of storing power. Given that, the suspension in late 1980s of the construction of Elektrownia Wodna Młoty (750 MW), followed by its sale to Électricité de France may

[1] *Gospodarka paliwowo-energetyczna w latach 2014 i 2015*, Główny Urząd Statystyczny, Warszawa 2016, http://stat.gov.pl/download/gfx/portalinformacyjny/pl/defaultaktualnosci/5485/4/11/1/gospodarka_paliwowo_energetyczna_2014_2015.pdf [access: 12 VI 2017].

[2] I. Kielichowska, E. Haesen, T. Sach, *Flexibility Tracker Country Report Poland*, http://www.leonardo-energy.org/resources/503/flexibility-tracker-country-report-poland-5814f41cb7050 [access: 12 VII 2017].

be somewhat surprising. The unfinished power plant was returned to Polish Polska Grupa Energetyczna S.A. thus the feasibility study concerning the costs of its completion may be expected soon. The only alternative location enabling the construction of a comparable scale power plant of comparable scale is the external soil bank by the Bełchatów Brown-Coal Mine. At present there are 6 pump-storage plants in Poland: Żarnowiec, Porąbka-Żar, Żydowo, Solina, Dychów, Niedzica. They all are capable of storing 10 GWh and their installed power equals 1 700 MW.

Consequently, just like few decades ago, the flexibility of the Polish power system is based on power supply levels, that is, on the flexibility potential of power customers rather than producers. The introduction of a chargeable limits on the consumption of power by selected customers DSR (Demand Side Response) helps to overcome political costs resulting from the introduction of the power supply levels (mid-2018 ca. 500MW[3]), but does not change the overall reasoning. Additionally, "*transmission networks are old and overburdened: more than 80% of 220kV networks, 56% of 400kV networks and 34% of sub-stations are over 30 years old; also in case of distribution networks their average age is more than 30 years.*"[4] The market of energy purchases by wholesale customers is based on forward contracts and a day-ahead market. We are only in the eve of shortening time slots to make prices more flexible and to steer the needs of industrial customer for power.

Ensuring energy security by making electric networks more flexible requires the implementation of the whole range of technological solutions, few billion zlotys' worth investments and the update of legal regulations. The awareness of the above needs is being raised by tech companies, which attempt to attract decision makers to their products and computer solutions. As a result of close ties and cooperation between energy sector and industry and the necessity to address the requirements of economy, one can hope that the negligence of the past three decades can be overcome at a faster pace than in the case of technical modernisation of the Polish Military Forces.

The energy independence and stability of power networks, however, is only a part of the problem. The diversification of domestic electrical power sources is of no less importance. The structure of our energy balance is the aftermath of decisions taken by the communist Soviet decision makers. In 1990 the power production was based in 98% on burning coal in public plants and thermal power stations, and in 2% on hydropower plants. Hard coal was then a source of almost 70% of conventional energy and brown coal of almost 30%. Even though our own resources were solely exploited at that time, that was not an optimal solution from the perspective of system security. As in any monoculture it exposed our entire electricity system to the risk of fluctuations in the coal sector (e.g. the increase in material prices or introduction of the EU anti-coal policy). To date we have been limiting the share of coal to 86% in the market, although some part of the remaining 14% makes up for a co-incineration of biomass in coal

[3] https://www.pse.pl/uslugi-dsr-informacje-ogolne [access: 8 VI 2018].

[4] *Elastyczność w energetyce – wyzwania stojące przed Polską*, http://nowa-energia.com.pl/2017/03/30/elastycznosc-w-energetyce-wyzwania-stojace-przed-polska/ [access: 20 VII 2017].

installations. Still, we cannot boast a proportionally diversified energy balance, in which a share of various 4-5 sources makes up 15-30%, which seems to be an optimal solution.

The development of domestic energy balances in the world was a result of the long-time processes influenced by a range of endo- and egzogenous factors. The percentage share of renewable energy, atomic energy, coal energy or gas energy differed among countries and were conditioned on the particular circumstances. The energy mix in a given country was predominantly determined by its topography, water supplies, raw materials supplies, geopolitical situation and the stage of technological development. Consequently, the primary energy balance as well as the structure of power generation and the exploitation of fuels in urban and domestic sector can significantly differ between very similar and neighbouring countries, since it may only be one factor that disturbs radically the contribution of each energy source.

It should be noticed that the structure of energy production for a particular country is relatively stable. The processes of a deliberate transition towards other energy sources take years (planning and construction cycle of a conventional power plant lasts from 5 to 12 years, its construction generates significant costs, and in case of the change in balance occurring in a medium-sized state more than one power plant is needed) and are motivated usually by a discovery of more effective energy sources on site, for example by launching an extraction of thus far undetected resources of raw materials or developing new technology (or otherwise the withdrawal due to natural or anthropogenic catastrophes). With most changes, the new sources instead of replacing the previous ones, triggered a growing demand of the economy for electric power. The examples of such deliberate changes are Japan[5] and Germany, which chose to gradually phase out nuclear power plants until 2022. It seems that Polish energy transition is not likely to be so radical and the introduction of a new power generating source will proceed in response to a growing demand. What kind of source will be chosen by the Polish government, remains to be seen. The question will reoccur later in the text.

From the economic point of view the energy balance is a function of availability and the cost of power production. In case of Poland the accessibility of various energy sources can be classified into three segments:

Table 2. Availability of energy sources in Poland.

High	Hard coal, brown coal, solid and liquid bio-fuels (plant and animal solid waste, solid and liquid industrial waste, urban waste, biogas from dumping sites and purification plants), geothermal energy.
Average	Natural gas (including shale gas), wind energy.
Small	Crude oil, water energy, nuclear energy, solar radiation.

Source: private study of the author.

[5] In Japan, several years after the catastrophe in Fukushima we can notice a gradual moving away from such radical decisions. J. Malko, *Energetyka japońska. Jak radykalna transformacja?*, Energetyka, no. 6/2013, http://www.cire.pl/pliki/2/energ_japonska.pdf [access: 18 VIII 2017].

The sources broken down by unit production technical costs:

Table 3. Individual technical costs of power production in Poland (PLN/MWh).

	2012	2013	2014	2015
Brown coal	139,7	134,6	134,9	130,4
Water energy	186,2	153	170,5	164,2
Hard coal	212,5	199,3	183,9	172,3
Wind energy	208	222,1	227,8	210,9
Natural gas	303,1	372,2	261	241,2
Biomass	446,1	405,6	361,6	367,9

Source: Z. Kasztelewicz.[6]

The above data show that in our case economic factors favour the use of brown coal, hard coal and water energy and affect the limited use of natural gas and biomass. The Polish energy mix lacks nuclear power, and the solar energy or geothermal energy occur in trace amounts, because their exploitation generates even higher costs. The economic criteria, however, are not decisive in a decision-making process. They should obviously be taken under consideration in the context of a slump in international competitiveness of energy-intensive sectors of the economy accompanied by a high price of the energy but the energy policy of the state should take into account other factors alongside the economic efficiency. From the perspective of the energy security both geographical and technological factors come into play i.e.: the availability of the energy sources and mastering of the power generating technologies by a domestic industry. We cannot speak about energy independence only on the grounds that we have energy sources (fossil or renewable) at our disposal. It is only possible after business undertakings and the S&R institutions acquire the know-how in the field of the entire process of development of the extraction and generating facilities and the production of the relevant machinery.

Domestic business enterprises (duly registered, taxpayers, carrying out production and R&D activity, state-owned or citizens-owned) in Poland are able to realise projects of minerals extraction from the existing conventional deposits: hard coal, brown coal, crude oil, natural gas and geothermal energy. We are a significant solar panels producer (heating of water storage tanks) and we are achieving remarkable progress in the development of wind energy technologies (also at sea), even though the key elements (wind turbine and generator) are still supplied by foreign contractors. Mastering of power generation technologies looks slightly bleak. Despite the fact that our installations benefit from the production capabilities based on hard coal, brown coal and water energy, major investments in the past few years have been frequently carried

[6] Z. Kasztelewicz, A. Tajdus, T. Słomka, *Węgiel brunatny to paliwo przyszłości – czy przeszłości?*, Węgiel brunatny gwarantem bezpieczeństwa energetycznego, Kraków 2016, p. 237.

out by foreign companies or consortia of domestic and foreign companies, where the key technologies were delivered by Siemens, Hitachi, Mitsubishi, or General Electric. The following table presents a set of the most important upgrading and investment in producing installations.

Table 4. Contractors of selected investment projects aimed at enhancing generation capability.

Year/s of investment	Investor	Location	Contractor
1	2	3	4
1995-2004	Żarnowiec S.A. Hydroelectric Power Station	Żarnowiec	Westinghouse WDPF 2 System Brüel&Kjœr Compass System MCM and IRIS HydroScan System Automative System of Technical Control over Dams by Budokop Sp. z o.o.
2013-2017	Orlen S.A.	Włocławek Industrial Cogeneration Plant	Steam and gas block by General Electric and SNC Lavalin
2012-2014	Jastrzębska Spółka Węglowa S.A.	Przyjaźń Coking Plant in Dąbrowa Górnicza	General contractor: Energoinstal. Siemens Wind Turbine Generator System
2011-2013	KGHM Polska Miedź S.A.	Głogów Cogeneration Plant, Polkowice Cogeneration Plant	Steam and gas block by Energoinstal
2004-2011	PGE S.A.	Bełchatów Power Plant	Consortium of General Electric, Alstom and Rafako; the construction of the supercritical brown coal fired unit
2014-2017	Spółka Energetyczna Jastrzębie SA	Zofiówka Cogeneration Plant	Cogenerational Fluid Block by the consortium of Energoinstal S.A. (80%) and Przedsiębiorstwo Budownictwa Ogólnego Skobud (20%).
2013-2017	PGE S.A.	Gorzów Wielkopolski Cogeneration Plant	Steam and gas block from Siemens Sp. z o.o. and Siemens Industrial Turbomachinery AB
2012-2017	Enea S.A.	Kozienice Power Plant	The construction of the supercritical coal fired unit by the consortium of Polimex-Mostostal and Hitachi Power Europe.

2015-2018	Fortum	Zabrze Cogeneration Plant	Alternative fuel, coal and biomass cogeneration block. Chief engineer of the contract ILF Consulting Engineers. Fluidal beds circulatory boilers by Amec Foster Wheeler. Turbine set, generator and heat exchangers system by Doosan Škoda Power. Xternal coal and alternative fiel feed system by BMH Technology. Steel construction from Mostostal Zabrze. Construction Works by Budimex S.A.
2014-2019	PGE S.A.	Turów Power Plant	Brown coal block from the consortium of Mitsubishi Hitachi Power Systems Europe (55,38%), Budimex (22,31%) and Tecnicas Reunidas (22,31%).
2014-2019	PGE S.A.	Opole Power Plant	Consortium of Rafako, Polimex-Mostostal and Mostostal Warszawa. Ultra supercritical block by General Electric. Two BP boilers by Rafako company. Generators and steam turbines of ultra critical parameters, boilers, power plant auxiliary systems and environment installations by Alstom company.
2014-2019	Tauron S.A.	Jaworzno Power Plant	Consortium of Rafako (99,99%) and Mostostal Warszawa (0,01%). Turbine by Siemens.
2014-2016	Zakłady Azotowe Kędzierzyn	Kędzierzyn-Koźle-Cogeneration Plant	Complete cogeneration installation from Rafako company

2012-2019	Tauron S.A. PGNiG Termika	Stalowa Wola Cogeneration Plant	Contract with general contractor Spanish Abener Energia company broken in 2016. Gas turbine by General Electric and gas turboset by Skoda Power. Construction in the EPCM formula (Engineering-Procurement-Construction-Management) finishes the consortium of Zakłady Pomiarowo-Badawcze, Energetyka Energopomiar and Energoprojekt-Katowice.
2017-2020	PGNiG Termika	Żerań Cogeneration Plant	Cogeneration gas and steam Block from the consortium of Mitsubishi Hitachi Power Systems Europe Gmbh, Mitsubishi Hitachi Power Systems Ltd, Mitsubishi Hitachi Power Systems Europe, Polimex-Mostostal.

Source: private study.[7]

The existence of domestic specialisations was explicitly indicated in *The Programme for the Hard Coal Mining Sector in Poland* of 2016 (...): *"Poland does have a developed mining sector, including mining machinery and equipment. Domestic companies producing mining machinery and equipment are private, often listed on the Warsaw Stock Exchange. The majority of the companies is based in the southern Poland. It should also be pointed out that Polish sector of mining machinery is very diverse. The machinery for mining mineral resources, sections of mechanized housing, conveyors (belt and scraper), machinery for transportation, security machinery, drilling equipment, electrical wires, transformers and pumps, working clothes are continuously produced. The Polish brand is a household name appreciated for its quality. At present the export goes mainly to Russia, China, Mongolia, Kazakhstan, Australia, Indonesia, India, Canada, USA, Argentina, Columbia, Ecuador and Congo. The national producers are recognized on all the continents, where mineral and energy resources are mined in opencast workings and other methods."*[8]

[7] Based on press materials of the companies and *Budowane i planowane elektrownie*, http://www.rynek-energii-elektrycznej.cire.pl/st,33,335,tr,145,0,0,0,0,0,budowane-i-planowane-elektrownie.html [access: 16 VIII 2017].

[8] *The Programme for the Hard Coal Mining Sector in Poland*, Ministry of Energy, Warszawa 2016, p. 80.

Polish industry specializes in a conventional resources mining. PGNiG S.A. company exploits national resources of gas and crude oil. JSW S.A., PGG sp. z o.o., Bogdanka S.A. is engaged in hard coal mining. PGE GiEK S.A., ZE PAK S.A. and KWB Sieniawa sp. z o.o. deal with the lignite mining. Polish companies are the largest manufacturers of machinery and equipment.

Famur S.A. Group (inter alia Kopex, Famak, Famago, Fugo, Pioma), Bumech S.A. and Fasing S.A. produce all kinds of mining machinery and conveyors. The RAMB company from PGE S.A. group has recently launched the execution of its first comprehensive orders for the benefit of KWB Turów. Research institutes and design offices e.g. Energoprojekt-Katowice S.A., SKW Biuro Projektowo-Techniczne sp. z o.o., Poltegor-Projekt sp. z o.o., Główny Instytut Górnictwa (the Main Institute of Mining), Poltegor-Instytut, Instytut Chemicznej Przeróbki Węgla (the Institute of Chemical Coal Modification) are very active on the market as well. The tycoons of the Polish market together with Polish sub-contractors have capacity for searching and exploring deposits as well as building shafts, mines designing and doing extractions. We have a comprehensive know-how and a production base for machinery and equipment to lead new extraction projects.

Things look slightly different in the case of generation installations caused by a technological underdevelopment of Polish companies in terms of efficiency and carbon footprint. Nevertheless, the construction companies Elektrobudowa S.A., Mostostal Warszawa S.A. and Polimex Mostostal S.A. perform the maintenance of construction contracts and deliver steel structures for power plants and thermal power stations constructed in Poland. The companies Rafako S.A. and Remak S.A. provide boilers and instrumentation for coal power plants and Energoprojekt-Warszawa S.A. and HydroErgia sp. z o.o. for the water power plants. Tens of small and medium-sized companies produce parts and equipment for mining and energy sector. Konsorcjum Przemysłowe INTEC-WAKMET, Grupa Revico, Ania Holding, CHEMAR sp. z o.o. or Fabryka Kotłów SEFAKO S.A. are additionally worth mentioning. There are no Polish producers of steam and gas turbogenerators. We employ the solutions of Siemens, General Electric, Doosan Škoda Power or Mitsubishi Hitachi Power Systems Europe. It seems unreal today that Zamech company from the city of Elbląg will restore its former state-owned structure. After its privatisation in 1990 the ownership of the company changed hands from ABB and Alstom to General Electric. However, the worst situation in the Polish industry can be observed in the renewable resources sector caused mostly by a shortage of companies producing modern and competitive gearless turbines. The situation in the area of solar energy is slightly better – major in the production and utilization of solar collectors (heating water storage tanks). FreeVolt company from the city of Bydgoszcz specialises in photovoltaic panels and it carries out further advanced research on the use of grapheme, which would increase the efficiency of the cells by several dozen percent. The development of the technologies could be stimulated by the industrial policy of the state to be realized by the four biggest state-owned

energy groups. As far as the distributed energy and micro-installations are concerned we are just at the start of a long road in spite of its advantages and scattered financing of thousands of small investors.

The availability of technological and production facilities, machinery and equipment for mineral exploration and generation of electricity offers additional advantages for the national economy. It generates technological development of Polish companies, high schools and research institutes and valuable well-paid work places requiring high skills (in case of Polish economy they amount to almost half a million work places).

The development of national industry concerns requires greater attention from the side of public authorities than the start-ups in new technologies sector, especially as the risk of negative verification of the business model in case of start-ups is much higher. Compared to its western counterparts Poland suffers from the shortage of major industry enterprises which translates itself into inability of the Polish technical universities to find a business partner and poor innovation of the overall economy. There is a deficit in terms of experienced companies with cash reserves and creditworthiness ready to take up a challenge of the commercialization of new technologies. This structural weakness of Polish economy is historically m motivated. Polish companies competition with other western entities on an open international market was hampered because of non-market growth conditions in the socialist economy and the consequences of organizational and cultural conditions, for example influences of anti-development groups or inflexible attitude of trade unions. In its difficult past Poland found it harder to be competitive in the open international business market as the obstacles to the market development prevailed in a social economy supported by an overall unwilling organizational and cultural approach displayed by the so called "groups of interests" compounded by an inflexible trade union's stance.

Commercial transactions were limited in the socialist economy for political reasons which instantly affected the insufficient development of companies of high degree product and technology specialization. Different competences were divided amongst different works instead of being concentrated in one entity providing services to those plants. Instead of focusing high skills in competences at one place they would be scattered among different establishments contributing thus to a further inefficiency. Following no top-down centralisation of competencies was carried out. The governments of the so called Third Republic of Poland abandoned a coordinated industry politics, and gave up collecting data on the progress of the companies privatized by the provincial and central authorities.[9]

Western model of capitalism produced companies based on technologies (patents, know-how), skilled employees, knowledge of markets, economic relationships, while the communist bloc exploited solely resources afforded to the by a state, which in turn owned all the existing business undertakings. There was no distinction in the ownership

[9] B. Godusławski, *Prywatyzacyjne fakty i mity. Do dzisiaj nie wiemy, ile firm sprzedaliśmy*, http://biznes.gazetaprawna.pl/artykuly/1087293,prywatyzacyjne-fakty-i-mity.html [access: 25 XI 2017].

of the mining and energy companies (mineral exploration and energy production) and the manufacturing companies (production of machinery and equipment for mining). Though there existed some manifestations of top-down coordination within economic policy in the socialist countries, potent technological companies matching the western standards could not be created.

Their presence on a huge market would require high costs of research and the fixed costs of employing specialists. The challenge of international expansion is not the discretionary management decision but results from the structural need to conduct a specific business activity. The Polish economy undergoing the transformation failed to provide the potential champions with stable conditions sufficient to withstand the strongest turmoil in the market. First of all, because of the dysfunctional model of the political system transformation we were keeping foreign markets away while the domestic market was not sufficiently adequate to accommodate highly specialized companies, devoid of the opportunity to take out loans which would allow them to make a progress in terms of technological development.

The economic failure during the Real Socialism resulted from the central planning policy promoted a far-reaching vertical integration of the industrial plants. Because of the limitation in goods and services available, energy companies created stockpiled in all possible areas (i.e. spur lines, means of transport, component production, refurbishment facilities, catering, hotel facilities, vacation facilities, sports facilities). There were even workplace farms at some bigger companies, aimed at supplying food to cafeterias. In the aftermath of the political changes simple services, like security provision, cleaning, logistics, catering, were handed over to external entities (although sometimes existing still in the holding/within the group). The processes requiring advanced competences and technical background remained within the state energy companies, for example construction works, renovation works, production of components and semi-finished products.

Once deciding on future investments in the production capacity of the subsequent power plants, the Polish government should aim at enhancing their financial condition and technological competences. The analogy to the programme for modernisation of the Polish Military Forces was therefore mentioned before on purpose. With the purchase of weaponry not available in the country, an offset agreement is signed to guarantee a transfer of technologies and involvement of the national companies in the production of components, service and assembly. The energy, oil industry, telecommunication and weaponry are the strategic areas as well, which should be provided with technological and business independence, as the example of South Korea and Taiwan's successful economies prove.

It is a wrongful assumption that the technologies development in the state should be correlated with the development of business organizational structures, which will, in turn, commercialize new products or solutions. The production implementation in Poland is relatively weak and the state-funded implementation of the S&R projects proves to be corporate governance. The political culture of our elites is not particularly

favourable towards new economic projects to be initiated by the state and is domineered by the negative experience in the gallium nitride, graphen commercialization or products based on CNG and LNG-based products.

Facing the upcoming energy transformation triggered by the aging power blocks and the changes within the scope of international regulatory environment, we should open the Polish energy balance to technologies that we already possess or technologies that we are able to master in terms of scientific development and production. Undoubtedly, Polish energy mix will still be based to a large extent on hard coal, lignite, natural gas, biomass and water power. The wind power is included in the options and nuclear energy is still under consideration. I think that given the choice between two types of technology of comparable costs (for example wind power plants at sea and nuclear power plants) we should take into account a higher share of polonisation of the financial stream which undeniably works in favour of wind energy. The reduction of the prolonged construction risk, exceeded costs calculations or even the risk of suspending works should convince us that nuclear energy is too complex for us. We have already stopped the construction of a nuclear plant in the town of Żarnowiec once and the work schedule described by the Council of Ministers in a document *The Polish Nuclear Energy Programme* of 28 January 2014 is already overrun. Unfortunately, at present we are following Brazil's footsteps. The country is a model example of the immature energy policy and its nuclear programme looks as follows:

The construction of the first Brazilian nuclear power plant started in 1971 in Angra dos Reis, a town with no manufacturing traditions ca. 130 km from Rio de Janeiro, 220 km from São Paulo and 350 km from Minas Gerais. One of the national energy business concerns was the investor and the American Westinghouse supplied technology. The first block, Angra with a capacity of 657 MW, was finished in 1985 after 14 years: construction and two court trials and numerous shortcomings on both sides. The contract with Westinghouse was a turn-key project without handing over key technologies (including uranium enrichment technology, i.e. fuel production for their own plant) to the Brazil party. Therefore the Brazilians signed a cooperation agreement already in 1975 with German Siemens for constructing subsequent blocks and additionally transferring the technology of nuclear fuel production across the ocean. The construction of the two reactors was launched based on the Siemens technology. Due to the money shortages, the construction was suspended in the years 1986-1995. It was only in 2000, when the construction of Angra II reactor was completed. Following the blackout in 1999 caused by the water plants shut-down caused by a draught, further construction has been accelerated. The construction of third reactor started in 1984 and has been continued since 2009 in cooperation with the French Areva, despite previous announcements that Brazil would achieve total technological autonomy in the whole cycle of uranium extraction and enrichment, power plant construction, power generation and nuclear waste disposal two years earlier. It is worth mentioning that Brazil is endowed with uranium resources, more than 5% of the world's resources,

so it is naturally destined to use nuclear energy (unlike Poland).[10] In spite of the ambitious plans from 1960s and periodically confirmed construction of at least three nuclear power plants, the construction of the first one is due to be completed only in a few years time, after the elapse almost 50 years since the implementation project began.

There is no doubt that Brazil is currently technologically much more advanced in nuclear energy than Poland. Nevertheless, the path it had taken (the costs of roughly several billion of the then dollars over 50 years), does not encourage to take up similar challenges by Poland. The acquisition of the nuclear technology from a foreign partner in case of a post-colonial country, with a poor institutional structure, financial markets, unstable political system and non-established political culture will, most probably, be doomed to failure. Such experience for Poland, although on a smaller scale, was the construction of a gas terminal in Świnoujście. Its contractor, Italian Saipem, exceeded investment budget and was overdue with the schedule of putting it into operation. For the last few years, it was the same with most nuclear investments conducted by western companies (Olkiluoto in Finnland, Hinkley Point in the UK, Vogtle in Georgia and Virgil C. Summer w South Carolina). Problems encountered by Slovakia are also worth mentioning. There are already four reactors in the state. It may be concluded that the country has some experience in nuclear technology. The construction of the two additional blocks in Mochovce power plant started in 1998 and it was resumed in 2008 after 10 years. The schedule of works was extended in 2017 for another six-year period, raising estimated expenses for the fourth time, although the costs exceeded twice the base level. Money is frozen for a long time without positive cash flow. This is the risk we should be aware of.

The cost of 1 MW in nuclear power plant has been constantly increasing and in case of the wind power plants at sea it has been constantly decreasing. So, maybe guided by the principle of the country's own energy sources (renewable and fossil) and our own energy production technologies, it would be much quicker to develop a company producing wind turbines than trying to master nuclear energy technology in energy sector. We would avoid the risk of growing costs and deadlines as well as future accidents and problems with radioactive waste disposal. The decision of the German government on the nuclear power abandonment should be a lesson to us not to follow the same path. Two companies executing at the moment their projects of wind farms on the Baltic Sea, i.e. Polenergia 1 200 MW and PGE Energia Odnawialna 1 040 MW had planned their power at the level of two out of the three nuclear power plants planned in the Pomerania Region. In 2017 the construction cost of 1 MW in a nuclear power plant exceeded (in case of the French and American technologies) the cost of the same investment in wind power. The advantages of wind power plants are lower operating costs, shorter construction time, reduced risk of failure and no fuel costs. The disadvantages are the lack of controll ability and the lower installed capacity

[10] *Angra-3 PWR Nuclear, Brazil*, http://www.power-technology.com/projects/angranuclear/ [access: 22 VIII 2017].

utilization rate. Therefore, they require their complementing with a reserve source (preferably gas), which is the cheapest in terms of investment level (CAPEX) and the most expensive in usage (OPEX). Nevertheless, we should remember that nuclear power plants are also inflexible: during night time hours with low energy demand they can reduce their production only by 10% of the installed power. A predominant argument in the decision making process as far as new energy mix for Poland is concerned shall be the possibility to use domestic technologies and the engagement of Polish suppliers of generating installations. Currently, the Polish shipbuilding industry (i.a. Stocznia Remontowa Nauta S.A. and Energomontaż-Północ Gdynia S.A.) provides components for the offshore wind farms. Nevertheless, this involves much lower investment costs compared to those that would be allocated abroad for the nuclear power plant. Maintaining the financial flow for the purposes of the transformation of the Polish energy sector will be decisive factor in the potential promotion to a group of developed countries. Since, the key to development is strengthening mining sector and energy production domestic companies. It is a chance for Polish industrial policy which cannot be overlooked and wasted.

Abstract

Energy security comprises of four factors: independence of energy sources; stability of energy system, electricity lines and pipelines; diversification of both foreign supplies of energy sources and energy mix structure; technology autarky meaning domestic ownership of energy enterprises. This paper is focused on the fourth factor. Author indicates that Poland has well developed industry of hard coal and lignite mining, building coal, wind and hydroelectric power plants. Polish industry's shortage is a lack of domestic producer of steam and wind turbines. Polish companies have the smallest potential in building a nuclear power plant. In case polish government decided to build one it would cause a leakage of billions of zlotys abroad.

Keywords: energy security, energy mix, energy independence, economy, energy sector.

Krzysztof Tylutki

The information of a mass destruction range – OSINT in intelligence activities

> Where is the wisdom we had lost in the knowledge?
> Where is the knowledge we had lost in information?[1]…
> Where is the information we had lost in bites…

In the current world defined as the information civilization, information has become an elementary and strategic raw material whose value, apart from its intellectual input, is perceived in terms of being a precious asset. It is claimed for a reason that the one who owns knowledge – information to be more precise and exact - owns power. One must agree with James Gleick that information is omnipresent, it governs the modern world – supplying it with blood and fuel.[2] The resolution adopted by the United Nations General Assembly in 2016 included recommendations to treat access to the Internet (regarded as the biggest source of information) in the same way as the right to live and one of the basic human rights.[3] The information itself has also became an element of an information war, the current mode of global fight to achieve superiority over the adversary, to gain certain strategic goals, to dominate in the security environment. Glynn Harmon assumes that information is a kind of metaenergy which tends to move more energy and decides about vibrancy of activities taken by individuals.[4] General Shalikashvili took note of this relationship professing that as long as the information on his victory shows up in the open source media, on CNN, he will not recognize that he had won the war.

The concept of information is complex and occurs in numerous scientific disciplines. It was used for the first time in the late 19th century by an Austrian scientist Boltzmann to describe changes in the physical processes. Nevertheless, it is an American mathematician, Claude E. Shannon, who is recognized as the father of the information theory. For him information constituted the selection of possible choices. He defined and assigned an information measurement unit to **a bit**, i.e. the volume of information which is essential to select between two equally probable and mutually exclusive options. According to the International Standard ISO 5127:2001 information is the data, processed, organised and correlated to give them

[1] T.S. Eliot, *Choruses from the Rock*, https://www.bayes.it/pdf/Choruses_FromTheRock.pdf [access: 19 VI 2018]

[2] J. Gleick, *Informacja – bit, wszechświat, rewolucja.* Kraków 2012, p. 14.

[3] See. *Report of the Human Rights Council on its thirty-second session*, UN General Assembly, Human Rights Council, Thirty-second session, A/HRC/32/L.20, 27 VI 2016.

[4] See. G. Harmon, *The measurement of information,* Information Processing and Management 1984, no. 1-2.

the real substance.[5] It applies to facts, notions, objects, events, ideas and processes.[6] According to Piotr Sienkiewicz information is a collection of facts, events, features included in a message/news, and provided in a form that enables the recipient to develop a relevant attitude towards it and undertake adequate mental or physical activities.[7] Information, as Merriam-Webster rightly points out, is simply the knowledge acquired from other people, studying, or observations and research. In other words, information – according to the definition given by *The Dictionary of Polish Language*[8], is basically intelligence.

The following particular functions of the information may give a better understanding of the notion itself:

- **illustrating function**– describing reality, reflecting its image;
- **decision-making function** – is a motive for actions;
- **steering function** – building computer systems, knowledge base, being at the core of planning and taking best rational decisions;
- **progressive function** – developing knowledge;
- **capital-building function** – making you dependent on financial resources, facilities, people and their knowledge;
- **culture building function** – addressing spiritual needs of people;
- **communication function** – enabling participation in the social life;
- **integration function** – fostering the development of interpersonal relations;
- **ideological function** – developing the awareness of the society's participation in the public life of the state;
- **opinion shaping function** – shaping views, public opinion on a given topic[9];
- **informative function** – providing necessary knowledge making analytical work more effective;
- **coordinating function** – organising and harmonising parallel actions;
- **monitoring function** – verifying and assessing the quality and coherence of data, its functionality according to the established security rules.

Based on the above list one may assume that information is virtually a commodity, an artefact made by human being, which has its price and a recipient. It is a constituent of human's knowledge and the key factor to be considered in the process of decision making and organizing processes at the production phase. Thus it contributes to the creation of a specific analytical product.[10] To make this product possibly most sufficiently valuable, the information should feature the following qualities to the maximum possible extent, i.e. it needs to be:

---

[5] ISO 22320:2011, *Social security – Emergency management – Requirements for incident response*, November 2011.

[6] ISO 2382-1:1993, *Information technology – Vocabulary*, Part 1: *Fundamental terms*, November 1993.

[7] P. Sienkiewicz, *10 wykładów*, Akademia Obrony Narodowej, Warszawa 2005, p. 62.

[8] *Słownik Języka Polskiego*, M. Szymczak (ed.), vol. 1–3, Warszawa 1978–1981, p. 863.

[9] See. B. Stefanowicz, *Informacja. Wiedza. Mądrość*, vol. 66, Warszawa 2013, pp. 42–45.

[10] Ibidem, p. 36.

- **precise** – providing accurate and reliable reflection of reality;
- **up-to-date** – available on an as-needed basis to decision makers, enabling them to act accordingly, and when it becomes the grounds for action-taking;
- **complete** – it gives decision makers all required facts and details, gives the full picture of situation without any distortions;
- **significant** – useful for decision makers to pursue specific requirements occurring in special conditions.

Each source of information has its inherent features, and is perceived differently by each of us. Information on the Internet is deemed as reliable and easily accessible, the TV-originating information is treated as unbiased and valid, and the press information balanced and solid.[11] From the studies carried out by Krystyna Polańska, it transpires that the key elements in assessing the veracity of information comprise: trust in a source providing the information, the validity of information, logical connection between the information and other facts or pieces of information as well as supplying such information by other independent sources.[12] The reliable, unbiased and current information is accompanied by the inflow of a confusing or wilfully misleading information. One cannot rely on the veracity of the information based on its volume – as it happens – the excessive influx of the information often proves untrue, fake and serves disinformation purposes.[13] The information manipulation can be revealed at the stage of its assessment, selection and choice. After all, the functionality of Web 2.0 allows posting anything by any random user of this virtual social network. Just to give a few examples of the information manipulation let us recall some anonymous editors from Wikipedia who "buried" on the net two, alive and still kicking, American senators Ted Kennedy and Robert Byrd prematurely. The article on the civil war in Syria which came out in 2012 was due to a very rapid and dynamic pace of developments in the area edited by the users of Wikipedia more than 7,500 times which, as a result, made it very difficult to get a clear, coherent picture of the conflict situation. However, it was none of other than George W. Bush, the former president of the USA who broke the record in having his own biography updated in excess of 20,000 times.

Considering the time information was obtained and the manner it can be exploited in the process of decision making the following types of information can be distinguished:

- **reporting information** – providing an account of a past or current event recounting an event which happened or has been happening;

---

[11] K. Stankiewicz, *Wpływ Internetu na percepcję wiarygodności informacji*, in: L. Haber, *Społeczeństwo informacyjne. Wizja czy rzeczywistość?*, Kraków 2004, p. 409.

[12] See. K. Polańska, *Informacja, jej wiarygodność i co z nich dla nas wynika*, in: *Informacja – dobra lub zła nowina*, A. Szewczyk (ed.), Szczecin 2004.

[13] Vladimir Volkoff, an expert on disinformation and conscious manipulation, defines disinformation as an activity taken with serious measures engaged, systematic and professional, always via mass media and addressed to the public. Its goal is to realize consistent program to change the consciousness and even sub consciousness of the public in terms of their views or beliefs regarded as unfavorable for disinformant into such that are favorable, See. V. Volkoff, *Dezinformacja: oręż wojny*, Warszawa 1991, pp. 6–8.

- **pre-emptive information** – revealing the actions planned, activities in the area of interest, proves to be the most desirable, valuable information in the decision making process;
- **verifying information** – acknowledging the existing knowledge with respect to some subject-matter, phenomenon occurrence.

The demand for information is not a fixed value. It fluctuates depending on time, actual situation. It differs on the particular levels of decision making process, starting from a tactical level or operational level to a strategic one. The higher management level the higher concentration of information and the broader substantive scope. The lower management levels should deal with information of a more detailed, limited scope nature. This information layout is referred to "an inverted information pyramid". The information pyramid featuring the volume, extent and the degree of the detail of information is inversely proportional to the structural pyramid defining duties, competences and responsibilities.[14]

The information generated by people is on a constant rise. The digital world we live in – according to the CIA Deputy Director, Andrew Hallman – undermines the rule of conspiracy underlying the intelligence activities, making it e.g. increasingly difficult to keep an officer under cover secret, once everyone carries a TV studio in their pocket.[15] The Big Data growth rate[16], i.e. the set of information of a large volume, diversity, variability, and value is continually increasing (ranging from 40 to 60 percent p.a.) constituting a processing and analytical challenge for those concerned.[17] In the mid-1980s, when the scientific centres and universities began to appreciate the added value and capabilities of the Internet, only 6% of all materials was digitalized. At present almost 99% of life and cultural heritage appears in a digital form. It is estimated that in 1992 100 GB was produced every day, while in 1997 the equivalent volume of data

[14] B. Nogalski, B.M. Surawski, *Informacja strategiczna i jej rola w zarządzaniu przedsiębiorstwem*, in: *Informacja w zarządzaniu przedsiębiorstwem. Pozyskiwanie, wykorzystywanie i ochrona (wybrane problemy teorii i praktyki)*, R. Borowiecki, M. Kwieciński (ed.), Kraków 2003, Zakamycze, pp. 205–206.

[15] P. Tucker, *Meet the Man Reinventing CIA for the Big Data Era*, 1 X 2015, https://www.defenseone.com/technology/2015/10/meet-man-reinventing-cia-big-data-era/122453/ [access: 3 I 2018].

[16] „BIG DATA" is defined by 4 factors describing the sets of information – 4 V, i.e. **Volume** (data amount), **Variety** (diversity of analyzed data and information), **Velocity** (processing in real time) and **Value** – value we can get by combining all previously mentioned factors, supporting analytical and decision making processes. See T. Słoniewski, *Od BI do „Big Data*", in: *Nowa twarz Business Intelligence*, (ed.) R. Jesionek, http://it-manager.pl/wp-content/uploads/Nowa-twarz-BI1.pdf [access: 7 V 2018].

[17] For example: the book collection of the Library of Congress in 2010 included 160 TB of information; eBay online in 2011 had 9 PB of information; Google search engine in 2008 was processing 24 PB per day, and to sort 1 PB of data in 6 hours and 2 minutes it needed 4000 computers. 4 experiments in the Large Hadron Collider by CERN produce more than 15 PB of data each year; Internet Archive in 2014 had 50 PB of data; during transfers of e-mail accounts from Hotmail to Outlook Microsoft transferred 150 PB of data; and the data gathered on Facebook in 2014 it is 300 PB – three times more than in 2013, every 24 hours was coming ca. 600 TB.

was generated in an hour, to reach merely a second in 2002.[18]At present 50,000 GB is generated every second. It has been estimated that in 2017 the digital space has reached 16 ZB. According to the forecasts provided by the Oracle, the mankind is likely to generate over 45 ZB (zettabyte) on the web until 2020, which will translate into over 5,2 GB of data per capita worldwide. The Digital Universe, IDC, in turn, assesses that in 2020 there will be 44 ZB of data generated and almost 40% of information in a digital world will be available in a cloud computing.[19] It is additionally argued that in 2021 the management of data will increase by 50% compared to 2011.[20]

It has been assessed that the volume of digital information generated up to 2007 equalled 281 EB (exabytes (trillion bytes), approx. 10^{18} bytes). It had been growing constantly over the years to reach in 2011 the amount of ca. 1,8 ZB (zettabytes). The authors of the report issued by the executive office of the US President came to that conclusions.[21] In terms of volume the information could be accommodated in 57,5 billion of Apple iPads 32 GB memory each. To get a clearer picture compare it to the Great Wall of China of a double average height. One can also learn that in 2011 20 billion times more information was generated worldwide (988 exabytes) than all that had been written up to date in the history of humankind.[22] To compare, this is so much information that an individual from a developed country has at their disposal during one hour or two generations back in the course of his whole life. In 2013 there were already 4 ZB of information generated worldwide. This volume corresponds to the total sum of pictures taken every second by every single US citizen for over more than 4 months of their life.[23] The Americans carried out the tests which disclosed that in 2008 people exploited, on average, 34 GB of information and 100 500 words per day. On average, 35% of it was derived from TV, 10% from films and 55% from computer games. Compared to 1980s the consumption of words had increased by 140%, while the increase of digital information went up by 350%. In 2008 media consumed 3,6 ZB information in total and 1,080 trillion of words per day.[24]

The rapid pace of data growth results from the need of a common communication and the development of the area called the Internet of Things, within the framework

[18] The gigabyte is a multiple of the unit byte for digital information. The prefix *giga* means 10^9 in the International System of Units (SI). Therefore, one gigabyte is 1000000000 bytes. The unit symbol for the gigabyte is GB. There are also **terabyte**, TB (10^{12}), **petabyte**, PB (10^{15}), **exabyte**, EB (10^{18}) and **zettabyte**, ZB (10^{21}) used in the text.

[19] Staying in the so called cloud. IBM defines the phenomenon as a model of maintenance and processing style, in which IT data and resources are provided as services.

[20] See. J. Gantz, D. Reinsel, *Extracting value from chaos*, in: *IDC analyze the future,* June 2011. https://www.emc.com/collateral/analyst-reports/idc-extracting-value-from-chaos-ar.pdf [access: 4 VI 2018].

[21] *Big Data: Seizing Opportunities, Preserving Values*, Executive Office of the President, The White House, Washington DC, May 2014, pp.7–8, data included in the report come from: J. Gantz, D. Reinsel, *Extracting Value from Chaos*, IDC, 2011; Mary Meeker and Liang Yu, Internet Trends, Kleiner Perkins Caulfield Byers, 2013.

[22] See. M. Karnowski, E. Mistewicz, *Anatomia władzy*, Warszawa 2010, p. 114.

[23] *Big Data: Seizing Opportunities* …, p. 8.

[24] R. Bohn, J. Short, *Measuring Consumer Information*, International Journal of Communication 6 (2012), 980–1000, University of California, San Diego.

of which the increasing number of devices is likely to gather and process data online. Within the next few years we can expect data explosion. The users themselves also take part in the chain of duplicating information – by copying all sorts of content, commentaries and by classifying them as a subsequent secondary source of information, without providing its original source. This phenomenon is referred to as the "echo effect".

As the Nobel prize winner, Herbert Simon, claimed information focuses the attention of its recipients. A slight tension, the so called cognitive dissonance may accompany this process, if the addressee of the information finds its content inconsistent with his/her opinions or beliefs. We tend to ignore such information, treat it less seriously or even distort it. The level of information absorption is different for everyone. It is contingent, to a great extent, on the volume and quality of the *a priori* information.[25] With time a fatigue syndrome develops, the so called attention crash, caused not so much by the inability to adequately select the simple message but to understand it. James Gleick calls this factor the Devil of Information Overload, i.e. Too Much Information – TMI.[26] It happens this way also because hippocampus[27] - the hardware of a human brain has its biological constraints. In 1986 Thomas K. Landauer, an academic at The Colorado University Psychology Department, assumed in his works that a human brain is able to retain ca. 11 TB of information.[28] According to contemporary studies by StorageCraft experts human brain can comprise from 100 TB to 2,5 PB data. To compare, if the *human hard disc* operated as a video digital recorder in a TV set, this volume would be sufficient to store 3 million hours of films. In order to exploit the entire memory, the TV set should never be switched off for more than 300 years. The studies by American scientists reveal that our biological computer is able to store not more than ca. 1 PB data.

Information overload makes it more difficult for people to process and understand it and ultimately leads to its misinterpretation. Therefore is not easy to assign a proper analyst to a particular task. The vastness of information passed by a colonel of the Russian Military Intelligence (GRU), Oleg Penkovsky made the Americans (CIA) and the British (MI6) engage together 30 translators and analysts.[29] The imprecise transcript of the conversation between the CIA officers and a KGB agent, Yuriy Nosenko, during which he was proffering his assistance to the West, brought about the rejection of his candidacy as a potential source of information and him being deemed a liar. The conclusions of the analytical report precluded the development of an objective analysis of the Russian captain. Most of the testimonies provided by him were written up on the basis of the memorised declarations of his, which made even worse by linguistic shortcomings of the examiners

[25] S.E. Zločevskij and others, *Informacja w badaniach naukowych*, Warszawa 1972, p. 231.

[26] J. Gleick, *Informacja – bit, wszechświat*…, p.16.

[27] The hippocampus belongs to the limbic system and plays important roles in the consolidation of information from short-term memory to long-term memory, and in spatial memory that enables navigation.

[28] T.K. Landauer, *How Much do People Remember? Some Estimates of the Quantity of Learned Information in Long-Term Memory*, Cognitive Science 1986, no. 10, pp. 477–493.

[29] J. Larecki, *W kręgu tajemnic wywiadu*, Warszawa 2007, pp. 157–158.

were interpreted by Americans in an unfavourable manner. The name of the school he graduated from was misspelled and instead of gen. Frunze Navy High School (a Soviet war hero), they wrote gen. Frunze Military Academy, the so-called Soviet West Point. Having analysed the extensive CIA archives, its former agent John L. Hart concluded that the counterintelligence studies and analyses were so lengthy and sophisticated that only a handful of superiors managed to wade through them and analyse the reasons of the purported duplicity of Nosenko.[30] General Robert Kehler, Chief Commander of the United States Strategic Command – US STRATCOM, with years of experience under his belt noticed that the Pentagon was sinking under a deluge of intelligence data. The increasingly more efficient and numerous satellites and spotter planes are capable of supplying such volume of intelligence that the analysts were not able to handle it. The amount of data has increased by 1500% over five years and the capabilities of processing it have increased merely by 30%.[31]

A National Security Agency (NSA) officer, William Binney reached similar conclusions, adding that gathering random data resulted in the officers overburdened with the influx of too much data abandoning the analysis in favour of a simple search of data bases on the basis of key words. It generates a lot of meaningless hits rather than significant connections between the data.[32] This could have been a reason for a delay in passing the information by the American Immigration Office to the Huffman Aviation International in Venice, Florida, that two of the latter WTC bombers, Mohammed Atta and Marwan Alshehi had been granted student visas. The aviation school got this information six months after the WTC attacks. A confirmation of these conclusions is the moment of intercepting by the National Security Agency – NSA in September 10, 2001 of the two pieces of information in the Arabic language which included the information on what was to happen the next day. The two pieces of information were translated only later after the World Trade Centre attacks took place. Additionally, in the summer of 2001, few months before 9/11, Osama bin Laden together with his commanders had given an extensive interview for the Centre of Middle East Media, in which there was a mention of some general leads on the planned large-scale attacks on American facilities.[33] Some experts assess that from 50 to 80% of data in the interest of special services of western countries is not published in the English language.[34]

---

[30] J.L. Hart, *Walka wywiadów. Rosjanie w CIA*, Warszawa 2003, p. 155.

[31] Costlow*, Kehler raises trial balloon: Put STRATCOM in charge of all GEOINT PED*, October 19, 2011, http://defensesystems.com/articles/2011/10/19/geoint-kehler-stratcom-geospatial intelligence.aspx [access: 2 V 2018].

[32] R. Koerner, *William Binney: NSA Claim Not to Be Mining Content Is an "Outright Lie"*, 22 VII 2015, https://www.huffingtonpost.com/robin-koerner/nsa-whisteblower-nsa-clai_b_7837806.html [access: 4 V 2018].

[33] P. Bergen, *Why U.S. can't find Osama bin Laden*, October 19, 2010, http://edition.cnn.com/2010/OPINION/10/19/bergen.finding.bin.laden/ [access: 2 V 2018].

[34] M.M. Lowenthal, *Open Source Intelligence: New Myths, New Realities*, in: *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, R.Z. George, R.D. Kline (ed.), Lanham 2006, p. 277.

Information may be a superpower if only it can be assessed at the place in need thereof, by an individual in the need thereof and for the purpose required. The excessive volume of disarranged information may be a liability rather than an asset. The more success in data gathering the more drowning in the ocean of data. David Foster Wallace calls this phenomenon "a tsunami of available facts, contexts and perspectives".[35] In one of the CIA's operations carried out between 1954 and 1955 at the border between two occupation zones in Berlin, the Americans recorded 6 million hours of telephone calls between Moscow and Karlshors, where the main KGB Rezidentura in the German Democratic Republic was located and between Moscow and Wünsdorf (housing – as per literature available - the Soviet military headquarters). The information thus collected was translated and analysed for the subsequent two years after the operation had been completed. Despite the passage of time the successor services still grappled with the information overflow. In 1989, when the German Democratic Republic ceased to exist, the staff of the Ministerium für Staatssicherheit – commonly known as the Stasi, analyzed materials derived from the phone-tapping in the mid 1980s.[36]

It is not difficult to get disoriented, muddled up in the process of gathering open sources information, especially if it comes from the Internet, the capacity of which was estimated by Eric Schmidt at 5 million TB. The consistently growing number of visa applications lodged by foreigners with the immigration offices leads to a chaos which makes it even more difficult for the authorities to accurately verify the actual reason for which the applicants wish to change their country of stay. This is a procedure of administrative nature, and consists primarily of the documentation collected on the basis of community interviews and background checks. The lack or cursory verification of the open source information by the immigration services and the FBI in the process of the assessment of the potential threats to the internal security of the state, enabled Tashfeen Malik settling down in the US. The immigrant from Pakistan, a high-risk country, for a couple of years had been declaring her support for the jihad and posted anti-American comments on one of the social websites. On 2 December 2015 she and her husband carried out an attack at the Inland Regional Centre in San Bernardino, California, in which 14 people were killed and more than 20 others were seriously injured.[37]

90% of intelligence comes from open sources. The remaining 10% which is gained in a more spectacular way comes from the secret one. The genuine hero of the intelligence activity is Sherlock Holmes not James Bond.[38] The potential

[35] J. Gleick, *Informacja*…, p. 374.

[36] P. Żuk, *Demokracja pod kontrolą – czyli podsłuch non stop*, 8 VI 2015, http://www.tygodnikprzeglad.pl/demokracja-pod-kontrola-czyli-podsluch-non-stop/ [access: 5 V 2018].

[37] M. Apuzzo, M.S. Schmidt, J. Preston, *U.S. Visa Process Missed San Bernardino Wife's Zealotry on Social Media*, December 12, 2015, http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html [access: 6 V 2018].

[38] Cited from gen. S.V. Wilson, Director of the US Defense Intelligence Agency.

of OSINT[39] (open source intelligence),[40] i.e. the data collected from an overt, publicly available sources was appreciated by humankind since time immemorial. The history of using publicly available information dates back to the early attempts at collecting intelligence of strategic value which supported the decision-making process of a sovereign - governments in the matters of national security and defence. The OSINT tools[41] have evolved in line with technological progress, events which were rightly recognized by the National Geographic[42] as those that revolutionised the world. The access to such tools was initiated and popularized by mass media[43] – press, radio, television with the major input of made by a computer and the Internet revolution developing social networks, i.e. enabling social media communication possible.[44]

[39] Three stages of open source analysis can be distinguished: **the Open Source Data** (**OSD**) – data from overt sources, the "raw data", from an original source in printed, digital form, presented as photographs, recordings, satellite images and so on; **the Open Source Information (OSIF)** – information from overt sources, extensively developed, contained in one piece, edited, verified, filtered in relation to its presentation (press releases, books, publications, reports); **the Validated Open Source Intelligence** (**OSINT-V**) – verified open source intelligence, with high degree of reliability thanks to analysis of covert information done by an analyst. It is possible to extend OSINT to **the Open Source Acquisition** – acquisition of over source information from available open sources which have already been collected and passed by a researcher, **Open Source** – it can be both a single individual as well as a group providing information. The information itself nor the relation between the information and the subject interested in gaining it, is not classified. Open source data can be publicly available but not all publicly available information is an open source. The notion *open source* refers to publicly available means and it should not be limited only to physical individuals. **The publicly available information** – generally available information, data, facts, manuals, published materials or publicly transmitted materials, available to all, gained by observation or hearing or gained during meetings open for the whole society.

[40] OSINT was defined, inter alia, by the US Director of National Intelligence (DNI) in: *National Defense Authorization Act for Fiscal Year 2014*, (Public Law 113-66, 26 XII 2013) and the US Intelligence Community in Intelligence Community Directive Number 301, NATIONAL OPEN SOURCE ENTERPRISE 2006.

[41] There can be distinguished two intelligence areas within OSINT: **the Social Media Intelligence** (**SOCMINT**) focused on the recognition and monitoring profiles of social media users and their posts, gathering information from open and closed social groups. The second area, **the Web Intelligence** (**WEBINT**), explores data, looks for and stores data in the Internet.

[42] See. *100 Events That Changed the World*, National Geographic, 2015. Special Issue.

[43] Radio broadcasting needed 30 years to get 50 million listeners, TV 14 years to gather such amount of viewers, the Internet gathered such amount of followers in only 4 years time.

[44] The Social Media Intelligence (SOCMINT) is one element of OSINT and refers to the collective tools and solutions that allow organizations to monitor social channels and conversations, respond to social signals and synthesize social data points into meaningful trends and analysis based on the user's needs. Social media intelligence allows one to collect intelligence gathering from the social media sites. The term SOCMINT was proposed in a 2012 paper written by David Omand, Jamie Bartlett and Carl Miller for the Centre for the Analysis of Social Media, at the London-based think tank, Demos – D. Omand, J. Bartlett and C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, Intelligence and National Security, 28 September 2012.

The open source intelligence[45] appears both in the civilian and the military world. It is mostly exploited by security-related public institutions and, more and more often, by private sector and even terrorist organisations because it supports all decision making processes by providing the required information. The OSINT fulfils the following functions[46]:

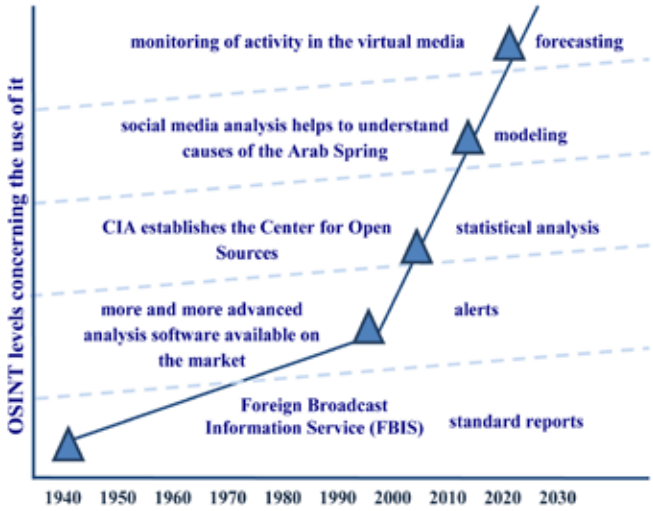
- it underlies every action at each single stage. It provides background for the information supplied whose meaning depends on social, cultural or political context.
- It meets intelligence requirements and without the need to seek support from experts or using other operational means (secret methods).
- It deepens and verifies the knowledge already possessed.
- Enables decision makers to use all available sources of information in a decision making process.

The history of OSINT involves to a great extent the history of the US intelligence. It used to be one of the major sources of information regarding the military capabilities and political plans of the adversaries (early warning and risks forecast including). The Americans were pioneers in gathering data as they developed monitoring capabilities, filtering, translating, or archiving information from the foreign media. With regard to the process of monitoring open sources, which, at the very beginning, involved following press reports, the commercial sector was ahead of the governmental activities for a long time. Before the intelligence got professional and formally institutionalized as a key element of the national security apparatus, in the second half of the 20th century gathering and analysis of open sources by the government had been evolving from a non orderly process to the activities of strategic nature requiring a certain set of methods and tools.

The following scheme shows a direction of OSINT evolution and its main areas allowing to develop a suitable analytical product for the intelligence purposes in 20th and 21st centuries.

[45] Apart from traditional sources of information there are also commercial data bases like economic catalogues, statistics catalogues, private registers, the so called grey literature, i.e. draft reports, unofficial governmental documents, reprints, studies and market research, research reports, individual experts, high school lecturers, scientific literature, conference materials, studies of scientific centres.

[46] Open Source Intelligence, Headquarters, Department of Army, Army Techniques Publication, ATP 2-22.9, Washington, DC, 10 July 2012, p. 2-2.



Scheme. Evolution of OSINT possibilities.

Source: Private study on the basis of Disruptive Innovation, *Case study: Intelligence – Open-source data analytics,* Deloitte, Washington, DC, 2012, p. 3.

The value of the open source intelligence data was appreciated already in the 18th century during the American revolution by George Washington, who drew upon an update on current developments from the press releases or generally accessible information on the British troops or activities of spies.[47] Some years later, in 1808, the British Duke of Wellington during a battle against Napoleon on the Iberian Peninsula advised his generals to read daily newspapers, including The Times, where the process of formation of the French infantry units was broadly described.[48] In 1863 during the Gettysburg Campaign General Lee's intelligence was monitoring movements of the troops in the north by monitoring press releases.[49] In the years 1899-1902 during the Philippine War the American military strategists had to rely on the intelligence reports which were actually copies of encyclopaedia articles.[50] During the two world wars books and newspapers were sources of valuable information used by the military intelligence. In France general Patton's army were using Michelin's maps for geospatial recognition[51], available at petrol stations.

[47] *A Look Back ... George Washington: America's First Military Intelligence Director*, 12 VII 2007, https://www.cia.gov/news-information/featured-story-archive/2007-featured-storyarchive/george-washington.html [access: 5 V 2018].

[48] S.D. Gibson, *Exploring the Role and Value of Open Source Intelligence*, in: *Open Source Intelligence in Twenty-First Century*, Ch. Hobbes, D. Sailsbury (eds.), New York 2014, p. 13.

[49] E.B. Coddington, Ch. Scribner's Sons, *The Gettysburg Campaign – A Study in Command*, 1968, p.19.

[50] B. McAllister Linn, *The Philippine War: 1899–1902*, University Press of Kansas, 2000.

[51] R.A. Norton, Ph.D., *Guide to Open Source Intelligence, A Growing Window into the World*, The Intelligencer Journal of U.S. Intelligence Studies, vol. 18, no. 2, Winter/Spring 2011, p. 66.

In 1939 the British government requested the BBC to launch a commercial service to round up foreign press releases and radio broadcasts in the Digest of Foreign Broadcasts, later called the Summary of World Broadcasts and currently it is known as the BBC Monitoring. In the BBC manual from 1940 the goal of the service was described as the creation of "the modern Tower of Babel where voices of both friends and enemies were heard".[52] In the mid 1943 BBC was monitoring 1,25 million transmissions per day. A formal partnership between the BBC and its American counterpart was established between 1947 and 1948 by away of an arrangement on the full exchange of information. In 1948 the Aeronautical Research Unit was transformed into the US Library of Congress in order to provide non-standard research and analytical services using broad library resources. At present it operates as the Federal Research Division.[53]

In 1941 by the decision of President Roosevelt the Foreign Broadcast Monitoring Service – FBMS in the USA was created. Its task was to provide monitoring, translation, transcription and the analysis of information derived from radio broadcasts aired by the Axis powers. Until the end of 1942 its capability to translate was more than 500,000 words per day from 25 radio stations broadcasting in 15 languages.[54] The Interdepartmental Committee for the Acquisition of Foreign Publications also monitored and analyzed press releases and publications overseas during the war. At the end of the war there was a tremendous volume of 45,000 pages of text per week dispatched for analysis. In the last days of war it had 300,000 of photographs, 350,000 volumes of magazines, 50,000 books, more than 1 million maps and 300,000 of other documents.[55]

During the Cold War the American Office of Strategic Research was getting information on the nuclear capabilities of other countries overseas from official, publicly known and available governmental reports from those countries as well as from scientist publications[56] (with the USSR, China and France remaining the focal point of interest). At the same time the Office of Economic Research was benefiting from overt, publicly available information regarding, inter alia, the oil production by the OPEC, the output of grain in the Soviet Union, the buying power of foreign currencies or the purchasing power of foreign companies.[57] The development of the Soviet space program was also monitored by the CIA and the US Air Forces via specialized literature available.[58]

---

[52] F. Schaurer, J. Störger, *Guide to the Study of Intelligence*. *The Evolution of Open Source Intelligence (OSINT)*, „The Intelligencer: Journal of U.S. Intelligence Studies" 2013, no. 3, p. 53.

[53] Ibidem.

[54] K. Leetaru, *The Scope of FBIS and BBC Open-Source Media Coverage*, 1979–2008 (U), Studies in Intelligence, vol. 54, no. 1, March 2010, p. 19.

[55] A. Olcott, *Open Source Intelligence in a Networked World*, London-New York 2012, p. 16.

[56] T.T. Stafford, *The U.S. Intelligence Community*, University Press of America, 1983, pp. 58–60.

[57] J.T. Richelson, *The U.S. Intelligence Community*, Fourth Edition, Chapter 12, Westview Press, 1999.

[58] J.J. Bagnall, *The Exploitation of Russian Scientific Literature for Intelligence Purposes*, Studies in Intelligence, Summer 1958, pp. 45–49.

During the Cold War the German Stasi had been analyzing ca. 1,000 Western magazines and 100 books per month and 12 hours of radio and TV broadcasts in the West Germany per day.[59] To date German services have been appreciative of the open source intelligence. In one of the key units of the Bundesnachrichtendienst – BND, playing an analytical role, most of the material being analyzed – 85% are open source information (magazines, newspapers, radio broadcasts, media reports, booklets and the Internet). Only 10% of the information comes from technical recognition and 5% from HUMINT.[60]

In the 1950s Sherman Kent, deemed the father of intelligence analysis, ordered a report on the American military forces to be drawn up by his university's historians. It was to rely on open sources only and incorporate the types, volume and status of all weapon available, as well as the info on the dislocation of units up to the level of a division. After a 3-month works Kent received a few hundred pages and analyses with a 30-page summary. It turned out that the report was in 90% accurate reflection of the American army potential, which gave a reason to make the report secret immediately.[61]

Apart from Americans and Europeans, the Chinese also appreciated the advantages of OSINT and opened in 1958 the Chinese Institute of Scientific and Technical Information – a central institution responsible for coordination of gathering, processing and distribution of foreign materials from open sources. Over a period of eight years they had build a vast scientific and technical information base, including information from more than 50 countries, i.e. 11,000 different foreign publications, 500 000 scientific reports, governmental publications, conference materials and scientific studies, more than 5 million foreign patents and a few million of samples possibly useful for Chinese industry.[62]

The significance of information derived from open sources was appreciated also by the Soviet special services. The FBI learned that after William Fisher was arrested in 1957, the KGB's spy, alias Rudolf Abel. After the analysis of information delivered by him it turned out that it was based mainly on open sources materials – the New York Times and Scientific American, and only few pieces of information were supplemented by the agents' intelligence.[63]

On the Polish ground the example of OSINT usage is the activity of colonel Mieczysław Wyżeł-Śnieżyński, a military attaché in Czechoslovakia. His operational reports to the Division II of the General Staff were based on the analysis of open sources, mainly press and catalogues of Czechoslovak military companies.[64]

---

[59] F. Schaurer, J. Störger, *Guide to the Study…*

[60] U. Ulfkotte, *Pod osłoną mroku. Wielkie wywiady bez tajemnic*, Warszawa 2008, p. 292.

[61] W. Zajączkowski, *Zrozumieć innych. Metoda analityczna w polityce zagranicznej*, Warszawa 2011, p. 14.

[62] W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese industrial espionage: Technology acquisition and military modernization*, London-New York 2013, pp. 19–20.

[63] W. Zajączkowski, *Zrozumieć…* p. 14.

[64] A. Wojciulik, *Rola „białego wywiadu" w działalności służb specjalnych na przestrzeni wieków*,

John L. Hart, the former CIA operational officer, boasting an extensive experience in leading intelligence operations overseas, after analyzing operational documentation of the service admitted that the intelligence officers had learned that giving their superiors a piece of paper with any content is much better than giving nothing.[65] One of the spies, a Soviet officer Peter Popov, learned from his superiors that his intelligence work was so much ineffective because more information could be found in newspapers.[66] In 1983 a Japanese journalist interviewed a KGB officer Stanislav Levchenko, working under cover of a press reporter in Japan, who defected to the US in 1979. During more than 20 hours talk that former officer was describing the corridors of operational work. Based on these talks there was a book written and many press conferences with Levchenko took place. According to one American intelligence officer they revealed more information than his CIA dossier had contained.[67]

At present the Arab Spring is a clear evidence that publicly available information, views and assessments published online are a powerful tool with a potential to influence the fate of the country and the society.

Christopher Sartinsky, the former deputy CIA director said, "After years secretly monitoring the public, we were astounded so many people would willingly publicize where they live, religious and political views, alphabetize their personal friends, e-mail addresses, phone numbers and hundreds of photos of themselves".[68] Eben Moglen, a network activist, in his interview „Who Needs the KGB when we have Facebook?" asks rhetorically: Who needs Lubyanka when you have Facebook? referencing the infamous KGB offices in Moscow. "In the old world they would put people into cells to try and find out information about someone. It was expensive, cruel and awful. Nowadays it is much cheaper and easier. You can spy on your friends a little bit, get spied-on a lot. If today every kid is a little spy and there is one supervising spy, who is the winner and who is the loser"?[69]

It looks the same today, to meet the current challenges, analysts of the American Open Source Centre, called nosey librarians, apart from monitoring media, read every day even 5 million posts on the social media and prepare reports on current social environments in chosen countries and draw up certain threats forecasts.[70]

---

in: W. Filipowski, W. Mądrzejowski (ed.), *Biały wywiad. Otwarte źródła informacji – wokół teorii i praktyki*, Warszawa 2012, p. 48.

[65] J.L. Hart, *Walka Wywiadów, Rosjanie w CIA*, Warszawa 2003, p. 58.

[66] Ibidem, p. 52.

[67] S.C. Mercado, *A Venerable Sailing the Sea of OSINT in the Information Age - A Venerable Source in a New Era*, Studies in Intelligence vol. 48, no. 3, p. 51, on the basis of Levchenko's book, *On the Wrong Side: My Life in the KGB*, Washington: Pergamon-Brassey's, 1988.

[68] J. Ortega Sim, *Facebook The Social Filter of World Intelligence*, 2 July 2012, http://thedailyjournalist.com/theinvestigative/facebook-the-social-filter-of-world-intelligence/ [access: 2 V 2018].

[69] A. Schechter, *Who Needs the KGB when we have Facebook? An Interview with Eben Moglen*, April 8 2015, http://moglen.law.columbia.edu/publications/Who-needs-KGB-when-we-have-Facebook Schechter.pdf [access: 1 V 2018].

[70] D. Goodin, *CIA 'Open Source Center' monitors Facebook, Twitter*, November 4, 2011, http://

The British Government Communication Headquarters keeps up with this trend thanks to the Network Analysis Centre, which collects more than 50 billion of records every day regarding Internet users and their entries to information pages and radio online all over the world, mostly linked to Islam.[71] The Director of the German Federal Office for Constitution Protection (BfV), Hans-Georg Maassen stresses that the Chinese intelligence services use social networks, like LinkedIn, to get access to German governmental agencies by establishing professional and businesslike contacts.[72] An effective use of social media show for example the activities of the Israeli Shin Bet. By analysis and monitoring the Instant Messengers it managed to thwart the alleged terrorist attacks on International Conference Centre in Jerusalem and on the USA Embassy in Tel Aviv.[73] European special services have also some successes in this area. The French DCRI (Direction Centrale du Renseignement Intérieur, DCRI and since May 12, 2014 Direction Générale de la Sécurité Intérieure (DGSI) stopped in 2013 Romain Letellier *alias* Abu Siyad Al-Normandy, a French convert, moderator of Ansar Al-Haqq, a jihad Internet forum. He was charged with inciting to terrorism and spreading terrorist propaganda. was the first French jihadist sentenced under the new legal regulation of 2012, the aim of which was to stop self radicalisation via Internet.

Mohammed Emwazi, known as Jihadi John drew the attention of the media and special services because of his role as the assassin of the Islamic State's hostages. He was identified while shopping online. Entering the personal code, he was using ever since the time he was a student, he enabled the services to establish his identity and a place of stay in Syria.[74] Monitoring of a digital trace in the net makes it possible to get to its source – the user. Paul Moore assesses that the pauses the user takes between pressing individual computer buttons or the length of time they are being pressed make up constant and unique values, specifying a man's behavioural trait. Based on such observation and analysis one can assess a profile of a specific PC user. The same methods were allegedly used by the British intelligence service during the World War II. Based on the interception of the individual speech pattern, speed and unique errors made by German telegraph operators, their relevant profiles were successively generated.[75]

---

www.theregister.co.uk/2011/11/04/cia_open_source_center [access: 7 V 2018].

[71] See. Broadcast/Internet Radio Exploitation and Analysis, 6 November 2009 – UK TOP SECRET/ COMINT, https://theintercept.com/document/2015/09/25/broadcast-analysis/ [access: 10 IV 2018].

[72] K. Grieshaber, *German intelligence warns of increased Chinese cyber spying*, December 10, 2017, https://www.seattletimes.com/business/german-intelligence-warns-of-increased-chinese-cyberspying [access: 2 V 2018].

[73] M. Peck, *Israel Thwarts Al Qaeda Plot to Blow Up U.S. Embassy*, January 20, 2014, https:// www.forbes.com/sites/michaelpeck/2014/01/22/israel-thwarts-al-qaeda-plot-to-blow-up-u-s-embassy/1 [access: 2 V 2018].

[74] J. Murray, *Jihadi John exposed by web error: Killer downloaded software using student ID*, March 1, 2015, http://www.express.co.uk/news/uk/561135/Jihadi-John-Mohammed-Emwazi-identified-web-error-student-ID-Westminster-university [access: 26 III 2018].

[75] See. P. Moore, *Behavioral Profiling: The password you can't change*, July 28, 2015, https://

The work of literature customarily widens the horizons and imagination but it can also inspire in an unfavourable manner. The scenario which could be created for the worldwide cinema audience can become a reality as the 9/11 events show how. The hijacking of an aircraft and suicide attack on the American Congress, the Capitol building was described in the book by Tom Clancy "Executive Orders" written 5 years earlier. Timothy McVeigh, who was sentenced for a bomb attack in the governmental building in Oklahoma City in 1995, was inspired by *Red Dawn* movie of 1984 and the book *The Turner diaries* by Andrew Macdonald, member of the American Nazi Party.

Published in *The Washington Post* and in the *The New York Times* the so called Kaczynski's manifesto on the potential threats arising from modern technologies was the reason of TJK's detention by the FBI in 1996. The American terrorist, Theodor John Kaczynski, also known as the Unabomber killed 3 people, and injured 23 using self-made bombs. His brother David recognized Theodor's views included in the published manifesto and tipped off the American services contributing thus to the completion of the investigation which proved ineffective until that very moment.

The metadata, i.e. the details of the data facilitating the identification and description of a digital object constitute an additional source of open information. It can retain, among others, the information on circumstances and location of the task performed and information on copyrights. The metadata of a picture posted on the Instagram by a Russian soldier in a military transporter revealed his place of stay in Ukraine. It was the time when Russia denied its presence in the eastern part of this country. The publication on Twitter of a picture of an IS terrorist featuring one of the command centres in the background allowed the American air forces to locate the place and to bomb it within 24 hours since the picture came out.[76] It is commonly known that there are some applications which enable precise recording of the routes taken by athletes thanks to a geolocation. Their activity along with the distance covered is reflected on a map, which they share eagerly afterwards in the social media. The example of the Strava application shows that the analysis of metadata from available joggers routes disclosed a secret military facilities location, including special services, the joggers served.

The terrorist organizations appreciate OSINT potential[77], particularly in

paul.reviews/behavioral-profiling-the-password-you-cant-change/ [access: 8 IV 2018].

[76] W. Castillo, Air Force intel uses ISIS 'moron' post to track fighters**,** CNN, 5 June 2015**,** https://edition.cnn.com/2015/06/05/politics/air-force-isis-moron-twitter/index.html [access: 13 IV 2018].

[77] Terrorist organisations used different tools in their social activities. Since the mid 1980s it was broadcast and VHS with preaching, pictures from battlefields and magazines and newspaper reports. In the mid 1990s – web pages created and controlled by prominent activists of the organisation. In the early 2000s – internet fora, and nowadays – social media. See. A.Y. Zelin, R. Borow Fellow, *The State of Global Jihad Online*, Washington Institute for Near East Policy, January 2013.

the recruitment process[78], radicalisation, training, planning, attacks[79] or cyber attacks.[80] The Al Qaeda manual assesses that public and open sources allow to gather at least 80% of information on the enemy.[81] Peter Bergan came to a conclusion that fighting with Al Qaeda and its affiliates is in fact the first war of open sources.[82] Up to this day no other terrorist organisation has used social media to the extent the Islamic State did. The FBI Director, James Comey, assesses that members of the organisation perfected the Internet[83] and revolutionised terrorism phenomenon.[84] They created the so called Open Source Jihad[85], i.e. widely accessible and easy to find pieces of information connected to terrorist activities. These intensive efforts of Islamic extremists were also noticed by the German Federal Intelligence Service (BND), according to which Al Qaeda and the IS waged a propaganda war on the Internet on an scale unprecedented. In some analyses emphasise that even 90% of the content created by terrorists on the web is spread via social media.[86] The Internet abounds in free books[87], like manuals and instructions for the potential attackers, lonely wolfs.

---

[78] Elizabeth Kendall assesses that poetry can be a significant tool in the recruitment process because it touches emotions of Arab listeners and readers, creating the climate of tradition, authenticity and legitimacy based on ideology. Osama bin Laden himself wrote the ode, in which he praised damaging the USS Cole by Al Qaeda in 2000.

[79] As the first order for terrorists on the Internet is regarded a statement by one of the Al Qaeda members, Abu Muhammad al-Hilali of 25 October 2005, who called for attacks in Sinai. Although already in 1995 arrested back then Hamas activist, Abd-al-Rahman Zaydan contacted with members of the organization on the web. See. K. Soo-Hoo, S. Goldman, L. Greenberg, *Information Technology and the Terrorist Threat*, „Survival" 1997, no. 3, p. 139.

[80] Open sources are a tool enabling publicity of the so called Media terror, which is or not a form of praising or disdain for terrorist acts, always brings a desired effect and fits into a scenario of terrorists strategy. Apart from that open sources allow to conduct psychological, disinformation operations, propaganda campaigns on the Internet.

[81] See. *Al Qaeda Training manual*, December 2001. It was mentioned by the US State Secretary Donald Rumsfeld in his speech of 15 January 2003.

[82] P. Bergen, *Why U.S. can't find Osama bin Laden*… .

[83] A British of Pakistani origin, Babar Ahmad, is regarded as the father of an online jihad. As a 22-year old student of London University he started the first web site for Islamic extremists in 1996. It was dedicated to Osama bin Laden and one of the Al Qaeda founders Abdullah Azzam.

[84] J. Ax, *No evidence California attackers were part of terrorist cell – FBI head*, December 16, 2015, https://in.reuters.com/article/usa-security-idINKBN0TZ29G20151216 [access: 17 IV 2018].

[85] Analysis of terrorist activities in the social media done by the British International Center for the Study of radicalization (ICSR) points out that they are used for informing (reporting) about current situation (online) on a battle field.

[86] See. D. Bieda, E. Riddle, *Cyberspace: A Venue for Terrorism*, „*Issues in Information Systems" 2015*, no. 16, International Association of Computer Investigative Specialists (IACIS), Leesburg 2015.

[87] See. *The Terrorist's Handbook*, *The Anarchist Cookbook* – manual describing how to make explosives using domestic chemicals. *Military Studies in the Jihad Against the Tyrants, How to survive in the west – analyses of organizing and carrying out military actions according to the jihadist military idea. The Mujahedeen Poisons Handbook – procedures of producing toxins***,** *Safety and Security guidelines for Lone Wolf Mujahedeen and small cells* – information on encrypting on the web, intelligence and counterintelligence methods of creating secret cells of jihad.

The American intelligence informed that Osama bin Laden had a computer centre in the Afghan mountains, from which he established a contact with Al Qaeda members via chatrooms and discussion groups.[88] The Internet must have been a tool to agree the details of and coordination of 9/11 attacks. After Abu Zubaydah, purportedly the operational chief of Al Qaeda, was arrested in March 2002, there were almost2,300 encrypted files from one of the Islamic net page found in his notebook. The analysis of data showed that the information was systematically exchanged between members of the group between May 2000 and September 9, 2011 and a frequency increased a month before the attack.[89] A Saudi terrorist recognized the significance of the media as well. In 2002 in a letter to a Talib leader, Mullah Muhammad Omar he wrote that it was obvious that in the century the fight via media is one of the strongest methods and in fact it could make up 90% of preparations for fighting. While preparing the Mumbai attacks in November 2008, terrorists used the Google Earth search engine to memorise the topography of the city, the names of the streets and the location of the landmarks. In 2009 in Pakistan a group of men from Washington, called later the "Virginia Five" was detained, who intended to join the jihadists on the border with Afghanistan. The undertaking was inspired by a Talib recruit, who had come across favourable to Talibs comments posted by one of the men on YouTube regarding the footage showing an attack on the American troops. The social ineptness experienced by some people, often, generated by social or cultural factors proves easier to overcome in the virtual reality. The online activity of the Dutch Muslim women did not go unnoticed by terrorist groups, which started to recruit those women as translators, programmers and designers of Dutch web pages concerning the jihad.[90]

A certain synergy between open source intelligence and terrorists can be observed.[91] Already in 1976 Walter Laquer gave his opinion in the Harpers magazine that media are terrorists' best friend and an act of terror does not mean a thing without the media coverage. It is the media that provide them with air, they need so much, as Margaret Thatcher used to say more than 30 years ago. As rightly described it Ted Kepel without television terrorism resembles a tree in the middle of a forest: if it tumbles down nobody notices it.[92] One could almost say that it is media that created terrorists making celebrities out of them. It is proved by the fact that during a 10 week time following the 9/11 the Times magazine placed on its cover the image of bin Laden three times compared to the image of the then president George W. Bush occurring only twice.

---

[88] D.E. Denning, *Activism, Hactivism and Cyber Terrorism: The Internet as a Tool for Influencing Foreign Policy*, in: *Networks and Netwars: The Future of Terror, Crime, and Militancy*, Santa Monica 2001, p. 259.

[89] J. Kelly, Militants wire Web with links to jihad, „USA Today" 10 July, 2002, http://usatoday30.usatoday.com/news/world/2002/07/10/web-terror-cover.htm [access: 20 IV 2018].

[90] *Jihadists and the Internet. 2009 update*, National Coordinator for Counterterrorism (NCTb) May 2010, pp. 65–66.

[91] According to the United States Institute of Peace report in 1998 only one in three terrorist organization had its own web page, and in 2000 almost all of them did.

[92] P. Rees, *Kolacja z terrorystą. Spotkania z najbardziej poszukiwanymi bojownikami na świecie*, Kraków 2008, p. 27.

The way the open source intelligence can be exploited showed a British blogger, Eliot Higgis, who drew astonishing conclusions after tracing down the activities in the web. Having analyzed the footage of the British journalist, James Foley execution by the Islamic State he managed to indicate the place of the execution – the hills south off the Syrian city of Ar-Rakka, although some wilderness was in the background.[93] When in August 2013 some missiles fell down on the Syrian cities, and the UN inspectors had difficulties in confirming or denying the use of chemical weapon, Higgins published on the same day some photographs and films found in YouTube showing that the missiles had not exploded immediately but kept falling down intact, releasing slowly sarin out of the heads. One could check social media to easily find huge amount of pictures from the eastern Ukraine with the BUK missiles in the background, posted online by the soldiers of the 53 Anti-Aircraft Missile Brigade from the Kursk Oblast, demonstrating clearly that the separatist groups had regularly backed military forces of the Russian Federation. At the same time Higgins proved that the Malaysia Airlines aircraft was shot down over Ukraine by the BUK missile[94], which belonged to the Russian troops.

To prove that the ostensibly innocent open sources may hide a potent message of top secret weight we can quote an example of a total foul-up made by an a FBI agent, the former chief of an antiterrorist unit. In 2010 he chose to reserve the copyrights to a manual designed for agents interrogating suspects, however, he failed to realize that once the entry was made into the register it became automatically, universally available to anyone interested. In order to register the manual he submitted with the patent office a copy of the manual, which can be accessed by anyone who wants to read it at the Library of Congress.[95] This error, though deemed unwilful in terms of classified information protection, does not bear much difference to the leaks perpetrated by Edward Snowden; in this case the classified information was disclosed to unauthorized persons. It appears that the weakest link in the chain of securing information against the unauthorized disclosure is not a technical security but a human factor. To give an example,the White House exposed their agent in Afghanistan who, due to the position held, was in possession of knowledge, the disclosure of which could pose a threat to the national security of the US and its allies. The name and position of the Chief of Station (Chief of the CIA Station) appeared on the list forwarded to journalists because of the President Barack Obama's visit to the Bagram Base in Afghanistan. The information was transferred immediately on a Twitter and was loudly commented there.[96]

---

[93] J. Ensor, *Is this where James Foley was beheaded?* August 24, 2014, http://www.telegraph.co.uk/news/worldnews/middleeast/syria/11053544/Is-this-where-James-Foley-was-beheaded.html [access:4 VIII 2017].

[94] The lost digit – Buk 3x2 A bell¿ngcat Investigation, s. 2. https://www.bellingcat.com/wp-content/uploads/2016/05/The-lost-digit-BUK-3x2_EN_final-1.pdf [access: 1 VIII 2017].

[95] See. J. Baumann, *You'll Never Guess Where This FBI Agent Left a Secret Interrogation Manual*, December 20, 2013, http://www.motherjones.com/politics/2013/12/fbi-copyrighted-interrogation-manual-unredacted-secrets/ [access: 1 V 2018].

[96] G. Miller, *White House to investigate inadvertent naming of CIA officer*, May 27, 2014, http://www.washingtonpost.com/world/national-security/white-house-to-investigate-inadvertent-naming-

Even those who are aware of the value of OSINT in the intelligence work hold accounts on social portals and their identification, despite numerous attempts to hide, is not difficult, it requires only time and determination. That was also the case of the FBI Director James Comey, whose accounts on Twitter and Instagram were quickly disclosed after he publicly admitted that he had such accounts. A journalist Ashley Feinberg started first to look for accounts of his family members, which – as she rightly assumed – were easier to find. His son Brian, a player of a university basketball team happened to be her first target. Among the tweets of his team she found links to Brian's account and his photograph with a link to the same photo on Instagram, which appeared to be blocked. Using false account she asked for liking it on Instagram. The portal automatically offered further accounts of the people she might have known. Among them the journalist found some relatives of the FBI Director, including his wife Patrice Comby/Failor and a mysterious Reinhold Niebuhr, who had only a few friends on his account. After further research and analysis on the web Feinberg established that during his studies Comey wrote a thesis on a theologian called Reinhold Niebur which made her confident that she managed to identify Comey's account. Next, using the nickname „Reinhold Niebuhr" she browsed in some other accounts on Twitter and found out that the one nicknamed: projectexile7 referred to a project Comey was working on in his previous job.[97]

To conclude deliberations on the OSINT and its added value advantages to intelligence activities, the author would like to point out that as a result of rapid technological progress and continuous development of computer infrastructure the open sources of information, in particular these of virtual nature tend to impact the global reality to an ever increasing extent. The Americans noticed this trend and in response launched in 2011 the Open Source Indicators project within the DNI Office, responsible for research and studies of projects in the field of intelligence. Activities in publicly accessible and available open sources are being monitored. It enables to combine joint indicators in the web, forecast – and intercept early - significant social occurrences which may potentially entail some risks.

The Director of the National Intelligence, James R. Clapper, at a meeting of the Senate intelligence committee in 2016, assessing global threats pointed out that in their intelligence activities, apart from using the OSINT, special services may start using Internet of Things (IoT), i.e. monitor and derive information from the Internet-connected devices. Robert Steele went on further in his deliberations claiming that the services in the 20th century will most likely focus on each and every source available – the so called Open Source Everythings, which probably can get small scraps of information, giving some footholds, answering questions that are

of-cia-officer/2014/05/27/5d5f41f0-e5e6-11e3-afc6-a1dd9407abcf_story.html [access: 4 IV 2018].

[97] A. Feinberg, *This Is Almost Certainly James Comey's Twitter Account*, 30 III 2017, https://gizmodo.com/this-is-almost-certainly-james-comey-s-twitter-account-1793843641 [access: 10 IV 2018].

the foundation of an analysis as Arthur S. Hulnick[98] claimed. It is worth mentioning that it is, or, to say the least, it should be a priority tool at the disposal of the intelligence activities at each stage of the proceedings conducted, allowing their verification and more insightful perception of the phenomenon under examination.

Abstract

The article is devoted to the nature, function and value of open source information in the context of intelligence activities. Analysis of selected examples of the use publicly available information show that over time, they are a tangible complement to the knowledge acquired through other methods known as classified. The author concludes that obtaining these desirable information is more and more difficult nowadays due to the amount of information that grows with each individual unit of time. The exponential rise of multi-source information causes an overload of analytical capabilities and information chaos, which requires additional verification and evaluation of their reliability. It appears advisable to say that due to its nature, taking into account the challenges of today, information is a "weapon of mass destruction", which can be used in two ways: as a tool of disinformation against the enemy, or in case of positive verification may contribute to the anticipative action giving the advantage in a security environment.

Keywords: Information, OSINT, open sources, open source intelligence, intelligence activity.

[98] A.S. Hulnick, *The Downside of Open Source Intelligence*, „International Journal of Intelligence and Counter Intelligence: 2002–2003, no. 4, p. 565.

Piotr Karasek

Social Media Intelligence as a tool for immigration and national security purposes[1]

Introduction

Detecting and interdicting terrorist attacks as well as maintaining proper border security are among the key issues in current public security debate, and the role of social media in achieving these goals could still be increased. While countering terrorism is a responsibility of relevant national law enforcement agencies, all possible fronts of threat detection should be used. This is especially important after recognizing that contemporary extremists often act on their own and are not a part of any terrorist organization, therefore the threat may be very difficult to detect using traditional means of protection. From this perspective, public servants who process visa applications may play an important role in a multi-agency approach to maintaining security. With access to verifiable personal data provided by visa applicants and open source information they may be able to use Social Media Intelligence techniques to detect threats and deny individuals entry whenever it is appropriate. Moreover, using such techniques may allow revealing other information relevant to immigration procedures. Such tools are known to have already been employed in the US immigration procedures.[2] While the actual effects of such policies are difficult if not impossible to determine at current point, there are some clear shortcomings of SOCMINT tools one needs to remember about. This paper based on literature review, available case studies, and research interviews with immigration security practitioners aims to explore the possibilities associated with the use of Social Media Intelligence in the field of national security and immigration, and to describe the risks behind it.

Law enforcement, terrorism, and the Internet

The vast possibilities offered by rapid development of the Internet are often perceived as enabling criminal activity, including terrorism, which is not necessarily the whole truth. Limited anonymity, decentralised black markets, dark web forums, and access to all sorts of dangerous content – all this and more come along with the Internet access and indeed help the criminals achieve their goals. On the other hand, the Internet may

[1] The article was prepared within the FP7 PRIME Project that has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no 608354.

[2] B. O'Brien, *U.S. visa applicants to be asked for social media history: State Department*, Reuters 30 March 2018, online: https://www.reuters.com/article/us-usa-immigration-visa/u-s-visa-applicants-to-be-asked-for-social-media-history-state-department-idUSKBN1H611P, [access: 15 IV 2018].

also be very useful for the purposes of regular crime and terrorism prevention as it increases law enforcement intelligence gathering possibilities, potentially benefiting the governments and counterterrorists more than terrorists.[3]

Intelligence practitioners and academics are often referring to social Media Intelligence (SOCMINT) as a new type of intelligence falling into the general Open Source Intelligence category (OSINT)[4], yet specific uses of SOCMINT still remain mostly an unexplored topic. Social media themselves, regardless of their specific definition[5], have become a global phenomenon and contain a tremendous amount of freely uploaded, often easily accessible information about individuals. SOCMINT efficiency is partially based on the fact that while users express themselves, they often give up information they would not want to share when asked directly[6] (especially if asked by the law enforcement). In contrast to subject-specific online forums, social media are designed to allow free expression of lifestyle. Such design actively encourages users to share their thoughts, plans, opinions, photographs, and facts from their lives online. There is and observable tendency among the social media users to 'over-share' private information, which may have dangerous consequences as it makes them vulnerable to various types of crime.[7] On the other hand, it is exactly the 'over-sharing' phenomenon that makes SOCMINT techniques truly effective.

Social media are therefore already one of the obvious sources of intelligence in policing. In criminal investigations, 81% of (American) law enforcement professionals use social media as a tool for information gathering although in almost half the cases (48%)[8] such practice is not encouraged by their superiors. It is important to notice that some information from social media may be accessed freely, without court order or subpoena, even for unregistered users with the use of open source intelligence techniques. Other methods of using social media by law enforcement agencies may include employing powerful SOCMINT tools, e.g. using

[3] D.C. Benson, *Why the Internet is not increasing terrorism,* Security Studies, 23/2(2014), p. 308, 311, 328.

[4] A.N. Liaropoulos, *The challenge of social media for the Intelligence community*, Journal of Mediterranean and Balkan Intelligence, vol. 1 no. 1 (2013), p. 6.

[5] Popularly social media are defined as 'a group of Internet based applications that build on the ideological and technological foundations of Web 2.0 and allow the creation and exchange of user generated content', where the Internet sites are used 'only' as infrastructure allowing their users to upload their own content. See: A. Kaplan, M. Haenlein, *Users of the world, Unite!*, Business Horizons, 53/1(2010), p. 61.

[6] C. Arslan, M. Yanuk, *A New Discipline of Intelligence: Social Media,* ICMSS Istambul 2015, pp. 69–70.

[7] K. Paullet, J. Pinchot, *Cybercrime: the unintentional effects of oversharing information on Facebook*, 2012 Proceedings of the Conference on Information Systems Applied Research, New Orleans 2012, pp. 1–7.

[8] LexisNexis, *Social media use in law enforcement: crime prevention and investigative activities continua to driver usage*, November 2014, online: https://www.lexisnexis.com/risk/downloads/whitepaper/2014-social-media-use-in-law-enforcement.pdf, [access: 15 IV 2018].

'geofencing' technology[9] (such as 'Geofeedia') allowing to locate and manage near real-time threats.[10]

All the methods used to fight 'regular' crime are also very useful in countering terrorism, with particular emphasis on so-called 'Internet monitoring', a category that SOCMINT fall into. As the European Commission FP7 PRIME[11] research project findings show, methods applied by law enforcement to counter solo terrorism do not really disperse from those used to fight group terrorism or even 'regular' and organized crime.[12] As a result of the interviews and questionnaires collected from European, American and Indian practitioners, a hierarchy chart of the most effective and least costly methods of countering terrorism has been compiled.[13] 'Internet monitoring' has been identified as the most effective and least expensive method (94% of responses).

In the context of Internet and social media monitoring, it is important to understand the nature of modern lone actor (or 'lone wolf') terrorists and how they express themselves through social media. While presenting a strict definition of a 'lone actor' terrorist is still problematic in the field of criminology, they are described as individuals who have no formal ties to any terrorist organisation, but who commit an act of violence inspired by an extremist ideology. An archetypical 'lone wolf' follows a path of radicalisation, attack preparation, and attack phases, without any external help. However, lone actor terrorists may (not necessarily consciously) somehow communicate their intent weeks, days or even hours before the attack. A previous research claim that as many as 76% of the post 9/11 lone wolf terrorists in the US have broadcasted their intent (often more than once) using e-mails, text messages, and more importantly – Facebook postings and Twitter feeds.[14] Even when not communicating their intent to attack directly, future perpetrators often reveal signs of radicalization. Much too often it remains undetected prior to the attack.[15]

Social media and the immigration procedures

Taking into account the abovementioned possibilities arising from the use of open source intelligence in regular crime and terrorism prevention, it is worth considering how it may be employed for the purposes of immigration procedures. Or conversely:

[9] M.D. Dabhi, *Geofencing: a generic approach to Real time location based tracking system*, International Journal of Computer Networks and Wireless Communications, vol. 6 no. 6/2016, pp. 35–37.

[10] K. Cooke, *US Police used Facebook, Twitter data to track protesters*, Reuters, Oct 11 2016, online: http://www.reuters.com/article/social-media-data-idUSL4N1CH4J1, [access: 15 IV 2018].

[11] http://www.fp7-prime.eu/home_page.

[12] FP7 PRIME WP7 Deliverable D7.1, *Counter-measures review report,* Restricted access confidential document.

[13] Ibid.

[14] M. Hamm, R. Spaaij, *Lone Wolf Terrorism in America: Using Knowledge of Radicalization Pathways to Forge Prevention Strategies,* February 2015, p. 9.

[15] For example: George Sodini (aka 'the Gym Killer') explained his entire attack plan on his personal blog over many months between 2008 and 2009. See: *Full text of Gym Killer's blog,* online: http://nypost.com/2009/08/05/full-text-of-gym-killers-blog/, [access: 15 IV 2018].

how OSINT and SOCMINT may enhance the role of immigration procedures in safeguarding national security.

The possible role of visa applicant's social media background check is well illustrated by the case of San Bernardino shooting in December 2015. Shortly after the attack some have reported that Tashfeen Malik, the female shooter who has been in the United States on a fiancée visa, posted jihadist propaganda on her Facebook page prior to obtaining the visa.[16] It has to be fully acknowledged that this information turned out not to be entirely true[17], however, it illustrates how such hypothetical situation would be perceived by the general public and what problems may emerge in the future if visa applicants are not vetted correctly.[18]

Contrary to what one may think, performing social media background checks of visa applicants does not necessarily overlap with the tasks of national security agencies. Although intelligence on visa applicants may be delivered to the immigration services by other national agencies (through databases and dedicated sub-agencies such as the Terrorist Screening Center in the U.S.[19] or Schengen Information System in Europe[20]), because of the decentralised nature of modern terrorism it may be not safe enough to rely only on one source of information. Security agencies are good at finding links to terrorist groups or organized crime, but lone radicals may slip through. Moreover, there are numerous of factors that are taken into account when assessing one's visa application, but are not in security or law enforcement agencies field of interest. Applicant's past criminal sentences or serious health problems are good examples, as they usually may be grounds for visa denial, but are not necessarily the type of information gathered by security and law enforcement agencies.

OSINT and SOCMINT techniques may therefore be viewed as a part of a broad identity and security management system embedded into the immigration process framework to achieve at least two goals: (a) to detect individuals who are prone to violent extremism, and (b) to identify other unique circumstances that may be grounds for visa denial. There are, however, some limitations and risks, which must be considered before implementing such tools. OSINT should be used by the immigration

[16] M. Apuzzo, M.S. Schmidt, J. Preston, *U.S. Visa Process Missed San Bernardino Wife's Online Zealotry*, The New York Times, December 12 2015, online: http://www.nytimes.com/2015/12/13/us/san-bernardino-attacks-us-visa-process-tashfeen-maliks-remarks-on-social-media-about-jihad-were-missed.html?_r=0, [access: 15 IV 2018].

[17] R.A. Serrano, *FBI chief: San Bernardino shooters did not publicly promote jihad on social media*, Los Angeles Times, December 16, 2015, online: http://www.latimes.com/nation/la-ln-fbi-san-bernardino-social-media-20151216-story.html, [access: 15 IV 2018].

[18] See also: B. Ross, R. Schwartz, J.G. Meek, J. Margolin, *Secret US Policy blocks agents from looping at social media of visa applicants, former official says*, ABC News, December 14 2015, online: http://abcnews.go.com/US/secret-us-policy-blocks-agents-social-media-visa/story?id=35749325, [access: 15 IV 2018].

[19] See: *Terrorist Screening Center*, online: https://www.fbi.gov/about-us/nsb/tsc/tsc, [access: 15 IV 2018].

[20] See. *Schengen Information System*, online: http://ec.europa.eu/dgs/home-affairs/what-we-do/policies/borders-and-visas/schengen-information-system/index_en.htm, [access: 15 IV 2018].

services in an organized manner, which is not always happening in practice.[21] In the next sections of this article some key areas of this concept are explored. Firstly, it is necessary to specify how a social media background check could be performed in the course of immigration procedure. Secondly, it is equally important to take a hard look at the potential risks and limitations of such method.

Entry data

Searching for potential terrorists on the Internet is like searching for a needle in a haystack. A common problem with SOCMINT techniques is the deluge of information that needs to be processed in order to receive actionable intelligence.[22] Immigration services, however, have an advantage in this regard – they are in possession of reliable and relatively complete set of personal data submitted by applicants themselves on immigration forms. The data may be used as entry data to create a 'data filter' effectively reversing the search process – instead of trying to find worrying content and then trying to identify its author, the search may focus on finding worrying content posted on the Internet by a specific person. It is therefore possible to shift from searching for 'unknown unknown' to a search for 'known unknown', which is relatively more effective and easier to deal with.[23]

Entry data available to the immigration services in each case will vary depending on specific legal regulations. For example: western-European tourists visiting Australia on an e-visitor visa are required to provide their personal data (including full legal name, sex, date of birth, passport number, country of residence), and a working e-mail address. A different example may include an Egyptian applying for a Polish visa, who would have to additionally submit his photograph and other documents or information (such as e.g. official certificate of no criminal record), if requested by the consulate.[24] In case of long-term visas the requirements are usually higher. Typically the initial dataset available for the immigration services and usable for open source research contains at least: applicant's full legal name and date of birth, e-mail address, home address, workplace address, photograph. It is often enough information to identify the person online, provided he or she is not actively trying to hide personal details.

[21] Some Australian immigration service's practitioners, during confidential research interviews, have admitted that although there is no official SOCMINT policy in place, they sometimes use such techniques to check visa applicants out of their own initiative.

[22] D. Omand, J. Bartlett, C. Miller, *Introducing Social Media Intelligence (SOCMINT)*, Intelligence and National Security, n. 1–23(2012), pp. 6–7.

[23] See. N.N. Taleb, *Black Swan. The impact of the highly improbable*, New York 2007, p. 127, 272.

[24] Ministerstwo Spraw Zagranicznych RP, system eKonsulat, online: https://secure.ekonsulat.gov.pl/Uslugi/RejestracjaTerminu.aspx?IDUSLUGI=1&IDPlacowki=157, [access: 15 IV 2018].

Access

After a 'data filter' is compiled, access to relevant online sources must be established. One option is to openly ask the social media service providers for help, but they often do not willingly cooperate with state agencies (especially foreign state agencies). To gain access to user's data directly from social media companies often at least a subpoena or even a proper court order is required.[25] Some companies actively fight for their users privacy[26] or publish 'transparency reports' on law enforcement access demands[27], which, however exemplary it may be from civil rights perspective, has to be seen as an obstacle in the context of national security. It is too early to predict the impact of recent events involving Facebook's data leak[28] on users and companies behaviour, but this issue has definitely raised public concern about data privacy.

Open source background checks, however, do not rely on gaining official access to user's restricted data. The very idea of open source intelligence is based on the fact that a lot of meaningful information is publicly available. This is also true for social media profiles. Of course, users who are conscious of their privacy either do not use social media at all, do not post private information online, or at least set their privacy settings so no third party may access it freely. This, of course, is another obstacle in the context of the proposed method. However, surprisingly high number of social media users has their profiles fully or at least partially visible even for unregistered users.

Data access capabilities may also be enhanced by other means, including simple 'tricks' and elaborate OSINT-gathering systems. Among the most basic methods is the creation of 'false' accounts, so the social media platform recognizes the intelligence gatherer as a 'registered user' and allows more access. Although it is usually against the social media policies[29], this method is often used by law enforcement professionals (even though they are discouraged to do so).[30] Of course, accessing and gathering

[25] See e.g.: Facebook, *Information for law Enforcement Authorities*, online: https://scontentfra31.xx.fbcdn.net/hphotosxfp1/t39.23656/12532957_530107840495531_2074830868_n.pdf, [access: 15 IV 2018]; Twitter *Guidelines for law enforcement*, online: https://support.twitter.com/articles/41949#, [access: 15 IV 2018].

[26] A. Fine, *Twitter appeals ruling in bat tle over occupy Wall Street protester's information*, online: https://www.aclu.org/blog/twitter-appeals-ruling-battle-over-occupy-wall-street-protesters-information?redirect=blog/technology-and-liberty-national-security-free-speech/twitter-appeals-ruling-battle-over-occupy, [access: 15 IV 2018].

[27] See. *Google Transparency Report*, online: https://www.google.com/transparencyreport/userdatarequests/#!, [access: 15 IV 2018].

[28] D. Ingram, *Facebook says data leak hits 87 million sers, widening privacy skandal,* Reuters April 4 2018, online: https://www.reuters.com/article/us-facebook-privacy/facebook-says-data-leak-hits-87-million-users-widening-privacy-scandal-idUSKCN1HB2CM, [access: 15 IV 2018].

[29] All Facebook users should, in theory, use their authentic names, see: *Facebook community standards*, online: https://www.facebook.com/communitystandards, [access: 15 IV 2018].

[30] In an initially confidential guidelines for law enforcement Facebook also discouraged the use of false accounts by law enforcement, see: *Facebook law enforcement guidelines*, 2010, online: https://info.publicintelligence.net/Facebook2010-2.pdf, [access: 15 IV 2018].

information does not have to be performed manually, because of the existence of specialised commercial software designed to collect open source information from the Internet. Such systems are already available to state agencies and may be tailored to their needs and allow a very cost-effective information gathering.[31]

Assessing the information

After defining the initial dataset and establishing access to information, the key phase of any background check is the assessment of the data gathered. The approach to data assessment should depend on what information has been found online about the individual on one hand, and the specific visa and security requirements on the other.

There is a number of common visa requirements (such as 'good health' or 'good character') which may be at least partially verified through open source intelligence, but it is important to know where to look for relevant information. First of all, one should review all the available original content posted by the person checked. Due to the aforementioned 'over-sharing' of private information, online postings might reveal information, which may be grounds for visa denial. For example, visa applicants are usually expected to state that they have no criminal record and are not subject to any current criminal investigation, which may sometimes be proven untrue after a careful search of their Internet postings indicating past or present legal problems. There have been also many cases in which a photograph posted online was found by the law enforcement, which has led to a criminal investigation.[32] There is no reason not to use the same information gathering technique in the immigration process.

Apart from the original content posted online, it is also important to review one's 'shared' posts, 'liked' pages, 'followed' users, and joined 'groups' (on Facebook, Twitter and other micro-blogging platforms and social media – the specific terminology about 'sharing', 'liking', 'following' etc. may vary) which may indicate personal views, interests, and life situations which may lead to a visa denial. This may be important especially when looking for signs of radicalisation; someone 'following' accounts known to be posting terrorist propaganda[33] is an obvious cause to concern.

When making the assessment of the information gathered one should also know how to judge less 'obviously worrying' content. This has been already explored in previous research and a set of 'warning behaviour' signs has been already described.[34]

[31] A couple of major software manufacturers such as Symantec, Oracle, or Wynyard offer such 'intelligence gathering solutions' (terminology and specifications vary, but all these are commercially available for law enforcement agencies).

[32] There are many examples of such behaviour. See. A. Shontell, *7 People who were arrested because of something they wrote on Facebook*, Business Insider 9 Jul 2013, online: http://www.businessinsider.com/people-arrested-for-facebook-posts-2013-7?IR=T, [access: 15 IV 2018].

[33] See. J. Klausen, *Tweeting the Jihad: social media networks of western foreign fighters in Syria and Iraq*, Studies in Conflict and Terrorism, 38(2015), pp. 1–22.

[34] In particular, it is possible to detect some types warning behaviours online, using social media analysis (by detecting linguistic markers for 'leakage', 'fixation', and 'identification' warning

Whether the occurrence of a specific 'warning behaviour' should result in visa denial (or, in some instances, even further action against the individual such as informing the relevant authorities about the threat) should depend on the adopted internal policy.

Risks and obstacles

Using open source information gathered from the social media to assess visa applicants is associated with a handful of serious risks and may encounter various obstacles. Knowing them and having at least a sound plan how to react when such problems occur is an important step in adopting social media background checks as a policy designed to effectively ensure security. Among the most important problems are verifying one's true online identity, language and cultural barriers, organizational issues, legal and ethical concerns, and the problem of final decision-making.

True identification

Although in theory social media users should use their true personal data, in practice it is obviously untrue[35], which is perhaps the most significant problem associated with targeted social media intelligence gathering. An alias may be used for privacy reasons - a premeditated or instinctive decision not to post true personal data online (which, on the other hand, is a good sign of one's caring for security). Some users create fake profiles on purpose, to steal other's identity or to engage in 'cyber-bullying'. Whatever the reason for using an alias is, it limits the possibility of establishing a reliable access to one's online postings. The intelligence gatherer has to be also wary that even when a social media profile is created with a real name and surname, it does not necessarily belong to the person one is trying to review. Names alone do not allow identifying anyone online, as many users may share the same legal name. For example, searching Twitter for this paper's author's name[36] will result in a couple of records, none of which is his, as he not maintain a Twitter account at all.

Unfortunately, there is no ideal method to doubtlessly verify one's online identity without confronting the person in question. Best course of action is to (a) cross-check the data available from the social media profiles with the dataset created on the basis of the visa application, (b) remain suspicious about the users perceived identity, especially when drawing conclusions.

---

behaviours), see. K. Cohen, F. Johansson, L. Kaati, J.C. Mork, *Detecting linguistic markers for radical violence in social media*, Terrorism and Political Violence, 26/1(2014), pp. 246-256, and: J. Reid Meloy, *Identifying warning behaviors of the individual terrorist*, FBI Law Enforcement Bulletin, April 2016, online: http://drreidmeloy.com/wp-content/uploads/2016/05/2016_IndividualTerrorist.pdf, [access: 15 IV 2018].

[35] See. K. Raynes-Goldie, *Aliases, creeping and wall clearing: understanding privacy in the age of Facebook*, First Monday, vol. 15 no. 1–4.

[36] The author has decided to use his own name as an example due to ethical concerns about using other people's data. This experiment, however, may be reproduced with other names easily.

Language and cultural barriers

Language and cultural barriers may be problematic when gathering information especially by the immigration services. Obviously, social media users post their content using many national languages, not always known to immigration officers. These issues may be partially addressed by promoting diversity among immigration workers and employing those with higher language skills. Machine translation is another option as more and more advanced automatic translation services are being developed, which may at least reduce the need for the analyst to be fluent in the original language of the text.[37]

Cultural barriers and lack of knowledge may prohibit some immigration workers from understanding the specific context and true meaning of one's postings. Without the proper knowledge about current trends in extremist ideology and propaganda it may be difficult to pinpoint suspicious Internet activity associated with terrorism. For example, in 2014 ISIS successfully used World Cup themed hashtags (e.g. #Brazil2014) to disseminate its propaganda[38], and anyone posting under such hashtag could be either a genuine sports fan or an ISIS supporter. This problem may be addressed with appropriate training programmes within the immigration services.

Legal and ethical issues

Collecting personal information about foreign individuals, other than willingly provided by themselves on visa application forms, may raise questions about legality and ethics of such process. Information from social media profiles very often will fall into the category of 'personal data', and whether its collection by the immigration services is legally acceptable or not will depend on the specific legal system. For example, such methods would be at least questionable under European law which strongly protect personal data and describes who and when is allowed to process it.[39] Therefore in some jurisdictions minor changes in legislation would be necessary to allow it.

Another option to address this issue is to semi-overtly ask visa applicants for their consent to gather additional personal data, which may allow to move the intelligence gathering process away from the legally and ethically gray area. This is unfortunately associated with the risk of alarming those who may try to remove or hide relevant information. A general consent form could be included in the visa application documents,

[37] K. Cohen, F. Johansson, L. Kaati, J.C. Mork, *Detecting*, op. cit., p. 251.

[38] C. Milmo, *Iraq crisis exclusive: Isis jihadists using World Cup and Premier League hashtags to promote extremist propaganda on Twitter*¸ The Independant 22 June 2014, online: http://www.independent.co.uk/news/world/middle-east/iraq-crisis-exclusive-isis-jihadists-using-world-cup-and-premier-league-hashtags-to-promote-9555167.html, [access: 15 IV 2018].

[39] See the newest EU personal data protection act, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

and it does not have to disclose exactly what information and how will be gathered by the immigration services. More specifically, visa applicants may consent to 'a search for relevant information from other sources accessible to the immigration services', which should cover all the SOCMINT gathering techniques without sounding too alarming. Similar consent forms are known to exist both in the public and private sector, where employees agree to background searches.[40] Too vague consent form may, however, still be not enough to assure the legality of the discussed methods in some jurisdictions, especially when sensitive information (such as information about one's health and personal views) is to be gathered.

Decision-making

Whenever suspicious social media content is found, it is essential to take into account all the limitations of SOCMINT techniques to exclude any misunderstandings. A questionable social media posting may be misunderstood, falsely attributed to a specific person, simply untrue or even published as a jest. Posts meant to be humorous were known in the past to cause people problems on the international border. Such was the case of Leigh Van Bryan and Emily Bunting - a couple of British tourists who 'tweeted' that they were going to 'destroy America'. Although what they meant by that statement was merely 'heavy partying', the context of the post was not taken into account and the couple was denied entry to the United States.[41] In another example: someone who applied for a one-week tourist visa, but posted online 'farewell message' indicating several months of planned absence may want to overstay his or her visa, but might as well be planning to visit many countries in that time or switch visa classes (e.g. due to a genuinely planned marriage).[42]

It is essentially true that the success of intelligence gathering is not the information itself, but the value it adds to decision-making.[43] Therefore the most important part is the evaluation of the data gathered and the resulting decision-making, which should ensure the legitimacy and integrity of the visa granting process. Creation of a sound internal policy in this respect is highly advised, so no immigration officer is left alone with the decision about how to react in specific cases. It is essential to define internal rules of conduct in SOCMINT gathering, containing specific guidelines on how and when to react, what content should be flagged for further investigation, how to cross-check information, when to ask for additional documents, or personally confront the individual about their social media postings in questionable cases before making a final decision.

[40] See e.g. background check consent form for candidates for public office positions required in Canada, online: http://www.fja-cmf.gc.ca/appointments-nominations/forms-formulaires/bc-va/bc-va.pdf, [access: 15 IV 2018].

[41] R. Hartley-Parkinson, *'I'm going to destroy America and dig up Marilyn Monroe': British pair arrested in the US on terror charges over Twitter jokes*, Daily Mail 31 January 2012, online: http://www.dailymail.co.uk/news/article-2093796/Emily-Bunting-Leigh-Van-Bryan-UK-tourists-arrested-destroy-America-Twitter-jokes.html, [access: 15 IV 2018].

[42] Such case has been presented to the author during an anonymous research interview with an Australian government agency representative.

[43] D. Omand, J. Bartlett, C. Miller, *Introducing…*, op. cit., p. 7.

Conclusions and recommendations

SOCMINT use opens many possibilities for all types of state and private entities (including those involved in terrorist or criminal activity). Applying SOCMINT techniques in the immigration procedures may serve to gain an additional layer of security against terrorism threats as well as to help check applicant's visa eligibility better than before. Its use in the field of national security is therefore highly recommended. Immigration services are in perfect position to create appropriate 'data filters' using real personal data, which is an essential asset in terms of open source intelligence gathering. However, such use of personal data may require validation through at least vague background check consent form – depending on the specific conditions of the legal system.

Assessing one's social media postings may reveal threats to national security or other grounds for visa denial, but because of the potential problems with online identity verification and context-sensitive content it must be done with extreme care and with an 'innocent until proven guilty' mindset. Taking all the possible benefits and risks associated with SOCMINT use, it is highly advisable to develop an internal agency-wide policy concerning social media background checks. To conserve resources and minimise the risks, appropriate SOCMINT policy should cover such issues as: when to perform background checks (should all visa applicants be checked or just some groups, e.g. first-time visitors?), what tools should be used to gather information (will a SOCMINT gathering software be purchased?), where to look for information, how to cross-check findings and verify perceived online identity (should visa applicants be confronted with the suspicious content found on the social media profiles?), and how to assess various findings when it comes to the point of decision making. Creation of such policy should be followed with appropriate specialist training given to those who are to use it.

Abstract

Internet monitoring and open source intelligence techniques are becoming an important part of terrorism detection and prevention system. The abundance of personal information in the social media is currently used not only to detect terrorist activities but in 'regular' policing as well. The article explores the possibilities of the use of the so-called Social Media Intelligence (SOCMINT) in immigration procedures. Immigration services have unique capability to screen visa applicants in the context of their Internet postings. Such activity may allow to detect serious threats to national security, as well as verify visa eligibility in a more effective manner. However, SOCMINT techniques have their shortcomings which should be addressed in an appropriate internal policy governing their use.

Keywords: terrorism, immigration, OSINT, SOCMINT, social media

Marek Świerczek

The "Matryoshka System"[1], or the perfect disinformation. Introduction to the topic

Preface

In order to understand the principles on which the Russian system of disinformation is based, one must precisely define this phenomenon. Recently the disinformation concept has taken on an extremely wide meaning. However, borders of the term definition are vague and above all, they have practical consequences in the form of "detecting" by homegrown investigators of Russian conspiracies ever new manifestations of "disinformation evil", most often understood as any information activity aimed at influencing the people attitudes. In this way, the disinformation means both propaganda (in all its variants, including propaganda that is openly made by Russian state media), as well as so-called *fake news,* that are constantly detected and analyzed as a very serious risk to the security of the state, although as yet there are no convincing studies indicating the long-term effectiveness of using them.

Bu the main result of expanding the meaning of the notion of disinformation is shifting attention from an extremely dangerous phenomenon to phenomena of marginal importance. Figuratively speaking: a real disinformation drowns in the cacophony of media reports about the fake messages and manifestations of brazen propaganda of the Kremlin, which makes the actual disinformation, devoid of protective measures on the part of counter-intelligence, become even more harmful. It is therefore necessary first of all to define more precisely the concept of the disinformation phenomenon. In the author's opinion, the following definitions of the phenomenon are representative for most of the works devoted to this problem:

1. (...) an extremely complex method of operational work, by influencing the current or potential opponent state, hostile special service or specific groups or social strata in another, but sometimes also own country. The term was invented by German special services during World War I; at the headquarters of the German army until the end of the war, there was a disinformation unit controlled by the military intelligence service. Later, the special services of other countries introduced this form of action as a methodological method of influencing the opponent, undertaken with the intention of creating a targeted influence on the formation of opinions and the course of foreseeable events. Disinformation is a secret action based on a unified concept consisting

[1] A matryoshka doll (Russian: матрёшка, a diminutive form of Russian female first name "Matryona") – is a set of wooden dolls of decreasing size placed one inside another.

of preparing, developing and, in consequence, transferring to an opponent (its special service) or publicly disseminating, but with hidden goals, in the society of the opponent's country partially or completely false information, documents (letters, publications, manuscripts, etc.), photographs or other forms of false data intended to create a seemingly true picture or opinion and shape an opinion about a person, event or phenomenon in accordance with the operational interests of a special service undertaking disinformation and/or political activities of the state, in whose interest the given service implements them, usually for causing direct or indirect damage to the current or future interests of the opponent. The effect of such actions is influencing the decision-making processes of one state by another state (government, parliament, economic organs), which may use such information pieces to make decisions that harm the vital interests of that country.[2]

2. Intentionally false information that should affect a specific group of people or the entire population. This is one of the basic methods of operational intelligence work, serving to influence the behavior of the opponent, to make the oppononent's intelligence service's work easier. (The opponent may be a hostile intelligence or another organization or person against whom the service's activities are directed). Disinformation is divided into strategic, long-term plans and intentions, as well as operational disinformation, which is created depending on the momentary situation. Disinformation in terms of form can be linguistic, pictorial or demonstrative (presentation of physical objects).[3]
3. Creating and spreading the misleading or false information, to distort the opponent's image.[4]
4. Disinformation (...) it is a deliberate dissemination of false data by means and methods of operational work in order to mislead an opponent, to obtain planned results.[5]
5. (...) the essence of disinformation is provocation, not a lie (...) states use their secret services, to create a provocative image, to make the opponent make erroneous judgments.[6]
6. (...) disinformation aims at the implementation of a consistent program aimed at replacing in consciousness, and above all the sub-consciousness of the masses that are the subject of these activities views considered as disadvantageous to them, but beneficial to the disinformator.[7]

---

[2] J. Larecki, *Wielki leksykon służb specjalnych świata: organizacje wywiadu, kontrwywiadu i policji politycznych świata, terminologia profesjonalna i żargon operacyjny*, Warsaw 2007, pp. 159–160.

[3] *Encyklopedia szpiegostwa*, Warszawa 1993, pp. 72–73.

[4] N. Polmar, T.B. Allen, *Księga szpiegów. Encyklopedia szpiegostwa*, Warszawa 2000, p. 151.

[5] H. Lewandowski, *Podstęp, inspiracja i dezinformacja w działalności służb specjalnych*, Warszawa 2000, pp. 81–82.

[6] E.J. Epstein, *Podstęp. Niewidzialna wojna między KGB a CIA*, Krosno 1993, p. 31.

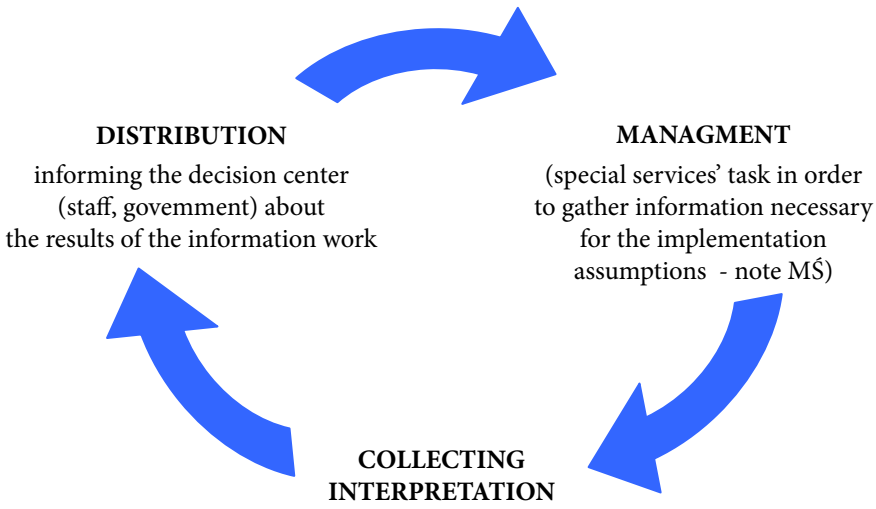
[7] *Dezinformacja – oręż wojny*, V. Volkoff (ed.), Warszawa 1991, p. 8.

7. This term means systematic efforts to spread false information and to falsify or block information about the actual situation and policy of the communist world. As a consequence, disinformation practices were to lead to confusion, misleading and influencing the non-communist world, to undermine its policies and to persuade the opponent from the West to unwittingly contribute to the realization of communism's goals.[8]
8. Disinformation is a special type of "black" propaganda which is supported by false documents.[9]

It can be easily noticed, the above-cited definitions of the concept of disinformation have several elements in common. These include declaring that disinformation is the domain of special services and that it consists of creating a false image of reality in the opponent mind, which is to lead to making erroneous decisions. That requires keeping the process secret, above all, a source of the distorted information, to deprive the victims any possibility of the verification (because then they can not only falsify distorted data, but also - on the principle of *cui bono* – mark out a probable disinformator). In connection with the above, the above-mentioned elements of disinformation disqualify both propaganda and so-called *fake news* (and other forms of information war carried out with the help of the mass media and the Internet) from being disinformation *sensu stricto*, because, although in their case it is difficult to identify the actual source of information, but it is impossible to deprive the victim of the possibility of data verification. Moreover, the thesis that the conduct of the wider form of the information war is the domain of special services, is highly questionable, since the secret services usually do not have the means to carry out the scale propaganda activities.

In order to avoid the logical problems that occur while too wide definition of the concept of disinformation is used, one should start from a simple assumption based on understanding, how - in general terms - decision-making processes in the centers of state power are conducted. The simplest illustration of such a process is the so-called intelligence cycle (presented below), showing the close connection of political and military decisions with information provided by specialized state agencies, including intelligence and counterintelligence services:

[8] A. Golicyn, *Nowe kłamstwa w miejsce starych*, Warszawa 2007, p. 6.
[9] V. Marchetti, J.D. Marks, *The CIA and the Cult of Intelligence*, New York 1974, p. 173.



Scheme: Intelligence cycle showing a close relationship between the politico-military decisions and the information provided by specialized government agencies, including intelligence and counterintelligence.

Source: J. Hughes-Wilson, *Największe błędy wywiadów świata*, Warszawa 2002, p. 13.

Slightly simplifying the above diagram, it should be said (though it borders it with a truism) that the vast majority of governments make politico-military decisions basing on the verified and analyzed information provided by state institutions established for the purpose of collecting, verifying and processing of intelligence and not on the basis of opponent's propaganda, misinformation, mass-media fake news, etc.

Of course, influencing public opinion by disseminating false media reports may in the long run affect the functioning of the state, e.g. by gaining voters support for specific political parties or activates dynamics of large social groups (provoking riots etc.) to what governments must react in some way. However, in general, it must be assumed that in most situations the state centers of mature democracies operate on the basis of the information considered reliable, i.e. from certain sources, such as the state services usually specialized obtaining and analyzing the intelligence. From this point of view, one can therefore - for the purposes of this article - adopt the following definition of disinformation: **disinformation is a process of influencing the behavior of a subject disinformed by distorting its perception of reality, leading the victim of disinformation to undertaking actions consistent with a deformed image, and at the same time corresponding to the interests of the misinforming entity. It is a process planned and carried out by specialized state institutions that have adequate resources to do this and to try to control the any channels used for obtaining information by the disinformed object.**[10]

[10] V. Marchetti, J.D. Marks, *The CIA and the Cult of Intelligence*, New York 1974, p. 173.

The most important for the above definition is understanding that for **conducting of disinformation activities it is necessary to control the channels of obtaining information by the victim of these activities -** in short, it means blocking the victim's activities regarding the reliability checks of information channels. One can not conduct the effective disinformation operation, when the victim can verify the acquired data from other, reliable sources. Therefore, neither *the fake news,* nor fundamentally false or manipulated content or propaganda pronouncements, placed in the media by influence agents or so called resonance boxes can not have a real impact on decision-making processes of any mature state organisms. They can certainly lead to social problems, decision-making uncertainty or information noise, but ultimately, they must make the authorities verify and correct the originally incorrect assessments. Moreover, providing credible information in the media space about such practices of the entity responsible for spreading the untruth, weakens its credibility also in cases where it is the source of real information.[11]

Therefore, if disinformation operations are to be effective, it must as completely as possible cut off the victim from alternative sources of information. If it succeeds, the object of disinformation attack - in accordance with the basic principles of syllogism - having false premises **must** come to false conclusions, even if it applies the most stringent logical procedures.

The best illustration of this disinformation scheme were the actions of the British The XX Committee (i.e. counterintelligence body), which, during the operation known as the *Double Cross System,* in order to deceive the German Abwehr, managed to intercept practically all German spies, put them against the alternative: the cooperation with MI5 or being hanged (which, incidentally, gave practically 100% effectiveness of recruitment) and control the results of their disinformation activities thanks to the effective Enigma decryption.[12] The British counterintelligence, however, had the task facilitated by the geography of the United Kingdom, whose insular position meant that they were able to catch Abwehr agents almost immediately after landing in England.[13]

Continental services, especially of large countries, unable to effectively control not only borders, but also the whole of its own territory, are usually not able to implement this type of action, because it can not prevent an opponent from receiving information from sources not controlled by the counterintelligence. This problem was solved by the Soviet (now Russian) service in the early 1920s, when the Soviets adopted the principle

[11] The Russian Federation ran into a trap like this. After numerous media campaigns recognised as spreading manipulation or false information it could not oppose in no way Western narration also in cases when the accusations against Russians had no substantial basis. Former proved manipulations of the Russian media undermined their credibility, which, in the end, led to serious losses in their information war.

[12] This operations was described by its co-author in: J. Masterman, *Brytyjski system podwójnych agentów 1939–1945*, Warszawa 1973.

[13] Similar situation took place in case of Cuban services which carried out a disinformation operations under the supervision of the KGB against the CIA. The Americans were deceived by double agents for almost 25 years.

of conducting so called offensive counterintelligence, which consisted in **actively** providing to foreign intelligence services with soviet agent as objects of recruitment and through it – disinforming the opponents (so-called *opierativnaja nastupatielnost*).

But the activity of counter-espionage double agents was not enough (for a misled espionage agency was still able to make contact with other sources, searching for some verification), so the Russians (or actually so called *Internacyonaly,* as the Cheka/GPU were created mainly by Poles, Jews and Baltic nationals) came up with a brilliant idea: they offered their victims **a possibility to verification** of the obtained **information.** The core of the idea was the assumption that if you give a victim an apparent choice of sources, even if the victim does not trust one source, would be likely to trust the second one, or the third one and so on. This is the principle extremely similar to the rules used by the commercial television, which, apparently offering multiple channels tailored to specific audiences, in fact, serve only as a source presenting ads, and therefore making money on advertisers.

The Soviet version of running disinformation can be figuratively called "matryoshka system", because any attempt to verify the information through looking for reliable sources always drove to the appearance on the scene of another "matryoshka", that is, the source completely different than the previous one, but offering still the same content, matched to the needs of the recipient.

An excellent illustration of such a model of Soviet service activities was the activity of the OGPU counterintelligence unit against Russian emigration after exposing in April 1927. the supposed monarchist organization MOCR-Trust (in fact the cover-body of OGPU, which since 1921 effectively misled the leadership of "white-immigrant " and Western intelligence).

The following sequence and the OGPU actions should serve as a perfect illustration of the above outlined "matryoshka system".

Case study of the "matryoshka system"

On April 12, 1927 an OGPU agent who was also a member of the management board of the so called MOCR-Trust organization, Eduard Opperput, along with the messenger of General Aleksander Kutiepow Maria Zacharchenko-Shultz crossed the border from the USSR to Finland. Almost immediately after the acquisition of refugees by the Finnish Border Guard and the transfer to the Finnish II Division (intelligence - also bearing the name "Branch II") A. Opperput gave extensive testimony, which showed that the underground organization MOCR-Trust, with which the white-armed organizations and most of the Western intelligence agencies cooperated, was a legend of the OGPU, used to disinform the governments and general staffs of the West. Theoretically speaking, it was the end of the disinformation operation carried out by the Soviets from 1921, because E. Opperput's enunciations have discredited the Trust. However, apart from the fact that the Trust structures in the West remained unchanged,

the Soviets reached for the outlined above "matryoshka system" replaced the Trust with alleged verification alternatives.

Already on April 12, 1927 gen. Aleksandr Kutiepov, the head of Russki Obszczewoinski Sojuz[14], received a letter from an OGPU agent, an alleged member of the Trust's Board, general Nikolai Potapov.[15] In that letter Potapov accused Opperput of being still an OGPU agent (and earlier of VChK)[16] and of (...) *financial machinations* (...) standing behind his escape. At the same time, he gave a lot of information magnifying the information chaos of the enemy (in the OGPU jargon so called *putanica*[17]).

However, the main Potapov's message was the suggestion that part of the organization MOCR-Trust survived and was ready to keep on acting, and the escape of E. Opperput was merely a result of his financial frauds. It was the first consistently implemented *new line of the* OGPU, which was to replace the Trust offering the new hope for the white emigration.

On April 20, 1927, the Soviet news agency TASS provided information re-published a day later in "Izvestiya" and "Pravda" about the breakup of a monarchist group dealing with (...) *military espionage and financial machinations.*[18] At the same time, interestingly enough, both the Parisian "Vozrozhdenie" and the Berlin "Rul" were in the position that this piece of information was not true.[19]

The multiplicity of press reports on the escape of E. Opperput (initiated by the publication from April 24, 1927 in the Helsinki-based "Hufvudsadsbladet"[20]) did not change the attitude of emigration to the leaders of the Trust (in fact - organization of covers for the OGPU) operating in Central and Western Europe. At least so can be assumed after the command of A. Kutiepov to the Trust proxy in Warsaw, Yuri Artamonov, to maintain contact with the Polish Division II (military intelligence) somewhat apart from the Trust board in Moscow.[21] This was surprising, considering

[14] The Russian All-Military Union – an organization that was founded abroad by General Pyotr Wrangel in 1924. Its purpose was provision of aid to the veterans of the Russian White movement, who lived outside the USSR and maintaining a Russian military organisation which emigrated from Crimea in 1920; more: see S.J. Rybas, Генерал Кутепов, Moscow 2010.

[15] The content of the letter in: L. Flejszman, В тисках провокции. Операция Трест и русская, зарубежная печать, Moscow 200, pp. 140–142.

[16] Clearly, E. Opperput used it later to reject allegations from the Savinkov followers as a Soviet disinformation – see: „Siegodnia" of 17 May 1927.

[17] Usually in OGPU activities it was gained due to mixing suggestions with true information. N. Potapow, inter alia, (truthfully) accused E. Opperput of being an agent of the then CheKa; He described drunken escapade of G. Radkiewicz of 5 April 1927, hysterical reactions of his wife and attempt at blackmail by E. Opperput who wanted money for silence.

[18] This information was immediately re-published by the migratory press, inter alia, in „Последних Новостиях" and „Возрождению".

[19] L. Flejszman,.В тисках провокции..., p. 144.

[20] By the way, surnames were written in a wrong way in the text, which suggested that the editorial office could get an oral information or in a form of someone's handwritten note.

[21] S. Wojciechowski, Трест. Воспоминания, Canada 1974, p. 111.

that general A. Kutiepov in conversation with the head of the "East" Division of Branch II, major Michał Talikowski, hinted that the ROWS lost its confidence in the Division II, as the staff and the Polish government should be infiltrated by the OGPU and that therefore ROWS would move the center of its activity to Finland.[22]

On May 18, 1927 Pavel Arapov (OGPU agent) wrote a letter to his uncle general Piotr Vrangel[23], in which he discredited the Trust. He wrote that E. Opperput, contrary to what is said, (...) *was not the only provocateur* (...) that the operation was used to discredit gen. Kutiepov and that the fall of the Trust could only strengthen another structure associated with the Trust - Eurasia.[24] It should be presumed that, where the OGPU figured out that emigration had ceased to believe in the credibility of the Trust structures in the West, it offered so called Trust's *dvoinik* (a copy) in the form of Eurasia. Because gen. P. Vrangel from the beginning the Trust was mistrustful to the Trust and E. Opperput's public pronouncements spoke of provocation of the OGPU to the embarrassment of gen. A. Kutiepov, the OGPU gave him a relative who confirmed the original conviction of P. Vrangel of the Trust as a Soviet provocative organization. Vrangel's kin, P. Arapov, as a Eurasian representative, was a perfectly prepared lure: he conveyed the same opinion as the general's about the Trust's plot and represented Eurasia, which was allegedly uncontaminated by Soviet infiltration (as opposed to the MOCR- Trust organization) though - as we remember - in accordance with the letter of N. Potapov. Trust was supposed to be still active, though weakened by the arrests.

On July 10, 1927 P. Arapov sent another letter to gen. P. Vrangel, in which he wrote openly that regardless of the failure of the Trust, it was necessary to maintain contact with the Soviet Russia.[25] By implication, of course, through the Eurasian structures.

On July 13, 1927 in the Parisian "Vozrozhdenie", the obituary of Maria Zacharchenko-Shultz was published, which was the beginning of her later glorification as "the martyr of the white matter". The publication was an attempt to stop the rumors persistently circulating among the emigrants that the **whole** E. Opperput's "Troika", which allegedly had to carry out an attack in Moscow as part of a rematch for misleading

[22] L. Flejszman, В тисках провокации…, p. 149.

[23] Hoover Insitution Archives (HIA), Vrangel Coll., Box 151, file No 44, pp. 366–367.

[24] Eurasia – philosophical and political movement in Russia that points out the succession and cooperation of the Russian-speaking culture with Nomadic empires of Euro-Asiatic steppes. It originated in a migrant environment in the 1920s. The organisation was taken over by agents and thus became the next disinformation channel for the GPU (more: T.K. Gładkow, Артур Артузов, Moscow 2008). Just before self-exposure of the Trust, the GPU abstracted the Eurasia organisation from its structure to stay in contact with emigration through it (see: G. Bailey, *The Conspirators*, London 1961, p. 82). After the MOCR-Trust exposure the Division II had no idea that/was unaware that Euroasia can be another GPU legend. It was proved by the letter of the General Command of the Polish Army col., T. Schaetlz to the military attaches in Paris, Prague, Belgrade and Moscow with a request for a discrete explanation, which of the powers was financing the movement – see: AAN, sygn. A.II.23, MSWojsk, SG, Oddział II, No 15567/II.inf./Ros. of 7 December 1927.

[25] (...) Что бы то ни было, я по прежнему считаю, что опасно терять связь с противником; Hoover Institution Archives (HIA), Vrangel Coll., Box 151, file, nr 44, k. 368.

emigration through the Trust, consisted of OGPU agents[26] and Maria herself with her lover E. Opperput survived.

From the end of July 1927, information about the activity of the Bratstvo Russkoi Pravdy (Brotherhood of Russsian Truth) - a group previously marginal and cooperating with the Trust[27], issuing a low-circulation anti-Soviet writing Russkaya Pravda"[28] appeared in the emigration press.

According to the leaders of the BRP, an anti-Soviet uprising was to break out in Russia, especially in the southwest and the Far East of the USSR.[29] Gen. P. Vrangel initially soberly recognized this organization as another OGPU legend[30], but after meeting with the leader of BRP Sokolov (in November 1927), under the influence of documents presented to him by Sokolov, he unexpectedly changed his attitude. Then he published a memorandum in which he stated that BRP was not a OGPU legend, and the head of the BRP "Brother No. 1" served the motherland well.[31] What is more, he maintained that members of the BRP were participants in the terrorist small groups*, Troyki* (including the one directed by E. Opperput and M. Zacharchenko-Shultz) sent to the USSR. This interpretation was then picked up by the émigré press, which first claimed that the member of the BRP was M. Zacharchenko-Shultz herself[32], but then - under the influence of a letter sent to the editor of the journal: "Rossiya" by her husband Grigori Radkievich, who denied it[33] - it began to claim that a member of the Brotherhood was another participant of the *Troyka*, named Yuri Vozniesienskiy, who was to die with Maria in the manhunt carried out by the OGPU.[34]

---

[26] See. L. Flejszman, *W tiskach prowokacji*…, p. 222.

[27] By the way, BRP was active in the Republic of Poland and assisted from our country further Trust operations – see: Когда в июле 1924 года возник «Русский Обще-Войсковой Союз» (РОВС), почти все члены пинской монархической организации и БРП вошли и в РОВС. Пинская полиция не могла тогда разграничить БРП и РОВС: «Деятельность «Братства Русской Правды» и «Русского Обще-Войскового Союза» так взаимно переплетена, что трудно отличить, где кончается деятельность одной организации и начинается – другой, и наоборот. Обе эти организации работают солидарно на территории советов, а разделение труда является таким, что БРП, главным образом, занимается сбором денег на нужды двух организаций, однако руководство принадлежит РОВС». Пинские монархисты (Семен Бродович, Дмитрий Копацинский, Станислав Мацкевич, Николай Котович и др.) были вовлечены в знаменитую чекистскую операцию «Трест»: поддерживали контакты с её активными участниками – евразийцами Юрием Мукаловым и П. Демидовым (Орсини). See. Петербургский и пинский архитектор *Николай Котович*, http://brama.brestregion.com/nomer24/artic16.shtml# [access: 20 XI 2015]

[28] A. Dobkin, С.А. Соколов-Кречетов: От «Золотого Руна» к «Русской Правде» *In memoriam: Исторический сборник памяти А.* И Добкина, S.-Petersburg–Paris 2000, pp. 91–99.

[29] See. Ataman Kreczet, Там*, где еще бьются. Из записной книжки повстанческого атамана*, „Возрождение" of 31 July 1927.

[30] Все это, думается, такая же ловушка для доверчивых дураков, как в свое время пресловутая „монархическая организация" Фёдорова; HIA, Vrangel Coll., Box 147, file 34, k. 390.

[31] L. Flejszman, В тисках провокции..., pp. 279–281.

[32] A. Amfitieatrow, Листки, „Возрождение" of 8 November 1927.

[33] „Россия" of 19 November 1927.

[34] A letter of an alleged member of the BRP, Wasiljew, to the editorial office, published in

On July 30, 1927 gen. P. Vrangel received a letter from another Soviet unconscious agent (resonator), Alexander Guchkov, in which he called to cease all activities in Soviet Russia (i.e. carrying out terrorist activities that the OGPU feared[35]). It should be assumed that A. Guchkov was influenced by his daughter Vera, who was recruited to work with the GPU by her lover Konstantin Radzevich[36] who in 1926 came from Riga to Paris (he lived in the same house as another Soviet agent, known writer Sergei Efron).

On August 7, 1927, gen. P. Vrangel informed gen. A. Shatiilov in the letter[37], that gen. A. Lukomski (who had not spoken to him for more than a year, then suddenly began to write several letters a week) suggesting, among others, that the Trust continued to operate because only part of the organization had been exposed.

In September 1927, in turn, G. Radkievich sent a letter to the officer of the OGPU Wiktor Steckiewicz[38], in which he proposed cooperation with the OGPU in return for the delivery of letters from Maria Zacharchenko-Shultz[39] which was believed to stay in the inner prison of the OGPU. It was a piece of intrusive rumors spreading among the emigration and suggesting that Maria, like E. Opperput, was actually a Soviet agent and that she was not killed in the forests of Smolensk. Missing data on the reaction of the OGPU, but considering the fact that Mr Radkievich was then a combat branch manager of gen. A. Kutiepov organization in Finland, responsible for the implementation of further terrorist attacks on the territory of the USSR, should be taken for granted that the letter was received by the OGPU with great interest. Perhaps this piece of information is closely related to the fact that two more *Troykas* sent to Russia by gen. A. Kutiepov were immediately liquidated (the first - already when crossing the border - all members killed, the second one - captured and used for the demonstration process, in time which its members repented and gave evidence, used later in the Soviet press accusations against the Finnish government, as well as in the note sent by the Soviet government to the government of Finland accusing Finns of involvement in terrorist activities[40]. As a result of this *demarche* Finland expelled the organization of gen. A. Kutiepov, including G. Rakievich, who moved to Poland.[41]

„Возрождению" on December 9, 1927.

[35] (...) после провала „треста" (...) приходится, конечно, приостановить всякую активную работу в России (...); HIA, Vrangel Coll., Box 151, file No 44, k. 265.

[36] The fact that both OGPU agents stopped hiding their political affection in the 1930s can suggest how big the number of agents must have been among the Russians in Paris. Vera was a member of the French communist party and Radziewicz took part in the civil war in Spain as an officer of the Military Brigades.

[37] See the Łukomski's letter of 2 August 1927: (...) одна из линии связий (sic!) была открыта и предана. Но из этого далеко ещё до вывода, что провалились все; see. HIA, Vrangel Coll., Box 147, file nr 33, k. 346–349.

[38] It should be stressed once again that this means maintaining active channel of communication with the trust although there is no information on the sorts of channel the correspondence was being passed.

[39] L. Flejszman, В тисках провокции..., pp. 232–233.

[40] See. W. Ulrich, Необходимо разрушить гнездо террористов в Финляндии , „Izwiestija" of 4 October 1927.

[41] L. Flejszman, В тисках провокции..., p. 272.

On September 11, 1927 the Berlin "Rul" posted *Pis'mo s Gielsingfors*, in which it was reported that the killed member of the E. Opperput Troyka, J. Vozniesienski, was actually named Peters and came from a family of well-known communists.

On October 22, 1927 an anonymous letter titled *Triest and GPU. Pokazanija nieposriedstwiennogo uczastnika* appeared in another émigré newspaper "Bor'ba za Rossiyu", in which a rational (and truthful) assessment of the goals set for the Trust by the OGPU was made. Above all but it stated, that not all of the Trust consisted of OGPU agents, and even - that part of his activists had conspired within the organization, resulting in that the elimination of this organization did not mean the discontinuation of some of its parts, uncontaminated by the infiltration.[42] Presumably, the author of this magazine was G. Radkievich, who was also responsible for sending next *Troykas* to the USSR. It is worth noting that the analysis of the objectives of the Trust presented in the letter was so logical and written in such a clear language that it did not correspond to the level of written expressions of G. Radkievich stored in the Polish Division II archive. One can infer that if he was hiding under the anonymous letter, then he was only the channel of somebody's thoughts. This letter was then reprinted by most of the emigration newspapers.[43]

In 1928, the work of Nikolai Kichkasov was published in the USSR. *Belogvardieiski tierror protiv SSSR*, in which there was distorted information about the liquidation of the *Troyka* of E. Opperput. The information was illustrated with a photograph reportedly presenting M. Zacharchenko-Shultz, shown as a beautiful girl, without actual any similarity to M. Zacharchenko-Shultz. Probably it was supposed to confirm the emigration in the belief that the white activist, who had been killed in Smolensk, was not Maria Zacharchenko-Shultz.[44]

Shortly afterwards G. Radkevich carried out a bomb attack on the OGPU office in Moscow. His actual motive is still unclear to this day (it is not known whether Radkievich wanted to avenge his wife, or it was another OGPU provocation).

The above, short review of the OGPU actions against Russian emigration is, of course, only a piece of the OGPU's activities, which would soon move from disinformation and manipulation to kidnapping and physical liquidation of emigration leaders. From this description of events eventuates that OGPU, ending one legend, **at the same time** offered another one to the victims, hoodwinking the desperate white emigrants, who wanted to hope that this time they would deal with the true patriots fighting against communism. It is also easy to notice that in this game the planners from Lubianka were so brazen that they did not create new organizations or new characters, but to a large extent they used resources existing previously (probably due to pure pragmatics and laziness of officers supervising the operation). While eliminating

[42] The most ridiculed victim of the Trust, Vasiliy Shulgin, was a vivid example of the efficiency of this disinformation. For the rest of his life he believed that the MOCR-Trust members, whom he had met, were true conspirators, maybe even linked to Lev Trocki.

[43] L. Flejszman, В тисках провокции..., p. 273.

[44] Ibidem, p. 303.

the MOCR- Trust organization, the OGPU offered to the emigration Eurasia and the Bratstvo Russkoy Pravdy (both organizations were connected to the Trust, had been known to the OGPU and - at least - infiltrated by the OGPU or since the beginning established as cover organizations Trust type[45]). And the Russian emigres, disappointed and ridiculed, let themselves be caught in the next trap set up by Soviet manipulators playing on the most human feelings: hope, longing for their homeland and fear for the family.

Because each service operates on the basis of the applicable manuals it can be assumed that the above outlined mechanism of continuous provocations could take place in relation to other organizations cooperating with the Trust, including the Polish Division II. The two main activists of the Warsaw Trust organization, Yuri Artamonov and Sergey Voyciekhovski, remained in close contact with the officers of the Department "East" of the II Division, also after unmasking the Trust in 1927. Only written explanations about contacts with the Trust organization were requested from them and the cooperation proceeded without further discussions. Although S. Voyciekhovski, probably fearing that his correspondence had been read by the Division II, wrote openly about his spy analyzes of the political situation, which had been dispatched to Moscow.

Bratstvo Russkoy Pravdy worked in Poland probably like many other provocative or infiltrated structures of the Russian emigration. But the II Division did not carry out any serious investigation to verify the suspicions against its own officers cooperating with the Trust, although - as is clear from the above analysis - the GPU was accusing authentic agents, just to give credence to them and leaving others above suspicions. It can therefore be concluded that although the Trust as an organization was ended, causing an international scandal and compromising cooperating with the Western intelligence white emigration centers, but the large operation which the Trust was only a part of, was continued. The Soviets allowed their victims to open only the first layer of matryoshka, under which, unfortunately, there were other layers of deception.

Conclusion

The above-outlined train of events - in the humble opinion of the author - perfectly illustrates the method of Soviet manipulators described in the introduction. As soon as one source of disinformation was compromised in the eyes of the victims, planners from Lubianka immediately offered another one, but often of a different political provenience. This method due to its simplicity was effective. The apparent multiplicity of sources of information gave the illusion of the possibility of verification and

[45] The problem of the true nature of the organisation – despite the efforts of Russian right-wing historians trying to prove its anti-Soviet nature – is still unclear. One is for sure though, the information passed by the Brotherhood to the West (for example on the alleged common anti-Soviet insurgency) were untrue and their tactics of contacts with the emigration was exactly the same as the tactics of the Trust.

the false comfort of making decisions based on the information allegedly from many sources, then the analysts from the disinformed countries – had to draw the conclusions which **had to be** convergent with the aims of the manipulators, who suggested shreds of information from reportedly many sources.

The Russian Federation, which was founded on the ruins of the Soviet Union, took over the main elements of the Soviet state system, including all the instruments of the special services invented long time ago and perfected by years of disinformation operations Therefore, it is not surprising that the "matryoshka system", i.e. the multiplication of fictitious information sources or seemingly different actors of social processes, who - at least on a strategic level - prefer the same solutions, beneficial to a specific political entity, is still used by Russians today. The methodological problem is only that - unlike historical sources - modern examples of the use of this system are not fully documented and are therefore difficult to accept in the scientific discourse. A good example of this thesis is never repeated information of RTR Planet TV stations from the first days of the Russian-Georgian war, claiming that counterintelligence service of the Russian Federation arrested several dozens of soldiers and officers of the Russian army of Georgian origin who, working for Georgian military intelligence, allegedly fell through the stupidity of their leading officers. The Georgian officers supposedly phoned their agents on using their mobile phones, to quickly get information about the movements of Russian armored columns. Later, this information has never been repeated, nor did the data appear about the mass trials of alleged traitors, what may suggest that Georgian intelligence may have been the victim of provocation using numerous agents reinforcing the primary message.

Accepting the fundamentals of the "matryoshka system" one can put forward the hypothesis that, in accordance with the methodology described above, Russian agents varied from regular "bites" offered to the Georgian intelligence to recruit to classic bidders openly proposing their services, but all of them of the different political background and motivations. The adoption of the perspective of multi-source disinformation, using a trick with an apparent possibilityof verification data, explains both incomprehensible from a military and propaganda point of view the Mickhail Saakashvili's decision to attack South Ossetia and Abkhazia, what ended with a loss by Georgia the both rebel areas and - if not for the intervention of diplomacy of the West – could have led to establishing in Tbilisi authorities fully submissive to the Russian Federation, as well as incomprehensible delay of President Dmitry Medvedev in providing immediate assistance to the peacekeeping Russian troops attacked by the Georgians.

It is worth noting that before the war began, Russian satellite TV channels had broadcast for almost a year a series of reports illustrating the tragic state of the Russian army, in which war ships rusted in the ports, pilots were unable to practice flights due to the lack of fuel, soldiers begging for cigarettes in the streets etc. Aggressive journalistic programs were aired until the outbreak of the conflict, despite the fact that they struck directly in the tandem ruling Russia, i.e. the Prime Minister Vladimir

Putin and President Medvedev. However, during the fights and after their end, the tone of the TV and press reports suddenly changed - they took on a triumphal character. In the context of the whole course of the conflict, which in the opinion of the majority of analysts was marked by the Russian provocation, these actions could indicate the use by Russians of multi-source, mutually reinforcing itself disinformation, which was to convince the Georgians of the inability of the Russian army to intervene decisively.

It is also possible - without a full documentary base – to draw attention to the use of the "matryoshka system" in the protection of the geopolitical interests of the Russian Federation after the breakup of the Soviet Union. The fact that most post-Soviet republics led (and continues to lead) policies in line with the interests of the post-colonial center in Moscow, regardless of the political background of the leaders, may indicate that the Russian agents could be evenly distributed throughout the whole political scene of the post colonial states, and to secure interests of the Kremlin without the risk of changing the pendulum's political course.

Similar phenomenon may be observed also in Central and Eastern Europe, in which Russian intelligence services reaches both to leftist parties and people with nostalgic attitude towards the communist past and, at the same time, to movements representing traditional values, right-wing nationalists, sometimes with the clearly fascist tendencies. From the point of view of pure logic, money supplies to the ideological extremities on both sides of the political stage seems absurd. However, when accepting the assumptions "the matryoshka system" used for the post-imperial *Realpolitik,* it becomes an effective way of realizing the interests of the Russian Federation, immune to the swings of the political or economic environment.

"The matryoshka system", despite its simplicity, is effective. The life of modern man is based on faith to a much greater extent than the life of our ancestors who at least usually knew their surroundings at first hand. Contemporary times meet reality through intermediaries: through mass media, scientific or false truths with no alternatives, so-called. dispersed authority, in a word - almost always second-handed information. Such a construction of reality implies faith in those who are the providers of information. The human mind needs support in order to be able to function. Human thought without faith in the truth is helpless, because the very nature of reasoning requires the acceptance of the truth of the premises. The creators of "matryoshka system" understood it well, and therefore gave (and give) victims an apparent multitude of choices, so that victims, revealing one lie, could not even guess that they are assisted with it by successive manipulators, who gain the victim's trust by exposing the previous lies only to create new ones.

Abstract

The author analyzes one of methods of manipulating with victims of disinformation operations carried out by the Soviet/Russian special services, consisting

of the inclusion of the disinformation agents during the operation, which seemingly offer the opportunity to verify the intelligence obtained by victims of disinformation from previous disinformation agents, but who may also - to win the trust of the victims - participate in unmasking and undermining trust in the agents previously used to deceive the vitims. This method is described graphically as the "matrix system". The article, although describes the use of the "matrix system" on the example of Soviet counterintelligence activities against the white emigration in 1927, simultaneously attempts to put forward hypotheses based on assumptions of the described method, referring to contemporary events like the war in Georgia or infiltration by Russian services of groups placed on opposing extremes of the political spectrum.

Keywords: disinformation, manipulation, political extremities, Russian intelligence, Russian emigration, the policy of the Russian Federation.

V

REVIEWS

Marek Świerczek

T.K. Gładkow, *Artur Artuzow*[1]

The notion of „genius" is usually associated with science and art. There are areas, in which human intellect can lift its spirits based on the stereotype. However, sometimes such terms are extended to other non-creation related areas, like war or criminality. The terms like "military genius" or "criminal genius" shall sometimes be applied. They are accepted and do not offend linguistic purism.

Gladkov's book fits into the above semantic deliberations. The book tells a story of a true genius, devoted to the service of the criminal system, that eventually killed him after using him and his work. The man's name is Artur Artuzov. In the beginning of the 1920s he created the basis for what has been and still is a challenge for the free world – a mechanism of the strategic disinformation carried out by Russian special services.

Artuzov was not even of Russian origin. He was a Swiss citizen, his surname at birth was Frautschi after his father, the cheese maker, and his name was Christian after his grandfather. He got in Russia due to his father, who – like many other nationals of western Europe - wanted to make a fortune in the fast growing Romanovs' empire. Young Christian studied at the St. Petersburg Polytechnic but his interests went far beyond mechanics and chemistry. He wrote poems, dealt with literature, music, foreign languages and, above all, theatre, which resulted some time later in incorporation of some theatrics in Soviet counterintelligence activities. It was probably that got him closer to the chief of the OGPU, Vyacheslav Menzhinsky in the future, who published his works. Additionally, young Frautschi, like the whole Russian intelligentsia, was adopting ideas shaking the basis of the empire up. After 1905 the Russian intelligentsia, as S. Cat wrote, turned to hate their own country. New ideas started to come from the West. The spiritism was developing, mystical movements and Masonry took place of the former attachment to the Orthodox Church. The Masonry together with bourgeoisie and generals aimed at rebuilding the then country under Tsar Nikolai II, who combined - in a typical Russian way - depressing incompetence with a holy belief that his power over millions of people was given him by the God, and therefore he could not share it with anyone. This set of ideas dizzied Russian intelligentsia which combined the Slavic idealism with an almost Mongol mentality of rulers of that Euro-Asiatic empire. Consequently, numerous revolutionary movements developed, and – defied the European logic – claiming he necessity of eradicating parasitic classes, were, at the same time, supported by at least) part of those classes passing lots of money for terrorist activities. This was the way to bring down the hated monarchy. The blinded and thoughtless tsar hit back with repression and extended police apparatus. It resulted in interpenetration of the security and revolutionary

[1] T.K. Gładkow, *Artur Artuzow*. Moskwa 2008, Mołodaja Gwardia, 477 s.

organizations infiltrating each other with double agents. At the same time, the circles of no political activity, noticed Stolypin's reforms and rapid pace of development, which, in the end, had to lead to social and political changes in Russia. One can assume that this balance of power shaped by the corrupt and ruled by the Rasputin tsarist court, the bourgeoisie full of the West, the intelligentsia discussing in Masonic circles and aggressive revolutionary organizations could last checking each other.

Yet, the tsar's foolishness got in the way. Encouraged by ambitious generals he got the totally unprepared Russia in war with central states. The imperial army defeat coincided with a typical for Russian folk contempt for rulers' weaknesses as well as with an active propaganda of the opposition composed of utopia-believers revolutionaries, parochial Masons and the bourgeoisie dreaming of a plutocracy based on the western model. The February Revolution broke out despite the fact that the Russian army was withdrawing in no panic, the economy managed to supply military troops with food and equipment and Russia was the only struggling country with no ration cards. In a paroxysm of failure and for fear of insurrection in the empire – Nikolai II gave up his throne. The festival of the political freedom started. It led to the dismantlement of the state machinery ending in a military coup, grandly called the October Revolution. The seizure of power by the Bolsheviks was not the end of the story. Russia plunged into the economic chaos, civil war, mass terror and constant failure.

This brief historical background is necessary to understand what exactly is this T. Gladkov's story really about? In his work the Russian author creates the picture of Artuzov as taken directly from the stories about Felix Dzerzhinsky in a way typical for writers and researchers linked to Lubyanka. At the picture Artuzov is a noble figure. He is modest, dedicated to the cause of the revolution, giving up the privileges, having nothing to do with Cheka crimes, a real counterintelligence genius.

This is nonsense. Artuzov was recommended for the service in the counterintelligence structures by a pre-war revolutionary, Mikhail Kedrov and like him was extremely cruel and barbaric without human feeling. The Russian historian leaves the facts unsaid or distorts them. By describing next counterrevolutionary organizations by agents provocateurs sent by Artuzov, he does not mention the fate of their members, shot after turning them beaten out of the Cheka torture chambers. He does not mention extorting confessions by torture, psychopathic interrogation methods, like locking a prisoner in a cellar full of decomposing bodies or waterboarding. No mention of "removing one's gloves", i.e. peeling man's skin from captives' palms after pouring their hands with boiling water. No mention of arrests of family members and threats of death in case of no cooperation, no mention of crushing shin bones between railway tracks, squeezing heads in a vice and throwing the convicted into a blast furnace. He was just a Soviet genius of counterintelligence, having – in accordance with the "Iron Felix" rule – clean hands, a cool head and a warm heart…

However, without the propaganda pretentiousness and the ordinary disinformation, Gladkov's book allows us to understand more or less the Artuzov phenomenon.

We got to realise that the Soviet Russia, apart from mass graves, state terror, the system of concentration camps and a lie as the tool of politics, had one undeniable achievement, i.e. an ordinary human lie and duplicity were transformed into a method of the state organs work. Thanks to Artuzov, Soviets discovered that it was not necessary to exterminate opponents, much better was to deceive them. Basically, because of Artuzov, Soviet special services discovered the mass defiance and the strategic disinformation as basic tools for secret services.

Although Artuzov and his kind sent hundreds of people to a brutal death, he differed from them in intelligence. Additionally, he was extremely happy because he was supervised by other intellectually gifted psychopaths of Polish origin[2], i.e. Felix Dzerzhinsky and Vyacheslav Menzhinsky.

And it is due to Artuzov that the systematic and mass provocation was included in the Soviet services methodology, as well as indiscriminate use of double agents, setting up alleged underground organizations or taking control of existing organizations, long lasting and sophisticated counterintelligence operations with opponents not to take advantage of their gullibility once, but to deceive them systematically for as long as possible. Artuzov and his followers refined the method. First operations of this kind, like bringing to the Soviet Russia a Soviet enemy, Boris Savinkov, were relatively short, ca. few months' time. In the form of the developed operation "Trust" they had been lasting between 1921 and 1927. The last known operation of this kind had been run in Cuba against the CIA for over the last 25 years!

Artuzov was behind taking over basic assumptions of the best tsarist criminologist, colonel Arkadiy Koshko. According to him infiltration of hostile organizations and environments should be performed by people coming from them, in all aspects similar to their victims and being able to win their trust. Artuzov took also advantage of the lessons learned from the Jewno Azef case by the Okhrana, which showed that double agents are usually an effective weapon if fully controlled. The Cheka and then the GPU gave Artuzov control tools unavailable to services of civilized countries. He could send out his agents provocateurs planting them to foreign intelligence services and underground organizations because of the collective responsibility, they were always committed to the Soviet authorities. The same authorities which gave themselves the right to punish for disloyalty not only the agents but their families and friends as well. Using such gruesome methods, Artuzov was an eminently intelligent person with a fanatical belief in the communism. Always when tortures and fear failed, he reached for other methods like brainwashing applicable by modern sects. Victims of such "soft" methods of influence became, *inter alia*, members of the Polish Military Organisation (POW), who were caught by the Cheka while on spying mission in the Soviet Russia. Thanks to the ideological input by Artuzov, they became communist fanatics combating their own state. The whole range of Polish renegades changed their positions, including Wiktor Steckiewicz, Ignacy Dobrzyński, Wiktor Marczewski,

[2] In case of Menzhinsky it has not been definitely confirmed.

Juna Przepilińska, Irena Zatorska, Karol Czyllok, Maria Nawrocka-Niedźwiałowska… All of them followed Artuzov blindly like children followed the Rat-Catcher of Hamelin. It was not only that they betrayed Poland but encouraging others to the betrayal. Like a tumour on a tissue that spreads metastasis or vampire victims biting their prizes.

Avoiding mass executions in his Lubyanka stories, Gladkov is pleased to focus on the second, brighter side of Artuzov. He describes his operations resembling theatrical performances. Provoking organisations were used to attract foreign services and the Russian opposition: „the Doggies", „the Liberal Democrats", „the Monarchic Organisation of the Central Russia" called the Trust… And their victims, usually intelligent and experienced people who were deceived by Artuzov's stories. A former terrorist and Bolsheviks' enemy, Boris Savinkov, was deceived first and then was made to do public penance. In the end he was thrown through one of the Lubyanka windows. Fighting with the Soviets, Yurko Tyutyunnyk, was also „persuaded" to cooperate with the Bolsheviks and was executed by a firing squad at the end. Sidney Reilly, a British spy, was besotted by Artuzov to such extent that he did not understand what was going on with him until the very end. He was also shot in the back of his head. Western intelligence services were deceived regularly and on a massive scale. Artuzov reported to the Politburo that 95% of information collected by foreign spies were products of the disinformation office, established by Artuzov himself. Gladkov continues with Artuzov's set of activities until eventually – reluctantly and scantily - describes unavoidable end of that Bolsheviks' loyal servant. Artuzov died like his victims, without knowing what was going on and why he was murdered by the system, to which he had devoted himself so much. Charged with treason, tortured and shot in the back of his head, Artuzov was not the only one. His workmates, Polish renegades died the same way. This was the way the Soviets expressed their gratitude for the loyal service, beating with strings, crushing genitals and sending their families to lagers. Artuzov, like tens or hundreds of thousands of others, giving their lives to the destructive golem, could not understand that the new system had to dispose of them because the mix of cruelty and intellectual panache was just unacceptable for it. For new generations of the NKVD members, the bourgeois intelligentsia the worldliness of the Leninist guards was a pure betrayal of the proletarian home country. Getting rid of them made the career for Soviet villages upstarts easier because they were unable to compete with the multilingual and knowing Europe first generations of the Cheka members other way.

Luckily for Europe or even for the whole world, final chapter of Christian Frautschi's life was only a reminiscence of the special services created by him. The core of the Soviet services survived and developed but after killing its best workers off, it had never regained its initial panache and invention. No one could charm their victims with sharpness and ideology. Out of two elements of the Artuzov's system, i.e. cruelty and intelligence, only cruelty left.

Krzysztof Izak

Nabeel Qureshi, *Answering Jihad: A Better Way Forward*[1]

The reviewed book is dedicated to Islam and not directly to security and the terrorism phenomenon. It was published two years ago but it is worth describing because of two reasons. First, it has been written by an ex-Muslim who had abandoned Islam and converted to Christianity. Second, he sets some views on Islam as the religion of tolerance and peace straight and views on terrorism as the phenomenon inconsistent with Islam. The views are propagated by most Muslims, numerous non-Muslims, some politicians, supporters of migrations to Europe. It is not the first work of this kind. A book by a Swiss journalist, Sylvain Besson, *The Conquest of the west: The Secret Project of the Islamists*[2] should be mentioned here as an example. It is based mostly on court records, analyses and special services materials declassified after the 9/11 attacks. Four years later, Thilo Sarrazin, former senator and a Bundesbank executive board member published a book *Deutschland schafft sich ab: Wie wir unser Land aufs Spiel setzen.*[3] Although he cited publicly known facts on the lack of migrant integration with the receiving country society, German politicians and media attacked him acknowledging his arguments as heresy. Sarrazin was pressured to resign from the post in Bundesbank in a scandal. Although he was a left-wing supporter, not only Angela Merkel's CDU dissented from him but also his own SPD party did. Some Muslim organizations in Germany sued him. Accusations of being anti-Semitic (although unfounded) caused the most damage to him. If Qureshi was a national of western Europe, not the US, he would probably be ostracized as well. Despite the fact that German politicians did everything they could to hush up the debate on immigration and Islam, Sarrazin's book was a bestseller with 2 million items sold. Luckily, another French writer, Michel Houellebecq did not meet such attacks for his novel *Soumission*[4]*,* which describes a future situation in France (2022) when a Muslim party becomes probably a ruling party in the country. The novel was published on the date of the Charlie Hebdo shooting, i.e. on 7 January 2015. Some Polish writers like Bogdan Dobosz[5], Paweł Lisicki[6] and Marek Orzechowski[7] take up this topic as well. The study of a priest, Krzysztof Kościelniak[8] and analysis of Islam and its legal system by Mirosław Sadowski[9] are the closest works to Qureshi's book.

---

[1] N. Qureshi, *W odpowiedzi na dżihad. Lepsza droga ku przyszłości*, Ustroń 2016, p. 211.

[2] S. Besson, *Islamizacja Zachodu? Historia pewnego spisku*, Warszawa 2006.

[3] T. Sarrazin *Deutschland schafft sich ab: Wie wir unser Land aufs Spiel setzen*, Munich 2010.

[4] M. Houellebeck, *Uległość*, Warszawa 2015.

[5] B. Dobosz, *Emiraty francuskie*, Warszawa 2016.

[6] P. Lisicki, *Dżihad i samozagłada Zachodu*, Lublin 2015.

[7] M. Orzechowski, *Mój sąsiad islamista. Kalifat u drzwi Europy*, Warszawa 2015 and *Mój sąsiad islamista*. Tunis-Paryż-Bruksela. Second updated edition, Warszawa 2016.

[8] K. Kościelniak, *Dżihad, święta wojna w islamie*, Kraków 2001.

[9] M. Sadowski, *Islam. Religia i prawo*, Warszawa 2017.

Nabeel Qureshi studies Islam in depth and clarifies the issues of jihad, Islamic terrorism and the ISIS/IS origins. Paris attacks of 13 November 2015, in which 137 people were shot dead and over 300 were wounded, and San Bernardino (California) shooting of 2 December 2015, in which a Muslim married couple Syed Rizwan Farook and Tashfeen Malik killed 14 people and wounded 21 others, and eventually got away from the spot, inspired the American author to write *Answering Jihad: A Better Way Forward.* They were killed in a police shootout. Qureshi is also the author of a *New York Times* bestseller, *Seeking Allah, Finding Jesus,* in which his conversion to Christianity at the age of 22 was chronicled. Nabeel Qureshi was the Ahmadiyya believer, an Islamic religious movement accused of heresy because of Mirza Ghulam Ahmad, who claimed to have been divinely appointed as the Prophet. Because Muhammad is viewed as the final prophet of God in Islam and is called the Seal of the Prophets (Khatam an-Nabiyyin), most Muslims consider Ahmadi Muslims as heretics.[10]

Nabeel Qureshi has divided his work into three chapters: the origin of jihad, jihad today and jihad in the Judeo-Christian context, which contain 18 questions on jihad about things the author is mostly asked about and his comprehensive answers. They show the origin of the phenomenon and present its modern face. Each answer is followed by a short summary. Qureshi does not imply that his interpretation of Islam is the only right. He wants to disclose violence which is at the root of Islam, and that the Quran and the Sunnah are its foundations. The present wave of violence is a result of Salafi movement come back. As long as Islam will be worshipped this way, i.e. calling Muslims for coming back to their roots, it will be followed by violence. Undoubtedly, there are other factors that push Muslims toward radical Islam, no matter if they are of personal (seeking their own identity) or political nature (response to governmental oppression). Nevertheless, no matter what additional factors we are dealing with, the foundation and the history of Islam not only allow to use violence for Muslim dominance, they order it indeed. In the introduction he highlighted being a Christian who abandoned Islam after deeply studying both religions. He is trying to be objective in his message of jihad. He is also trying not to introduce clear Christian opinions although such themes appeared in question number 18 and in the conclusions. The author states in the end of the introduction that the Christian teaching of love directed to enemies, even in the face of death, can be the most powerful response to jihad we poses at the moment. It allows to counteract jihad and to treat Muslims with more dignity as people made in God's image (Islam believers reject this view).

[10] The Ahmadiyya Muslim Community was founded in 1889. Its members believe that Jesus was not crucified but fled to India, where he died in the town of Srinagara (Kashmir region) at the age of 120. The Ahmadiyya combines the features of the fundamental and conservative Islam with modernism. Its goal is to spread restored values of the early Islam by peaceful methods and means, which are addressed to Muslims, Christians, Jews and Hinduism believers. It is the so called „sixth pillar" of Islam. Although the Ahmadiyya followers deviate from the main Sunni tradition due to a specific status of the movement founder, they fulfill major Islam orders.

It is impossible to comment here on answers to each and every question asked by the author in the following chapters. There are six questions in each chapter. Allow me to list all the questions and comment on the most important issues that include selected Quranic verses and ahadith[11] to support the authors' arguments. I would also like to point out a mistake either by the author, or the translator, or the editor in the identical content of questions number 17 and 18: *How Does Jihad Compare with the Crusades?* The correction of the mistake was done in the contents by giving information: question number 17, and question number 18 was constructed as above. Accordingly the table of contents:

Chapter I:

1. What is Islam?
2. Is Islam a "Religion of Peace"?
3. What is Jihad?
4. Is Jihad in the Quran and the Life of Muhammad?
5. What is Sharia?
6. Was Islam Spread by the Sword?

Chapter II:

1. What Is Radical Islam?
2. Does Islam Need a Reformation?
3. Who Are Al-Qaida, ISIS, and Boko Haram?
4. Who Are the True Muslims – Violent or Peaceful Muslims?
5. Why Are Muslims Being Radicalized?
6. Are Muslims Trying to Take Over the West with Sharia?

Chapter III:

1. Do Muslims and Christians Worship the Same God?
2. Why Do Some Christians Call God "Allah"?
3. How Does Jihad Compare with Old Testament Warfare?
4. What Does Jesus Teach about Violence?
5. How Does Jihad Compare with the Crusades?
6. What Does Jesus Have to Do with Jihad?

While describing the concept of jihad, Qureshi distinguishes between the *greater* jihad (jihad akbar) and the *lesser* jihad (jihad asghar). Unlike authors who try to prove that the *greater* jihad means struggle against one's evil inclinations, greed or egoism and deepening of one's faith in the path of God, and the second one was defined as warfare, Qureshi reverses the sequence. He claims that the main meaning of the word "jihad" has always meant physical struggle. Presenting jihad mainly in its spiritual aspect is

[11] The Ahadith mean the record of the words, actions, and the silent approval of the Islamic prophet Muhammad. They are classified into categories such as "authentic", i.e. fully reliable and authoritative (sahih), "good", i.e. for which there are some doubts (hasana), "weak", i.e. the authenticity of which is often questioned (da'if), and "false" (mawdu). the authority of ahadith as a source for religious law (Sharia) and moral guidance within Islam ranks second only to that of the Quran. They are often published in a multi volume works entitled *Kitab as-sitta* („Hexateuch").

inconsistent with the Quran, the ahadith, the history of Islam and the classical Islamic hermeneutics. What is more, jihad as a military struggle was so much significant for the foundations of Islam that it sometimes was referred to as the sixth pillar of Islam (next to the Shahada – declaration of faith, the Salah – prayer, the Sawm – fasting during the month of Ramadan, the Zakāt – charity, and the Hajj – a pilgrimage to the holy city of Mecca). The propensity for violence and armed struggle among early Muslim societies escalated since the Hijra, i.e. Muhammad's emigration to the city of Medina in 622. During the Muhammad's life there were 38 military expeditions (according to some other sources 60), and the Prophet was supposed to be involved in 25 of them. They were the so called blessed attacks (maghazi al-mabruka) and raids (razzia). Their first aim was to get spoils and women, and then to control over the conquered territory. After the Prophet Muhammad's death in 632, the military conquest of the Middle East and the North Africa became more dynamic.

This growing need for a military action by the first Muslims has its reflection in the Quran. There are numerous verses calling for violence, which had been created between 622 and 632, when the Prophet lived in Medina. Nabeel Qureshi focused on the ninth surah of the Quran, Al Tawbah, which, according to him, is chronologically the last main chapter of the Holy Book of Islam. The author translates its title as *the Ultimatum*, while Polish edition of the Quran by Józef Bielawski translates it as *the Repentance*.[12] It is the same name in the well known English translation (*Repentance*) and other translations into English.[13] Bilingual Arab-Polish edition by the Muslim Society Ahmadiyya does not contain any translation of the titles of the Quran's chapters into Polish.[14] The word "at Tawba" can also be translated as "expiation". Anyhow this chapter seems to refer to violence the most. Because of the authoritative regulations and uncompromising nature its content is vied as the ultimate commandment of the Allah his envoy should obey. At the same time, it shall repeal earlier peaceful passages of the Quran of the Muhammad's Mecca period, when a small group of Islam followers living in an unwilling environment had to respect what the hostile majority had to say. After Muhammad had entered Mecca in 630, all previous agreements with polytheists were canceled and an ultimatum was issued, either they would convert to Islam, or they would be killed. The ninth surah orders dropping all agreements with polytheists and subordinating Jews and Christians. According to this surah Muslims should fight, if not their faith is questioned and they are called hypocrites (*munafiqun*

[12] The ninth surah is rarely called *Al-Bara'a* ("The Repudiation"). But this name appears in the ahadith. In his commentary to the Polish edition of the Quran, Józef Bielawski writes that the name of the ninth surah ("Repentance") came from the word „tawbah". Apart from this commonly accepted title another one is also accepted, the title coming from the first word of the first verse, i.e. „al-bara'a". The surah Repentance is one of the last ones and the majority of its content concerns the big war expedition of the Prophet to the north, stopped by Tabuk, the place the battle with Byzantine troops was taken. See. J. Bielawski, *Koran*, Warszawa 1986, pp. 875–876.

[13] Bilingual Arab-English text: M. Pickthall, *The Meaning of The Glorious Qur'an*, Kuala Lumpur 2002.

[14] AMS, Święty Koran. Tekst arabski i tłumaczenie polskie, Surrey 1996.

– it is the biggest insult being called *munafiq* in the Muslim world). If Muslims fight they are promised two types of reward: either spoils of war or paradise via martyrdom (the best example is the activity of the Islamic State and other terrorist organizations). Allah made a deal with the Mujahedeen (jihad fighters): either kill or being killed in a fight for the glory of Allah and Islam. The author of the book claims that *despite the fact that the Quran does probably not provide for something like terrorism of the 21st century*[15]*, it orders Muslims the use of terror and spreading fear: "Make ready for them all thou canst of [armed] force and of horses tethered, that thereby ye may dismay the enemy of Allah and your enemy, and others beside them whom ye know not." The Quran teaching is confirmed by the hadiths. As Muhammad says: I have been made victorious with terror (Sahih al-Buchari 4.52.220). Spreading fear in the hearts of Allah enemies is ordered by the Quran and is reflected in the Muhammad's life.*

The ninth surah confirms the author's opinion on the jihad as an offensive struggle, while many Muslims, being aware of Muhammad participation in numerous fights, believe and claim that the fights were of defensive nature although the Battle of Badr (624) was the ordinary interception of the caravan from Mecca. The surah Repentance orders Muslims also to fight with Jews and Christians because of their religion, not because of any aggression on the part of them. This reasoning was confirmed by sending fighters by Muhammad against the Byzantines for the Tabouk Expedition (630), despite the fact that Byzantine Christians had never threatened Muslim society. John of Nikiû's *Chronicle* is another testament of the offensive jihad in the period of the first Muslims. The Egyptian town was abandoned by Byzantine soldiers after the Arab forces under Amr ibn al-As had approached it and all the civilians there, including children, were killed. Residents of other cities of the then Christian Egypt suffered the same fate. Modern Muslims believe that the obedience of the first generation of Islam followers allowed the Muslim empire to expand so much. It was the time of the Islamic Golden Age perceived by the Muslims as the time of the allegiance to Allah. That was the time when Islam followers were at the height of their power. In the result Muslims are proud of their past, they praise former values and recollect the first generations of their noble ancestors al-*salaf* al-*Sālih* for their sacrifice. If they follow their example and follow the Prophet in unity, Allah will praise them again and restore their might. The wait for the hegemony of Islam and the notion of the Islamic Golden Age have become the source of the faith radicalisation.

In the second chapter the author raises the topic of radical Islam and modern jihad. It is obvious for him that the industrial revolution and the European colonisation brought about an end to Islam domination in many parts of the world. Muslim academics tried to answer the question how it was possible that the world of Islam got subordinated economically and culturally to "infidels". Some reformers tried to purify the religion of accretions skewing Islam and, in opposition to

[15] The author uses the phrase intentionally because the Quran has been existing next to Allah forever and, according to Muslim clerics, its content is still current and its re-interpretation in accordance with the changing reality is forbidden.

modernists, they looked for the rebirth of the Islam might in the roots of the religion and the strict compliance with its rules. Qureshi describes the figures of the three well-known representatives of radical Islam. Abul Ala Maududi (1903-1979) covered a range of disciplines in his works such as, for example, the Quranic exegesis. In his work *Jihad in Islam* he maintained that due to the fact that Islam is all-encompassing, the Islamic state was for all the world and should not be limited to just the "homeland of Islam". The non-Muslims could come into contact with Islam via jihad. Islamic warriors did not conquer new territories, did not kill, did not turn infidels into slaves, were not colonialists, in fact they were liberators and freedom fighters. He wrote that Islam is a revolutionary religion to destroy all states and governments anywhere on the face of the earth. Islam requires the earth — not just a portion, but the whole planet.... because its goal is a worldwide revolution. Al Maududi's understanding and apologetics are influential in the world of Islam to this day. It should be added that already in the 1940s, Ruhollah Khomeini, later leader of the Iranian Revolution indicated that he would be ready to use terrorist methods (and guarantee them the right material and theological support) to humiliate the enemies of Islam. *Islam says: "All the good exists because of the sword and in the shadow of the sword! People cannot be pounded into submission other than with a sword! The sword is the key to paradise, which will be opened only for holy warriors.[16]"* For Sayyid Qutb (1906–1966), who had spent two years in the United States (1948–1950), the West seemed as a terrifying culture of brutal and crude men with no spiritual values. After coming back to Egypt he became the Muslim Brotherhood ideologist (Al-Ikhwan al-Muslimin)[17]and called for bringing down the President Gamal Abdel Nasser, who became the first target for Egyptian radicals. According to the jihad teaching first thing was to tame "the near enemy" (adu karib), i.e. to clean the Muslim society. "The far enemy", i.e. the West, could wait until the Islam would be reformed by itself. It meant the introduction of the Sharia law in Egypt at least. Qutb taught that all human governments on Earth should be overthrown and the kingdom of God should replace them. He argued that the Muslims were responsible for their actions only to God. His approach to jihad was consistent. Jihad should proceed in stages like in the prophet Muhammad's time. First, Islam as the worldwide religion should be proclaimed peacefully. Second, some limited warfare should be introduced, then punishments for the ruler's oppressive actions toward Islamic society should be enforced, and, in the end, endless and unlimited warfare against the non-Muslim world should be started. However, influenced by al-Mawdudi, Qutb perceived jihad as the liberation of the non-Muslim part of humankind, on condition that they were given a chance to hear and consider the message of Islam. And this cannot happen until jihad is not executed.[18] Muhammad abd-al-Salam Faraj (1952–1982), the author

[16] L. Wright. *Wyniosłe wieże. Al-Kaida i atak na Amerykę*, Wołowiec 2018, pp. 67–68.

[17] The Brotherhood's "most frequently used slogan" is *Allah is our goal, the Prophet is our leader, the Quran is our constitution, the jihad is our path and the death in the name of Allah is our desire.*

[18] In the 1990s the Association of the Muslim Students in the Republic of Poland published Polish translations of works by Al-Mawdudi and Qutb in the city of Białystok, where the headquarters

of *The Neglected Duty,* followed Qutb and claimed that Muslim leaders became apostates and Muslims should come back to the concept of pure Islam. He emphasized the role of armed struggle with non-Muslims that would be praised by Allah, and that would give the Muslims new territories to establish the Islamic State and reestablish the caliphate. This is where Islam could be practiced in its pure form. Qutb's declaration on the leaders' apostasy was significantly reinforced by Faraj. This way the foundation for the Takfir criteria was laid, i.e. a concept denoting excommunication against those who do not profess their Islamic faith, applied by extremist Islamic organizations, first and foremost Al Qaeda and the Islamic State.

The criteria are as follow an open display of disbelief, ignoring the Sharia law and refusing involvement in jihad to defend the Ummah. The Islamic State has divided all Muslim people into those who are "the people of paradise", including themselves, and all the rest called "the people of hell". Any worshipper whose interpretation of the Quran and the Sharia law does not comply with the ISIS/IS model would be classified as the member of the second group – an apostate and a godless person that should be eliminated from the sacred society.

Taking the above considerations, the author argues that the radical Islam would come out of the frustration with the political inferiority of Muslim nations towards the West. Based on the Quranic promise that Allah would guarantee the victory those who fight for him, radical Muslims believe that those who are committed to the true teaching of Islam and are zealous in fulfilling its rules, would meet the next Golden Age. It is them who will see the restored glory of Islam. Radical Islam comes from the reasoning that the day-to-day practicing of Islam these days is too remote from the Quran and the teaching of Muhammad. Radicals regard the so called moderate Muslims[19] as apostates quite often because of the lack of their Islam eagerness. And the Quran justifies jihad against Muslim hypocrites (the munafiqun al-muslimin). The Islamic radicalism takes also advantage of the existential crisis among young Muslims, creates an effective link between teaching radical values in mosques and in the cyber space, between the extremist ideology, revolutionary activities and accepting the faith in martyrdom rewarded with the eternal happiness in the paradise. At the same time, contrary to what numerous western Muslims say about terrorists

of the organization was. Nowadays the publication of some works would not be possible as incentive for violence.

[19] The notion is too general and it is hard to say exactly what does it mean. In case it concerns non-practising, laicised Muslims, integrated or assimilated with societies of the host countries, according to the Islam doctrine they are not Islam followers any more. The reason why Muslims can be religious and peaceful despite full of violence teaching of the Quran and the ahadith is that Islam is interpreted by people of a substantial authority, according to different schools of thought and years of certain traditions. If Muslims want to circumvent the rules and come back to the roots of the faith, no matter if they are disappointed by the way Islam is expressed or they just want to please Allah and win his favour or blessing, they start to express Islam in a violent way. Those who want to foster a religious progress in Islam, no matter how few they are and how limited influence they have, are present risking quite often their lives.

as not true Islam followers, that is for Qureshi who they are indeed. Because they praise Allah, try to follow the Prophet's path, they fulfil the Islamic obligations and take care of the Ummah. Generally they make greater efforts to obey the rules of Islam than any average Muslim individual claiming that Islam is the religion of peace.The latter ones do not fulfil the order of the Quran to fight the enemies, even if they are their family members and to fight with those Muslims who do not fight other Muslims, even in the face of a martyr's death leading eventually to salvation. The ultimate goal of the constant struggle is to establish Islam the only religion in the world. Numerous peaceful Muslims ignore some traditions as if they did not exist. In spite of the fact that they consider themselves "good Muslims", there are some inconsistencies with their faith because the Quran and the Hadith contain a full of violence way of expressing Islam. Peaceful version of Islam would have to redefine the Prophet tradition to make it internally cohesive or ignore it. No matter which option the nonviolent Muslims choose, identifying Islamic terrorists as non-Muslims is totally false. One more important argument should also be pointed out here, i.e. the common factor of all radicalised Muslims is their final choice of being loyal to stricter and literally read rules of Islam than to the majority of the other Muslims.

A propensity for violence is manifested by the minority of Muslims, but according to Nabeel Qureshi almost half of them would wish to enforce the Sharia law in Europe and one third would wish to enforce Sharia in the USA. The author cited the former leader of Libya, Muammar Qaddafi of April 2006 talking to Al-Jazeera: *There are ca. 50 million Muslims in Europe. They are the sign that Allah would ensure victory in Europe – without any sword, without any weapon, without any conquest[…]. They would turn it into a Muslim continent in few decades. Europe is in a perplexing situation. Just as America is. They should accept Islam in the course of time, if not, they will have to declare war on Muslims.* This statement confirmed the fears of numerous conservatives in the West, that the Muslims have started a demographic and ideological war to overthrow western systems of law and the culture. It raised discussions focusing on two main subjects: Sharia and the Muslim demography. The Organisation of Islamic Cooperation (OIC) works actively towards the Islam domination in Europe. It is the second largest international organisation, after the United Nations, consisting of 57 countries and having its headquarters in Saudi Arabia. It submits an annual report on the islamophobia in the West. Qureshi points out that "islamophobia" is a poorly described concept, allegedly used for determining prejudices against Muslims, but mostly used just as a general term to determine any Islam criticism or any Muslim criticism, no matter true or imaginary. By the reports and political pressure, the OIC lobbies subjectively against the freedom of speech, counting on calming criticism of Islam, which is effective quite often when we look at the situation in many EU countries. According to the OIC the freedom of speech protects people who *tend to cause unjustified tensions, suspicions and social unrest time and again, aspersing the Islamic faith by huge distortion and misinterpretations, entering the questionable terrain and offending religious feelings of Muslims.* In other words, people who criticize Islam are to blame for unrests in Muslim societies.

This OIC's statement is directly in contradiction with the freedom of speech but is completely in line with Sharia. In the USA similar efforts are made by the Council on American – Islamic Relations (CAIR) that is under the strong influence of the Muslim Brotherhood movement. The CAIR accuses those Muslims who do not agree with its decisions of islamophobia. The author cites the study by Raheel Raza, the President of The Council for Muslims Facing Tomorrow, who claims that radicalism prevails in the Muslim world, it only depends how it is understood. If only mujahideen are regarded as radical Muslims, their number will be scant, but if those who want management consistent with Sharia are taken into account as radicals, they will dominate in the Muslim world. Most Muslims reject also the western model of the secular and democratic country which is inconsistent with the universal governance based on Islam. One of its features is the submission to Allah only, the second is a dominance, i.e. enforcing their laws on all the nations and gradually imposing their power on the whole world.

In the third chapter of his book, Qureshi takes interesting considerations regarding basic differences in the God's understanding by the Muslims and the Christians, and the essence of violence in both religions. As a former Muslim follower and currently a practising Christian knowing both the Quran and the Bible, he explains the contradictions and accusations of both religions representatives, hitting numerous stereotypes in the way the Christians and the Muslims think. To begin with, the author claims that the Muslims and the Christians, contrary to what many people think, do not believe in the same God. This is supposed to be in spite of the fact that he Quran ensures that the Torah and the (Canonical) Gospels are inspired works and the Jews and the Christians are The Book's People and that the Quran tells the Muslims to communicate to the Jews and the Christians that they have the one God. But the identity of the Muslims' God is different from the identity of the Christians' God. Jesus (Isa) is called in the Quran one of the prophets, not the son of God. The Muslims reject the faith in his crucifying, his resurrection and the Holy Mother worship (docetism). Islam rejects the Trinity doctrine, and, in contrast, it asserts their own fundamental dogma of Tawhid, i.e. "the oneneness of God" (monotheism). Tawhid rejects the Trinity so strenuously that it makes us to accept the concept of God in Islam totally different from the concept of the God in Christianity. They are almost contradictory. For Muslims the God is not a father of humankind because humans are only beings created by God. Those dogmatic differences in perceiving the God were reflected in one of the orders of the Higher Court in Malaysia of June 2016. The court issued a ruling that claimed illegal calling the Christian God "Allah" by local Christians. In the past the Catholic Church contested the ban because the Malaysian translation of the Bible had used the word "Allah" for ages. At the beginning the Catholic Church managed to convince the Malaysian government to lift the ban, but in response the Muslims started to attack Christian churches, which made the ban was eventually restored in October 2013. Three months later copies of the Bible were confiscated because they contained the word "Allah" as the name of God and in June 2014 judges confirmed officially uncompromising stance towards Christians.

The next important topic of Qureishi's considerations is the concept of jihad as the Islamic warfare doctrine and the Jewish wars from the Old Testament. Muslim theologians allege the Jews and the Christians that their Bible is also full of violence. However, sacred books of the Muslims and the Christians are different things. The Quran was verbally revealed by the God to Muhammad through the angel Gabriel, while the Bible and the Old Testament are different works written by people, in which there were numerous either true or untrue events included, not necessarily applauded by God. Such events should not be treated in the same way as struggles or wars ordered by Allah himself. Violence in the Old Testament ordered by the God himself started after 400 years of waiting. The God reminded Jews that banishing other peoples happened not because Jews were the best, what the Quran reminds Muslims, but because they sinned against the God. Struggling in the Old Testament is the pattern the Christians should not follow. The history of Christianity have not evolved from the peaceful and quite story to a full of violence reality but the other way round. Meantime, the life of the prophet Muhammad changed from a peaceful and quite into a full of violence. The Quran charges the Muslims to fight with the Jews and the Christians so that Allah could make Islam above any other religion. Love and mercy are the charge for the Christians, and jihad is a charge for the Muslims. Developing this strand the author compares the concept of jihad in Islam to the Holy War in Christianity. The Christians developed the concept only a thousand years after Jesus while Muhammad himself and the Quran taught that the struggle is benign. Jihad (the Holy War) lies at the heart of the Islamic faith. Nabeel Qureshi disputes with numerous politicians and authors about the crusaders, for example John Esposito, a professor of Islamic Studies at the Georgetown University, who wrote in his book *Islam: The Straight Path* that: *five years of peaceful coexistence fell apart because of political events and imperial and papal games which led to centuries-long series of the so called holy wars, directed the Christianity against the Islam and left miscomprehension and lack of trust until these days*. However, these words are based on a fiction that dominates in a common understanding of the crusades, also by numerous western authors. They forget that it was Muhammad himself, who stood up against the Byzantine Christians, subordinating Christian lands (and not only lands), like the Quran ordered. It were the Muslims who had conquered two thirds of the Christian world before the first crusade. In Qureishi's opinion, while condemning crusades, one should remember their reasons and circumstances, i.e. defensive efforts following the conquest of the Christian world by the Muslims. Nevertheless, the author condemns crusades, during which the slaughter of the innocent Jews in Europe and the Muslims in Jerusalem was committed. This unjustified cruelty was done in the name of God. The author admits that he would feel much better if the efforts of crusaders had resulted from the orders of the leaders of the European countries and not from the Church. However, as a Christian he was grateful that it took Christians a thousand years to distort the teaching of Jesus to such an extent that the crusades became a religious order as a holy war. Christ did not envisaged any concept of it, after all. It was born only in the XIth century. By contrast,

full of violence and offensive jihad carried out today by Muslim extremist organizations, is the Quranic order. Foundations of Islam urge its followers to participate in the holy war/jihad, offering them salvation in case they die in it. It took Muslims 1300 years to move away from radical foundations of their religion.

In the conclusions the author writes: *[...] almost all Muslims, no matter if peaceful or not, believe that they adhere to the original form of Islam. Those Muslims who study Quranic texts diligently, would face eventually the conclusions, that the foundations of their religion are full of violence. That was my case as well. I kept getting them out of my mind for years but when the reality became inevitable, I hit the crossroads and had to choose: either apostasy, malaise or radicalisation.* As we know, Qureshi chose the first option because he stood against the fully violent tradition of Islam. He had a Christian friend who showed him that Islam is not the only option for him and that there are particular reasons to become a Christian. According to his experience secularity and atheism are not an alternative to Islam because they are not spiritually developed, which most Muslims stick to. At present the number of frustrated Islam believers is snowballing. The reason is the content in the web space passed via social media which are a great source of propaganda, indoctrination and recruitment. The author suggests arousing actively positive emotions of love and friendship among Muslims, acknowledging the truth of Islam at the same time. In my opinion it is impossible because the truth of Islam presented by Qureshi deprives us of the optimistic vision of the future, particularly in view of the dynamic increase of the number of Muslims in Europe and their growing radicalisation.

The edition contains four appendixes: A – timetable for jihad in Islam since Muhammad was born until the San Bernardino attack in December 2015; B – the Prophet's statements about jihad gathered in the Muhammad ibn al-Buchari's set of hadith; C – the answer for what the caliphate is?; D – information on the Ahmadiyya movement. Additionally, there is also a glossary in the end of the book. Nabeel Qureshi's book is very interesting. It presents Islam to an ordinary Westerner from the little-known perspective. It shows religious source of terrorist attacks carried out by Islamic terrorists. It is easy and nice to read, and it gives a lot of thought. I truly recommend it to all interested in Islam and to all professionally dealing with recognizing and combating terrorism.

VI
REPORTS

Witold Ostant

The minutes from the Polish nationwide conference "Picture of the current terrorism phenomenon"

The first Polish nationwide conference entitled "Picture of the current terrorism phenomenon" was held from 23 to 24 April 2018 at the War Studies University in Warsaw. It was organised and co-organised by the Political Science and Journalism Faculty, Adam Mickiewicz University; the Political Science Faculty, Mikołaj Kopernik University; the Social Science Faculty, the University of Gdańsk; the National Security Faculty, the War Studies University in Warsaw; the Faculty of Cybernetics, the Military University of Technology; the Faculty of Command and Naval Operations, the Polish Naval Academy; the Faculty of Security Studies, the Military University of Land Forces; the National Security and Logistics Faculty, the Polish Air Force Academy; the Faculty of Internal Security, the Police Academy in Szczytno; the Faculty of Security Studies, Andrzej Frycz Modrzewski Krakow Academy; the Faculty of Political Science and International Studies, the University of Warsaw; the Institute of International Relations, the University of Wrocław; the Institute of Political Sciences and European Studies, the University of Szczecin; the Institute for Western Affairs in Poznań; the Scintific Institute for Security, the WSB University in Chorzów; the Centre for Political Analysis, the University of Warsaw; the Faculty of Security Sciences, the Rzeszów University of Technology; the Movement of Defence Communities and the Scientific Foundation of Research. The conference was held under the patronage of the following prestigious scientific journals: „Przegląd Zachodni", „Przegląd Strategiczny", „Przegląd Bezpieczeństwa Wewnętrznego", „Przegląd Politologiczny", and the Polish Geopolitical Association, the AT-System Group Foundation, Difin S.A. and the Polish Association of Political Sciences. The patrons of honour were: gen. bryg.dr Ryszard Parafianowicz – Chancellor-Commandant of the War Studies University in Warsaw; insp. dr Marek Fałdowski – Commandant of the Police Academy; płk dr hab. Bogdan Grenda – Dean of the Faculty of National Security, the War Studies University in Warsaw; prof. dr hab. Ryszard Zięba – the Institute of International Relations, the University of Warsaw; prof. dr hab. Zdzisław Winnicki – Director of the Institute of International Relations, the University of Wrocław; prof. dr hab. Janusz Ruszkowski – Director of the Institute of Political Sciences and European Studies, the University of Szczecin; prof. dr hab. Sławomir M. Mazur – Dean of the Faculty of Security Studies, Andrzej Frycz Modrzewski Krakow Academy; dr hab. Urszula Chęcińska – Dean of the Humanistics Faculty, the University of Szczecin; dr hab. Andrzej Stelmach – Dean of the Faculty of Political Science and Journalism, Adam Mickiewicz University; dr hab. Stanisław Sulowski – Dean of the Faculty of Political Science and International Studies, the University of Warsaw; dr hab. Stanisław Gędek – Dean of the Faculty of Management,

the Rzeszów University of Technology; dr hab. Zbigniew Karpus – Dean of the Political Science Faculty, M. Kopernik University; dr hab. Tadeusz Dmochowski – Dean of the Social Science Faculty, the University of Gdańsk; płk dr hab. Adam Radomyski – Dean of the National Security and Logistics Faculty, the Polish Air Force Academy; płk dr hab. Witalis Pellowski – Dean of the Faculty of Security Studies, the Military University of Land Forces; kmdr dr hab. Jarosław Teska – Dean of the Faculty of Command and Naval Operations, the Polish Naval Academy; dr Krzysztof Koj – Dean of the WSB University in Chorzów and dr Justyna Schulz – Head of the Institute for Western Affairs in Poznań.

The main goal of the conference was an in-depth reflection on the terrorism phenomenon, which has become one of the main challenges and threats to the security in a broader sense in the beginning of the 21st century. The main discussions were focused on a global war on terror – its background, dimensions and perspectives; the topic of terrorism and failed states or failing states; the topic of terrorism and migration problems in the current world; the topic of terrorism and democratic countries – challenges and threats; the topic of terrorism and weapon of mass destruction. The event was unique due to a careful choice of participants. Its multidisciplinary nature was guaranteed by the high level of the debate based on the methodology. Both practitioners and theoreticians took part in the considerations. There were representatives of different scientific areas from the major scientific and analytical centres in Poland. Apart from the scientific value of the conference its practical aspect should also be stressed. Establishing the level of the most important threats from a growing number of terrorist events seems a precious value which can be used by the state institutions and law enforcement agencies.

There were six scientific panels during the conference and 30 papers were read. There was also a reporter's debate held, in which, *inter alia*, Witold Repetowicz, Wiktor Bater, Rafał Stańczyk, Jan Wójcik and Dawid Wildstein took part.

On the first day of the meeting the tac-ops exercise with the use of a helicopter was presented. It was organised by the Bureau of Anti-terrorist Operations at the Police HQ. On the second day of the conference the equipment was demonstrated which is used by the representatives of the State Protection Service while performing their professional tasks.

The conference was officially opened by płk dr hab. Bogdan Grenda – Dean of the Faculty of National Security, the War Studies University in Warsaw; then the opening lecture was given by prof. zw. dr hab. Ryszard Zięba from the Warsaw University. The opening lecture by prof. R. Zięba was an in-depth study of the terrorism phenomenon in respect of other challenges and threats to security in the second decade of the 21st century.

There were two presentations in the first panel of particular interest. The first one entitled "Social goals of terrorists in the European Union states" was given by prof. dr hab. Jarosław Gryz from the War Studies University in Warsaw. The second presentation entitled „the Anti-Terror System" was a dynamic demonstration

of action taken by a single shooter in a situation of a direct danger. It was prepared by dr Aleksandra Gasztold from the University of Warsaw and Maciej Górski – both co-founders of the AT-System Group Foundation. Prof. J. Gryz presented operational, tactical and strategic goals of terrorist groups active in the EU states aimed at undermining fundamental cooperation and organization of the present democratic and liberal societies. The team from the AT-System Group Foundation showed the optimal model of behaviour in a situation of threat from the so called "single shooter" (the most frequently used method of terrorists attacks in the US and in the Western Europe states).

In the second panel there were two topics of a particular significance due to their timeliness. The first topic concerned the security of air traffic, which was presented in the most accurate and complex way by płk rez. dr hab. Adam Radomyski from the Polish Air Force Academy in Dęblin. The paper was entitled „The current aspects of countering the air terrorism". The second topic presented the problem of refugees and its potential effects in the context of terrorist threat. There were also two papers worth mentioning in the area: "Anti-Terrorist and Refugees Policy as the EU challenge in the 21st century" by dr hab. Izabela Oleksiewicz from the Rzeszów University of Technology and „Is a migrant a terrorist? Revision of migration solutions: the UNO 2018" by dr Joanna Dobrowolska-Polak the Institute for Western Affairs in Poznań.

The first day of the conference ended with a reporters' debate, which aroused similar lively discussion to the papers presented earlier. The experienced journalists practitioners took part in this discussion, inter alia, prof. dr hab. Piotr Grochmalski – Head of the Strategic Studies Institute of the National Security Faculty, the War Studies University in Warsaw and Witold Repetowicz.

The second day started with two parallel panels. There were ten papers presented, among of which the following ones should be distinguished: "The Islamic State Activity in the Syrian Conflict" by dr hab. Marian Żuber from the Military University of Land Forces, „The use of the Internet by Islamic Terrorists" by płk dr hab. Piotr Dela from the War Studies University, and „Personal Recognition In the Scope of Terrorist Threat. Groups of Risk" by podinsp. Przemysław Wrzosek and podinsp. Mariusz Kupniewski from the Police Academy in Szczytno. Considering the three so distant topic regarding one basic subject, it should be stressed that during the discussion the need of interdisciplinary teams for fighting terrorism was raised and the need of an in-depth reflection on the subject while preparing strategic documents in the security area.

Two further panels were dedicated to challenges facing Poland as far as the fighting of terrorism is concerned, both in internal and external aspect as well as in bilateral and multilateral aspect. Analyzing the most important subjects the value of the presentation by gen. dyw. (rez.) pil. dr Anatol Czaban from Adam Mickiewicz University „Terrorism in the strategies of the states' and organizations' security. Present challenges" should be stressed. The presentation "The culture of security in the Polish society from the perspective of terrorist attacks in Europe" by dr Maciej Magiera from Adam Mickiewicz University and the paper entitled „Anti-terrorist security in view of the specific competencies of the Polish special services in terms of foreigners'

surveillance" by dr Remigiusz Rosicki from Adam Mickiewicz University should also be mentioned here.

In view of the complex approach of the above cited authors we should bear in mind how many deficits are there still in scope of countering terrorism in Poland and how much effort should be put into enhancing the Polish anti-terrorist system in Poland directed not only to fight the phenomenon but also to prevent it. The security education seems to be the most effective tool of the prevention.

In conclusion, this nationwide scientific conference, the first of that kind in Poland, was a big event in the country in 2018. Due to a highly specialized knowledge it has a chance to become an element of an effectiveness of the public administration in the area of terrorism counteracting.

This definite success of the event would not have been possible without support and engagement of many people who worked for its best professional and organizational success.

In view of this, on behalf of the organizers and co-organisers of the conference particular thanks should be extended to: dr Cyprian Kozera – the War Studies University, dr Piotr Lewandowski – the War Studies University, dr Przemysław Gasztold – the War Studies University, ppłk dr Grzegorz Motrycz – the War Studies University, dr Anna Mróz-Jagiełło – the War Studies University, Ewelina Czerwińska – the War Studies University, Grzegorz Woźny – the War Studies University, Paulina Krawczyk – the War Studies University, Emilia Solarz – the War Studies University, Jowita Brudnicka – the War Studies University, Jagoda Gawliczek – the War Studies University, dr Monika Lewińska – the War Studies University press secretary, Monika Dzięciołowska – the War Studies University, dr Natalia Jackowska – the Western Institute („Przegląd Zachodni"), Anna Przyborowska – the Internal Security Agency („Przegląd Bezpieczeństwa Wewnętrznego"), dr hab. Magdalena Karg-Musiał, Adam Mickiewicz University („Przegląd Politologiczny") and prof. zw. dr hab. Sebastian Wojciechowski – Adam Mickiewicz University („Przegląd Strategiczny").

O autorach

Danuta Gibas-Krzak – doktor habilitowana nauk politycznych, bałkanistka. Pracownik naukowy Uniwersytetu Humanistyczno-Przyrodniczego im. Jana Długosza w Częstochowie, współpracownik ośrodków badawczych i naukowych w Serbii, Bośni i Hercegowinie oraz Chorwacji.

Dariusz Gradzi – adwokat, kancelaria adwokacka AKGK Adwokaci Kostański Gradzi Kuczara.

Konrad Hennig – doktor nauk humanistycznych, wykładowca Akademii Humanistyczno-Ekonomicznej w Łodzi.

Krzysztof Izak – emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Mateusz Jaremczuk – doktorant nauk społecznych (nauki o bezpieczeństwie) Akademii Sztuki Wojennej. Absolwent Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej. Autor publikacji poświęconych geopolityce.

Piotr Karasek – doktorant w Katedrze Kryminalistyki Wydziału Prawa i Administracji Uniwersytetu Warszawskiego.

Witold Ostant – doktor, adiunkt w Katedrze Badań nad Terroryzmem Akademii Sztuki Wojennej w Warszawie, ekspert w zespole Institute for Security, Energy and Climate Studies w Warszawie.

Tomasz Safjański – doktor nauk prawnych, emerytowany oficer Policji. W latach 2006–2007 zastępca dyrektora Biura Wywiadu Kryminalnego KGP, 2005–2007 – Szef Krajowej Jednostki Europolu (Head of Europol Nartional Unit – HENU) i reprezentant Polski na posiedzeniach tego gremium. W latach 2006–2007 zastępca dyrektora Biura Wywiadu Kryminalnego KGP.

Marek Świerczek – doktor, funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Krzysztof Tylutki – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Waldemar Walczak – doktor nauk ekonomicznych, Uniwersytet Łódzki.

About authors

Danuta Gibas-Krzak – PhD in Political Science; expert on Balkan issues; researcher at Jan Długosz Academy in Częstochowa, associate researcher at research and scientific centres in Serbia, Bosnia and Herzegovina and Croatia.

Dariusz Gradzi – defence attorney, AKGK Adwokaci Kostański Gradzi Kuczara law firm.

Konrad Hennig – PhD, the University of Humanities and Economics in Łódź lecturer.

Krzysztof Izak – retired officer of the Internal Security Agency.

Mateusz Jaremczuk – PhD student, the War Studies University (national security sciences); the Faculty of National Security at the National Defence Academy graduate; researcher in the area of geopolitics and author of the publication in the area of geopolitics.

Piotr Karasek – PhD student, the Faculty of Law and Administration, the University of Warsaw.

Witold Ostant – PhD, Assistant Professor in the Terrorism Research Department, the War Studies University; the Institute for Security, Energy and Climate Studies in Warsaw expert.

Tomasz Safjański – Doctor of Juristic Science, retired Police officer. In the years 2006-2007 deputy Head of the Criminal Intelligence Office of the Police HQ. In the years 2005-2007 the Head of the Europol National Unit.

Marek Świerczek – PhD, officer of the Internal Security Agency.

Krzysztof Tylutki – officer of the Internal Security Agency.

Waldemar Walczak – Doctor of Economics, the University of Łódź.

Informacje dla autorów „Przeglądu Bezpieczeństwa Wewnętrznego”

I. Zasady przyjmowania prac

1. Redakcja „Przeglądu Bezpieczeństwa Wewnętrznego” przyjmuje tylko materiały oryginalne (wcześniej niepublikowane).
2. Materiały autorskie kierowane do druku w „Przeglądzie Bezpieczeństwa Wewnętrznego” podlegają ocenie merytorycznej członków Redakcji i co najmniej dwóch recenzentów zewnętrznych.
3. Recenzje zewnętrzne mają formę pisemną i kończą się jednoznacznym wnioskiem dotyczącym dopuszczenia artykułu do publikacji (bez zmian lub po wprowadzeniu przez autora zmian sugerowanych przez recenzentów) lub jego odrzucenia.
4. W przypadku dwóch recenzji przeciwstawnych Redakcja przesyła artykuł do kolejnego recenzenta. Po analizie wszystkich recenzji Redakcja podejmuje decyzję o zamieszczeniu lub niezamieszczaniu artykułu.
5. Do publikacji są kwalifikowane artykuły, które uzyskały pozytywną opinię końcową.
6. Po zakwalifikowaniu artykułu do publikacji autor lub autorzy podpisują umowę o przeniesieniu na wydawcę autorskich praw majątkowych.
7. W przypadku utworu stworzonego przez kilka osób każdy z autorów jest zobowiązany do złożenia *Oświadczenia o wkładzie poszczególnych autorów w powstanie publikacji* (wzór *Oświadczenia* jest dostępny na stronie Agencji Bezpieczeństwa Wewnętrznego) i przesłania go na adres Redakcji PBW podany w pkt II ppkt 1.
8. Autorzy artykułów zakwalifikowanych do druku otrzymują honoraria w wysokości 30 zł brutto za jedną stronę tekstu, sformatowanego zgodnie z *Informacjami dla autorów „Przeglądu Bezpieczeństwa Wewnętrznego”* znajdującymi się w każdym drukowanym numerze *„Przeglądu…”* oraz na oficjalnej stronie internetowej Agencji w zakładce „PBW”.

II. Zasady przesyłania i opracowywania tekstów

1. Wszystkie teksty należy przesyłać w postaci zapisu elektronicznego (Word, Open Office) na adres Redakcji: redakcja.pbw@abw.gov.pl.
2. Do artykułu należy dołączyć:
   a) bibliografię załącznikową (według schematu opisanego w ppkt 13),
   b) streszczenie w języku polskim nieprzekraczające 15 wierszy wydruku komputerowego, zawierające cel i podsumowanie artykułu,
   c) notkę o autorze (zawód lub tytuł naukowy, miejsce pracy),

   d) słowa kluczowe (w celu maksymalnie zwięzłego określenia tematyki artykułu – mają one ułatwić klasyfikację treści oraz wyszukiwanie artykułu w elektronicznych bazach danych; słowa kluczowe nie powinny być powtórzeniem tytułu).
3. Teksty muszą być napisane antykwą (pismem prostym), czcionką Times New Roman, stopień czcionki – 12; interlinia – 1,0; marginesy – 2,5 cm. Objętość artykułu zgłaszanego do publikacji (wraz z bibliografią, streszczeniem, słowami kluczowymi) nie może przekraczać 15 stron wydruku komputerowego w formacie A4, sprawozdania z konferencji – 3 stron, recenzji – 10 stron.
4. Autorzy są zobowiązani do wypełnienia *Formularza zgody autora na publikację artykułu w czasopiśmie „PBW"* (Formularz jest dostępny na stronie Agencji Bezpieczeństwa Wewnętrznego) i przesłania go na adres Redakcji PBW podany w ppkt 1.
5. Rysunki i fotografie należy lokalizować w tekście głównym za pomocą podpisów.
6. Wszelkie ilustracje, zdjęcia oraz schematy, które autor chciałby umieścić w artykule, powinny być dostarczone w oddzielnych, oryginalnych plikach. Ich wymiary powinny być nie mniejsze, niż te, które mają być uzyskane po wydruku oraz możliwie jak najlepszej jakości (min. 300 dpi w skali 1:1). W przypadku dostarczenia ilustracji złej jakości Redakcja zastrzega sobie prawo do ich niezamieszczania.
7. Należy podać źródła wszystkich materiałów ilustracyjnych (zdjęć, rysunków, wykresów, schematów, tabel itd.).
8. Na końcu podpisu pod materiałem ilustracyjnym należy stawiać kropkę.
9. Odsyłacze do przypisów powinny być umieszczone w tekście przed znakami interpunkcyjnymi – kropką kończącą zdanie (wyjątek: skrót r. – rok lub podobny), przecinkiem itd.
10. Cytaty ze źródeł i literatury przedmiotu, nazwy ustaw oraz innych aktów prawnych, tytuły prac naukowych, utworów literackich, muzycznych, dramatycznych, obrazów, konkursów należy wyróżniać kursywą bez cudzysłowu. Cytaty dłuższe niż 3–4 wersy należy pisać antykwą, stopień czcionki – 11, oraz oddzielić je od treści odstępem przed cytatem i po nim. Cytaty w przypisach należy pisać antykwą w cudzysłowie.
11. Nazwy wystaw, konferencji i sesji naukowych należy pisać antykwą w cudzysłowie.
12. W przypisach powinien być zachowany następujący schemat opisu:
    a) przypis zaczynamy wielką literą (wyjątek stanowi przypis internetowy) i kończymy kropką,
    b) przypis archiwalny: nazwa archiwum, po przecinku – nazwa zespołu, po przecinku – sygnatura, po przecinku – nazwa dokumentu (kursywą) lub jego opis (np.: list, sprawozdanie) i data, po przecinku – numer karty (strony),

PRZYKŁADY:

AIPN, OBUiAD w Krakowie, IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57;

APK, UWŚl., sygn. 736, sprawozdanie z działalności Policji Województwa Śląskiego za 1928 r. z 5 I 1929 r., k. 57;

c) druki zwarte: inicjał imienia, nazwisko autora, po przecinku – tytuł (kursywą), po przecinku – ewentualnie tom, po przecinku – miejsce i rok wydania, po przecinku – numery stron; po tytule publikacji zamieszczonej w pracy zbiorowej stawiamy przecinek i piszemy: w: i tytuł pracy (kursywą),

PRZYKŁAD:

W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, s. 36;

d) artykuły w czasopismach: inicjał imienia, nazwisko autora, po przecinku – tytuł (kursywą), po przecinku – tytuł czasopisma w cudzysłowie, dalej (bez przecinka) rok wydania, po przecinku – zeszyt, numer, część (w opisie należy stosować cyfry arabskie), po przecinku – numery stron,

PRZYKŁAD:

W. Nowak, *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 13;

e) wydawnictwa internetowe: adres internetowy rozpoczynający się małą literą (bez podkreśleń i hiperłączy), po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:

http://www.pbw.gov/abw/cat.html [dostęp: 1 XII 2011];

f) artykuły lub dokumenty zamieszczone na stronach internetowych: tytuł artykułu (dokumentu) kursywą, po przecinku – adres internetowy, po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:

EU NAVFOR Somalia – mission, http://www.eunavfor.eu/about-us/mission/ [dostęp: 20 VII 2014];

g) podając numer strony, należy stosować skrót: s. (np.: s. 30); zakres stron

należy zaznaczyć półpauzą bez świateł, np.: s. 24–27,

h) należy stosować oznaczenia: tamże, tenże, taż (jeżeli tego typu zwroty rozpoczynają przypis, należy stosować wielką literę), inicjał imienia, nazwisko autora, po przecinku – skrót tytułu (kursywą), po przecinku – numery stron; nie stosujemy skrótów: op. cit., loc. cit.,

PRZYKŁADY:

W. Nowak, *Służba*…, s. 12.

Tamże, s. 14;

i) po skrótach: zob. i por. nie stawiamy dwukropka,
j) po skrócie: cyt. za stawiamy dwukropek,
k) po słowie: patrz stawiamy dwukropek.

13. Przy zestawianiu bibliografii załącznikowej kolejne pozycje szeregujemy w porządku alfabetycznym (również akty prawne). Opis każdej pozycji rozpoczynamy od nazwiska autora, po nim umieszczamy inicjał imienia, kropkę, przecinek, a następnie według schematu przypisu – tytuł zapisany kursywą itd. W przypadku druków zwartych na końcu opisu bibliograficznego należy podać łączną liczbę stron, w przypadku artykułu w czasopiśmie lub w pracy zbiorowej – zakres stron.

PRZYKŁADY:

Kowalski W., *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 12–20.

Nowak W., *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3,

K. Kowalski (red.), Warszawa 1999, PWN, s. 32–47.

Sekretna wojna. Z dziejów kontrwywiadu II RP, Z. Nawrocki (red.), Poznań 2014, Zysk i S-ka, 542 s.

W bibliografii załącznikowej akty prawne należy oddzielać od innych źródeł.

14. W tekście głównym należy stosować ogólnie przyjęte skróty (np., itp., m.in., rkps, mps, t., z. itd.), a także z reguły: r. (rok) i w. (wiek).
15. W tekście głównym, podając datę, nazwę miesiąca należy zapisywać słownie, np.: 3 lipca 1969 r. Wyjątek stanowi zapis podany w przypisie, gdy miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.
16. Różne sposoby zapisu daty stosowane w tekście głównym powinny być ujednolicone do następującej formy: dzień zapisany cyframi arabskimi, miesiąc zapisany słownie, rok zapisany cyframi arabskimi (np. jak wyżej – 3 lipca 1969 r.).

17. Przy podawaniu daty dostępu do źródeł internetowych miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.
18. W tekście głównym należy podawać pełne imiona i nazwiska osób, które są wymieniane po raz pierwszy.
19. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp., jeśli są wymieniane w tekście po raz pierwszy.
20. Obce nazwy organizacji oraz skróty od nich utworzone powinny być pisane antykwą.
21. Nie należy stosować tzw. twardych spacji.
22. Ortografię i interpunkcję tekstu należy uwspółcześniać.
23. Wszelkie wyróżnienia w oryginalnym tekście dokumentu, dokonane przez jego twórcę, powinny być wyróżnione wytłuszczoną czcionką.
24. Nawiasy ukośne /…/ powinny być zamieniane na nawiasy okrągłe (…).
25. Skróty słownikowe należy pozostawiać bez rozwinięcia.
26. Uzupełnienia odautorskie, itp. należy podawać w nawiasach okrągłych antykwą.
27. Opuszczenia pochodzące od wydawcy powinny być zaznaczone trzema kropkami w nawiasie okrągłym.
28. Opuszczenia w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie okrągłym.
29. Redakcja nie zwraca autorom nadesłanych prac, a także zastrzega sobie prawo do ich skracania, adiustacji tekstów oraz zmiany tytułów i śródtytułów.
30. Redakcja zastrzega sobie możliwość odmowy przyjęcia artykułu bez podania przyczyn.
31. Redakcja zwraca uwagę, że *ghostwriting** i *guest authorship*** są przejawem nierzetelności naukowej, a wszelkie wykryte przypadki praktyk niezgodnych z zasadami etyki obowiązującej w nauce będą demaskowane (ujawniane) i dokumentowane, włącznie z powiadomieniem odpowiednich podmiotów (instytucji zatrudniających autorów, towarzystw naukowych, stowarzyszeń edytorów naukowych itp.). W celu przeciwdziałania występowaniu tych zjawisk Redakcja wymaga od poszczególnych autorów ujawnienia wkładu w powstanie publikacji.
32. Wersją pierwotną (referencyjną) czasopisma jest wydanie papierowe. „Przegląd Bezpieczeństwa Wewnętrznego" jest dostępny także na stronie internetowej Agencji Bezpieczeństwa Wewnętrznego w zakładce „PBW".

* Z *ghostwriting* mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie publikacji, ale jego udział jako autora nie zostaje ujawniony lub choćby uwzględniony w podziękowaniach dołączonych do tekstu.

** Sytuacja określana też jako *honorary authorship* – osoba podana jako autor czy współautor tekstu miała znikomy udział lub wcale nie uczestniczyła w tworzeniu publikacji.