PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 22 (12) 2020

INTERNAL SECURITY REVIEW

WARSAW 22 (12) 2020

Zespół redakcyjny Anna Przyborowska (redaktor naczelna)
Elżbieta Dąbrowska (sekretarz Redakcji)
Aneta Olkowska, Grażyna Osuchowska,
Anna Przyborowska (redakcja, korekta)
Agnieszka Dębska, Aneta Olkowska (skład)

Przekład artykułów na język angielski
Daniel Jedziniak
Agnieszka Osuchowska
Magdalena Popowska

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
Wersja online czasopisma jest dostępna na stronie www.abw.gov.pl
Wszystkie artykuły zamieszczone w numerze wyrażają poglądy autorów

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) można odnaleźć w Index Copernicus Journal Master List z liczbą 67,57 punktu. 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 i Edukacji
im. gen. dyw. Stefana Roweckiego „Grota" w Emowie
ul. Nadwiślańczyków 2, 05-462 Wiązowna

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 w kwietniu 2020 r.

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

SPIS TREŚCI

TABLE OF CONTENTS

I. ARTICLES AND DISSERTATIONS

II. REVIEWS

III. SELECTED ARTICLES IN ENGLISH

I

ARTYKUŁY I ROZPRAWY

ARTICLES
AND DISSERTATIONS

Dariusz Gradzi

FinTech/RegTech. Ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu wynikające z nowych technologii w obszarze płatności elektronicznych

W pierwszym kwartale 2019 r. odnotowano ponad 1,2 mld transakcji kartami debetowymi i ponad 100 mln kartami kredytowymi[1]. W drugim kwartale 2019 r. całkowita liczba transakcji bezgotówkowych wyniosła 1,43 mld, a ich wartość blisko 93 mld zł[2]. Badania pokazują, że najpopularniejszymi instrumentami płatniczymi są: karta płatnicza, rachunek bankowy z dostępem do konta przez internet i konto w serwisie PayPal[3]. W dobie nieodwracalnej digitalizacji sektora finansowego jest on szczególnie podatny na ryzyko związane z działalnością przestępczą, w tym terrorystyczną. Z tego powodu od wielu lat prowadzi się prace legislacyjne, których wynikiem są nowe regulacje. Mają one być odpowiedzią na zidentyfikowane zagrożenia. W praktyce jest jednak inaczej, ponieważ długość procesu legislacyjnego powoduje, że już w momencie wdrażania aktów prawnych nie są one dostosowane do zmieniającej się rzeczywistości.

Przeciwdziałanie praniu pieniędzy (ang. *anti money laundering*, AML) oraz finansowaniu terroryzmu (ang. *terrorist financing*, TF) w instytucjach finansowych jest normowane przez IV Dyrektywę AML (dalej: AMLD4)[4]. Integruje ona system AML/CTF (ang. *counter terrorist financing*, CTF – zwalczanie finansowania terroryzmu) z międzynarodowymi standardami zwalczania prania pieniędzy (ang. *money laundering*, ML) i finansowania terroryzmu, przyjętymi przez Financial Action Task Force (FATF)[5].

---

[1] *Informacja o kartach płatniczych. I kwartał 2019 r.*, https://www.nbp.pl/systemplatniczy/karty/q_01_2019.pdf, s. 6, 15 [dostęp: 4 XII 2019].

[2] *Informacja o kartach płatniczych. II kwartał 2019 r.*, https://www.nbp.pl/systemplatniczy/karty/q_02_2019.pdf, s. 16, 17 [dostęp: 4 XII 2019].

[3] Zob. *Raport. „Płatności cyfrowe" 2019*, https://eizba.pl/wp-content/uploads/2019/11/PLATNOSCI_CYFROWE_2019.pdf?fbclid=IwAR1ol9GL6K85vybNy5iwjoctd4k7YPFuT1rki_OpLjTwSqw1DFpGNkBoXBk [dostęp: 2 XII 2019].

[4] *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 25 maja 2015 w sprawie zapobiegania wykorzystywania systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE* (Dz. Urz. UE L 141 z 5 VI 2015 r., s. 73).

[5] Znana także jako Groupe d'action financière (GAFI) – międzynarodowa Grupa Specjalna ds. Przeciwdziałania Praniu Pieniędzy założona w 1989 r. Celem jej działania jest rozwój praktyk służących

Stosownie do tych standardów w AMLD4 przyjęto, jako zasadę, podejście oparte na ryzyku (ang. *risked-based approach*). Zakłada się w nim, że ryzyko ML/TF jest różne w poszczególnych krajach. Dlatego też państwa i ich organy nadzorcze (ang. *competent authorities*, CA) oraz uczestnicy obrotu prawnego muszą identyfikować ryzyko oraz na podstawie standardów zawartych w AMLD4 – nim zarządzać, tj. podejmować odpowiednie i adekwatne środki prawne. Dnia 30 maja 2018 r. została uchwalona V Dyrektywa AML (dalej: AMLD5), z datą implementowania przez państwa członkowskie UE do 10 stycznia 2020 r.[6] Europejska ocena ryzyka prania pieniędzy i finansowania terroryzmu[7] identyfikuje kilkadziesiąt produktów i usług potencjalnie narażonych na ryzyko ML/TF, w tym: bankowość prywatną, platformy crowdfundingowe (ang. *crowdfunding* – finansowanie społecznościowe[8]), waluty wirtualne, wartości majątkowe o właściwościach podobnych do gotówki, takie jak: złoto, diamenty.

Stosownie do regulacji ML/TF nie na każdy podmiot nałożono określone obowiązki prawne. Prawodawstwo AML/CTF dotyczy wyłącznie tzw. instytucji obowiązanych, za które – na gruncie polskiej ustawy o przeciwdziałaniu praniu pieniędzy[9] – uznaje się m.in. (w zakresie istotnym z punktu widzenia przedmiotu niniejszego opracowania):

- banki krajowe, oddziały banków zagranicznych, oddziały instytucji kredytowych, instytucje finansowe mające siedzibę na terytorium RP;
- spółdzielcze kasy oszczędnościowo-kredytowe oraz Krajową Spółdzielczą Kasę Oszczędnościowo-Kredytową;
- krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego, oddziały unijnych instytucji płatniczych, oddziały unijnych i zagranicznych instytucji pieniądza elektronicznego, małe instytucje płatnicze, biura usług płatniczych oraz agentów rozliczeniowych;
- firmy inwestycyjne, banki powiernicze;
- zagraniczne osoby prawne prowadzące na terytorium Rzeczpospolitej Polskiej działalność maklerską;
- spółki prowadzące rynek regulowany;

zwalczaniu prania pieniędzy. Organizacja publikuje rekomendacje na ten temat, http://www.fatf-gafi.org/about/ [dostęp: 2 XII 2019].

[6] *Dyrektywa PE i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE* (Dz. Urz. UE L 156 z 19 VI 2018 r., s. 43).

[7] *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf [dostęp: 4 XII 2019].

[8] Mechanizm crowdfundingu zakłada wynagrodzenie przez projektodawcę osób wpłacających pieniądze na rzecz projektu, w formie wcześniej ustalonej (przyp. red.).

[9] *Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (t.j: DzU z 2019 poz. 1115, ze zm.).

- fundusze inwestycyjne, alternatywne spółki inwestycyjne, towarzystwa funduszy inwestycyjnych, zarządzający alternatywnymi spółkami inwestycyjnymi;
- zakłady ubezpieczeń;
- Krajowy Depozyt Papierów Wartościowych S.A.;
- przedsiębiorców prowadzących działalność kantorową;
- podmioty prowadzące działalność gospodarczą polegającą na świadczeniu usług w zakresie:
  - wymiany walut wirtualnych na środki płatnicze,
  - wymiany pomiędzy walutami wirtualnymi,
  - pośrednictwa w wymianie, o której mowa powyżej,
  - prowadzenia rachunków;
- przedsiębiorców niebędących innymi instytucjami obowiązanymi, świadczących usługi polegające na:
  - tworzeniu osoby prawnej lub jednostki organizacyjnej nieposiadającej osobowości prawnej,
  - pełnieniu funkcji członka zarządu lub umożliwianiu innej osobie pełnienia tej funkcji, lub podobnej, w osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej,
  - zapewnieniu siedziby, adresu prowadzenia działalności lub adresu korespondencyjnego oraz innych pokrewnych usług osobie prawnej lub jednostce organizacyjnej nieposiadającej osobowości prawnej,
  - działaniu lub umożliwieniu innej osobie działania jako powiernik trustu, który powstał w drodze czynności prawnej,
  - działaniu lub umożliwieniu innej osobie działania jako wykonującej prawa z akcji lub udziałów na rzecz podmiotu innego niż spółka notowana na rynku regulowanym, podlegającym wymogom dotyczącym ujawniania informacji zgodnie z prawem UE lub podlegająca równoważnym standardom międzynarodowym;
- fundacje, w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- stowarzyszenia posiadające osobowość prawną, w zakresie, w jakim przyjmują lub dokonują płatności w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- przedsiębiorców, w zakresie, w jakim przyjmują lub dokonują płatności za towary w gotówce o wartości równej lub przekraczającej równowartość 10 tys. euro;
- instytucje pożyczkowe.

Ryzyko ogólne dotyczące sektora usług finansowych

Wspólna opinia Europejskich Organów Nadzorczych[10] na temat ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu, mającego wpływ na sektor finansowy Unii Europejskiej, dzieli ryzyko na: wspólne dla wszystkich sektorów usług finansowych oraz właściwe (specyficzne) tylko dla konkretnych sektorów[11]. Na podstawie powyższego dokumentu można wyróżnić następujące rodzaje ryzyka wspólnego dla wszystkich sektorów finansowych w Unii Europejskiej[12]:

- ryzyko wynikające z wycofania się Wielkiej Brytanii z UE (ang. *Brexit risk*),
- ryzyko związane z rozwojem nowych technologii (ang. *new technologies risk*),
- ryzyko związane z walutami wirtualnymi (ang. *virtual currencies risk*),
- ryzyko związane z rozbieżnością legislacyjną państw UE oraz odmiennymi praktykami nadzoru (ang. *legislative divergence risk and divergent supervisory practices risk*),
- ryzyko związane ze słabością kontroli wewnętrznej (ang. *weaknesses in internal controls risk*),
- ryzyko związane ze zjawiskiem de-riskingu (ang. *de-risking risk*)[13],
- ryzyko związane z finansowaniem terroryzmu (ang. *terrorist financing risk*).

Ryzyko wynikające z wycofania się Wielkiej Brytanii z UE[14]

Brexit niesie za sobą wyzwanie polegające na niepewności, czy organy nadzorcze państw członkowskich UE będą w stanie poradzić sobie ze sprawowaniem właściwego

[10] Ang. European Supervisory Authorities (ESA) – Europejskie Organy Nadzorcze. Na ESA składają się: European Securities and Markets Authority (ESMA) – europejski nadzór giełd i papierów wartościowych, European Insurance and Occupational Pensions Authority (EIOPA) – europejski nadzór ubezpieczeniowy i emerytalny oraz European Banking Authority (EBA) – europejski nadzór bankowy.

[11] *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector* (Wspólna opinia Europejskich Organów Nadzorczych w przedmiocie ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu wpływających na sektor finansowy UE, z 4 października 2019 r.), https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [dostęp: 2 XII 2019].

[12] Tamże, s. 1.

[13] Ang. *de-risking* oznacza ograniczenie lub całkowite zaprzestanie przez instytucje obowiązane prowadzenia działalności, z którą są związane obowiązki wynikające z AMLD4, co w praktyce oznacza odmowę świadczenia usług dla podmiotów z obszarów o zwiększonym ryzyku ML i TF.

[14] W dniu 27 marca 2017 r. Wielka Brytania wyraziła intencję wycofania się z UE. Po wycofaniu się tego kraju z UE – przy braku stosowych umów – będzie on traktowany jako tzw. kraj trzeci (ang. *third country*). To oznacza, że nie będą się do niego stosowały regulacje prawne UE, a to z kolei będzie miało bezpośredni wpływ na sektor finansowy. Będzie on traktowany tak samo jak podmioty z krajów trzecich z siedzibą w Wielkiej Brytanii. Praktycznie oznacza to niestosowanie zasady jednego paszportu (ang. *single passport*), zasady jednolitej licencji (ang. *single licence*) i możliwości świadczenia regulowanych usług na terytorium całej UE, po uzyskaniu zezwolenia

i efektywnego nadzoru nad instytucjami finansowymi po ich relokacji z Wielkiej Brytanii na terytoria państw członkowskich UE. Przy braku umowy międzynarodowej, która unormuje m.in. stosunki prawne między Wielką Brytanią a Unią Europejską, ten kraj nie będzie już – w znaczeniu prawnym – traktowany jako państwo członkowskie UE.

To ryzyko jest szczególnie istotne, ponieważ od wielu lat Wielka Brytania jest zagłębiem firm fintechowych[15]. Sektor FinTech[16] w Wielkiej Brytanii wytwarza ponad 6,6 mld funtów zysku. Działa tam ponad 1,6 tys. tego rodzaju firm[17], obecne są m.in. takie spółki technologiczne, jak: Revolut, TransferWise, Monzo, Starling Bank, Oak North czy Funding Circle. W samej tzw. piaskownicy regulacyjnej[18] (ang. *regulatory sandbox*) funkcjonuje ok. 300 fintechów[19].

Do niedawna Europejski Urząd Nadzoru Bankowego (European Banking Authority, EBA)[20] miał swoją siedzibę w Londynie, jednak w związku z niepewnym statusem Wielkiej Brytanii jako członka UE siedziba została przeniesiona do Paryża (skutek wszczęcia procedury brexitu)[21].

Wycofanie się Wielkiej Brytanii z UE stwarza wiele sytuacji zakwalifikowanych jako ryzyko ML/TF. Zaliczono do nich[22]:

- sprawowanie nieefektywnego nadzoru nowych podmiotów,

w jednym kraju członkowskim.

15 https://biznes.wprost.pl/technologie/fintech/10013258/brexit-czy-wielka-brytania-straci-pozycje-lidera-fintech.html [dostęp: 2 XII 2019].
Fintechy – firmy finansowe działające wyłącznie w sieci (przyp. red.).

16 Ang. *FinTech* oznacza zastosowanie innowacyjnych rozwiązań technologicznych dotyczących sektora finansowego, skutkujące powstaniem nowych modeli biznesowych. Zob. *Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention* (raport Financial Stability Board (FSB) w sprawie implikacji FinTechu dla stabilności finansowej), https://www.fsb.org/wp-content/uploads/R270617.pdf, s. 33 [dostęp: 2 XII 2019].

17 https://www.money.pl/gospodarka/great-fintech-czyli-jak-to-sie-robi-w-wielkiej-brytanii-6440365075797633a.html [dostęp: 2 XII 2019].

18 Jest to powszechnie stosowany przez organy nadzorcze środek mający na celu umożliwienie spółkom technologicznym testowanie nowych produktów i usług finansowych bez konieczności ubiegania się i uzyskania skomplikowanych, czasochłonnych i kosztochłonnych licencji od tych organów, https://www.cashless.pl/cashlesspedia/piaskownica-regulacyjna [dostęp: 2 XII 2019]; https://www.knf.gov.pl/en/MARKET/Fintech/Regulatory_Sandbox [dostęp: 2 XII 2019].

19 Zob. raport *UK FinTech. State of the Nation*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf [dostęp: 2 XII 2019].

20 Urząd UE sprawujący nadzór nad systemem bankowym Unii. EBA został powołany 1 I 2011 r. na podstawie *Rozporządzenia 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 XII 2010 r., s. 12).

21 https://www.consilium.europa.eu/en/policies/relocation-london-agencies-brexit/ [dostęp: 2 XII 2019].

22 *Joint Opinion of the European Supervisory Authorities*…, s. 10 [dostęp: 2 XII 2019].

- przeniesienie się podmiotów z Wielkiej Brytanii do innych państw członkowskich i konieczność dostosowania się przez te podmioty do nowych regulacji[23] oraz procedur *compliance*[24] (migracja regulacyjna),
- konieczność oceny wielu nowych podmiotów, ich modeli biznesowych, struktury własnościowej, organizacji kontroli wewnętrznej oraz ich monitoringu przez nowe organy nadzorcze,
- prowadzenie przez relokowane podmioty dalszej działalności w Wielkiej Brytanii, mających w państwach członkowskich UE wyłącznie formalne siedziby bez żadnych struktur (tzw. *shell companies* – spółki fasadowe),
- dostosowywanie się instytucji finansowych do procedury AML/CTF, gdyż po brexicie Wielka Brytania będzie tzw. państwem trzecim w rozumieniu AMLD4.

W przypadku wycofania się Wielkiej Brytanii z UE bez ratyfikowanej umowy lub przy braku porozumienia pomiędzy organami nadzorczymi Wielkiej Brytanii i UE, równoważnego takiej umowie, organy nadzorcze UE będą mogły, w ograniczonym zakresie, wymieniać informacje dotyczące przeciwdziałania ML/TF. Jeśli do brexitu dojdzie na podstawie umowy, wymiana informacji (która jest newralgiczna przy płatnościach elektronicznych, ponieważ bardzo często występują w nich elementy transgraniczne) będzie zależała od przyjętych warunków. W tej sprawie zawarto już tzw. *Memorandum of Understanding* (MoU)[25] pomiędzy europejskimi organami nadzoru a Financial Conduct Authority (FCA)[26].

Ryzyko związane z rozwojem nowych technologii[27]

Tego rodzaju ryzyko jest związane z nowymi dziedzinami FinTech oraz RegTech[28]. Przykładowymi rozwiązaniami fintechowymi są bezpieczne aplikacje mobilne[29]

---

[23] AMLD4 przewiduje pewne minimalne, wspólne standardy, a państwa członkowskie mają możliwość podwyższenia tych standardów przy implementacji AMLD.

[24] Ang. *compliance* jest rozumiane jako zapewnienie zgodności działań podmiotu z przepisami prawa oraz ich monitorowanie, https://www.rewi.europa-uni.de/pl/lehrstuhl/pr/poloerecht/projekte/Compliance/index.html [dostęp: 2 XII 2019].

[25] Memorandum określa zasady postępowania w przyszłości i wyraża wolę przyjęcia określonych zobowiązań, https://pressto.amu.edu.pl/index.php/cl/article/viewFile/6437/6458 [dostęp: 2 XII 2019]

[26] Odpowiednik polskiej Komisji Nadzoru Finansowego w Wielkiej Brytanii, https://www.fca.org.uk [dostęp: 2 XII 2019].

[27] *Joint Opinion of the European Supervisory Authorities*…, s. 12 [dostęp: 2 XII 2019].

[28] Ang. *RegTech* to zastosowanie nowych technologii służących wsparciu wymogów regulacyjnych i ich stosowaniu – definicja opracowana przez Międzynarodowy Instytut Finansów (ang. Institute of International Finance). Zob. https://www.iif.com/Innovation/Regtech [dostęp: 2 XII 2019]. Zob. też: *Financial Stability Implications from FinTech*…, s. 34 [dostęp: 2 XII 2019]. Trzeci termin (oprócz RegTech i FinTech) – ang. *InsureTech* – odnosi się do zastosowania nowoczesnych technologii w rozwiązaniach, które skutkują zwiększeniem funkcjonalności sektora ubezpieczeniowego.

[29] Aplikacje płatnicze do integracji z urządzeniami mobilnymi (np. telefon, iPad).

dla banków oraz usługi online (pożyczki) lub *factoring* online, w których cała procedura (np. udzielania kredytu) oraz ocena zdolności kredytowej (płatniczej) klienta odbywa się elektronicznie i zdalnie (ang. *remotely*), a podmioty oferujące te usługi korzystają m.in. z baz danych biur informacji gospodarczej, portali społecznościowych typu Facebook, LinkedIn lub Instagram.

Najważniejszymi podmiotami fintechowymi, które mają siedzibę w Polsce, są: PayU, Blue Media, Polish Payment Standard – Polski Standard Płatności (BLIK), Currency One, Finanteq, VoicePIN, ZenCard. Wśród zagranicznych można wyróżnić: Revolut[30] oraz N26[31].

Przykładami rozwiązań fintechowych z segmentu płatniczego są: system płatności BLIK[32], systemy płatności na urządzeniach mobilnych[33]: Google Pay, Apple Pay, Samsung Pay, a także płatności zbliżeniowe, niezwiązane lub związane z powyższymi systemami.

Z kolei narzędzia RegTech umożliwiają podmiotom szybsze, tańsze i łatwiejsze gromadzenie oraz analizowanie danych, do których weryfikacji są one zobowiązane[34]. Ma to szczególne znaczenie z punktu widzenia AML/TF (zwiększenie transparentności operacji finansowych). Przykładem może być automatyczna weryfikacja listy osób zajmujących eksponowane stanowiska polityczne (ang. *politically exposed person*, PEP), czyli – zgodnie z AMLD4 – m.in.: prezydentów, premierów, posłów, ministrów oraz członków ich rodzin. Jednym z rozwiązań RegTech jest interfejs programowania aplikacji (ang. *application programming interface*, API)[35] zaprojektowany dla konkretnej instytucji finansowej. To działanie wynika ze spełniania potrzeb danej instytucji lub dostarczania jej danych gospodarczych z wielu źródeł i takie ich zintegrowanie, aby ta instytucja finansowa, np. bank, otrzymała w jednym systemie wszystkie wymagane informacje[36].

Rozwój technologii otwiera nowe możliwości dla dostawców FinTech i RegTech, jednak niesie zagrożenia związane z ML/TF. Na podstawie wspomnianej już wspólnej

---

[30] https://www.revolut.com/pl-PL [dostęp: 2 XII 2019].

[31] https://n26.com/en-eu [dostęp: 2 XII 2019].

[32] https://blikmobile.pl [dostęp: 2 XII 2019].

[33] 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), https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf [dostęp: 4 X 2017].

[34] http://fintechpoland.com/pl/projects/raport-regtech-znaczenie-innowacji-regulacyjnych-dla-sektora-finansowego-i-panstwa/ [dostęp: 2 XII 2019]; https://medium.com/blog-transparent-data/co-to-jest-regtech-i-jak-ma-się-do-fintech-f27bab5a3a55 [dostęp: 2 XII 2019].

[35] Interfejs programowania aplikacji; zestaw reguł opisujący, w jaki sposób programy komputerowe się ze sobą komunikują.

[36] Np. system Transparent Data, https://transparentdata.pl [dostęp: 2 XII 2019].

opinii Europejskich Organów Nadzorczych można zidentyfikować następujące rodzaje ryzyka wynikające ze stosowania FinTech[37]:

- świadczenie usług w postaci nieregulowanych produktów finansowych, które nie wchodzą w zakres prawodawstwa AML/CTF,
- poprawność informacji gromadzonych podczas procesu oceny klienta (ang. *customer due diligence*, CDD),
- niezrozumienie przez dostawców innowacyjnych technologii FinTech wymagań AML/CTF oraz pozostałych regulacji,
- różnice w kulturze *compliance*[38] pomiędzy nadzorowanymi podmiotami,
- powstawanie nowych technologii służących do zdalnego nawiązywania relacji z klientem (tzw. *onboarding*), bez zachowania środków bezpieczeństwa w zakresie zwalczania cyberprzestępczości oraz kradzieży tożsamości,
- zbytnie poleganie przez instytucje finansowe (np. banki) na *outsourcingu*[39] z fintechami, bez przykładania należytego znaczenia do mechanizmów ich kontroli (zjawisko powszechne w Polsce).

Przy wprowadzaniu nowych technologii wspomagających RegTech może wystąpić ryzyko związane z[40]:

- bezkrytycznym poleganiem firm na rozwiązaniach technologicznych, które może prowadzić do ograniczenia zaangażowania się ludzi w monitorowanie transakcji;
- brakiem regulacji prawnych w zakresie RegTech;
- niezrozumieniem nowych technologii wykorzystywanych w procesie oceny klientów, co czyni wprowadzające je podmioty podatnymi na zagrożenia ML/TF;
- zbytnim poleganiem na podmiotach, którym przekazano możliwość korzystania z pewnych procesów (zasada czystych rąk), bez należytego wglądu w ich działalność i procedury, co w konsekwencji może prowadzić do:
  - trudności w ocenie danych klienta,
  - wątpliwości w zakresie wiarygodności danych (rekordów), spowodowanych niebezpiecznymi praktykami ich pozyskiwania i przechowywania przez dostawców RegTech;
- brakiem transparentności przy przeniesieniu odpowiedzialności pomiędzy dostawcami RegTech, szczególnie gdy procesy zostały im przekazane na podstawie umowy *outsourcingowej* i te podmioty nie są instytucjami obowiązanymi na podstawie AMLD4.

---

[37] *Wspólna Opinia Europejskich Organów Nadzorczych*…, s. 12 [dostęp: 2 XII 2019].

[38] Zapewnienie zgodności działalności z regulacjami prawnymi, normami bądź zaleceniami (przyp. red.).

[39] Skrót od ang. słów: *outside-resource-using*. *Outsourcing* polega na przekazywaniu zadań, funkcji, projektów i procesów do realizacji firmie zewnętrznej (przyp. red.).

[40] *Joint Opinion of the European Supervisory Authorities*…, s. 13 [dostęp: 2 XII 2019].

Wymienione sytuacje stwarzające zagrożenie zostały opisane w opinii Europejskich Organów Nadzorczych (European Supervisory Authorities, ESA) dotyczącej używania innowacyjnych rozwiązań odnoszących się do CDD[41].

Transakcje finansowe zostały w pełni zdigitalizowane, co dostawcy różnych usług muszą uwzględnić, zwłaszcza że te zmiany istotnie zwiększają ryzyko ML/TF. Analiza profilu klienta ma podstawowe znaczenie z punktu widzenia obowiązków AML w zakresie identyfikacji i weryfikacji klienta. Można wyróżnić następujące rodzaje innowacyjnych rozwiązań przy ocenie klienta[42]:

- rozwiązania weryfikacyjne *non-face-to-face*, na podstawie tradycyjnych dokumentów tożsamości (paszport, prawo jazdy) z wykorzystaniem urządzeń mobilnych (np. smartfonu),
- rozwiązania weryfikacyjne oparte na centralnych repozytoriach dokumentów identyfikacyjnych (tworzonych jako przedsięwzięcia wspólne dla wielu firm lub zlecane zewnętrznemu partnerowi),
- rozwiązania, których podstawą jest sztuczna inteligencja (ang. *artificial intelligence*, AI) przetwarzająca znaczną ilość informacji z różnych źródeł, w różnych językach. Dzięki tym systemom można przeanalizować np. historię transakcji, lokalizację GPS, portale społecznościowe, publikacje internetowe, rejestry beneficjentów rzeczywistych, osób zajmujących eksponowane stanowiska polityczne lub członków ich rodzin. Pozwalają one także na zdalne wykrycie fałszywych dokumentów identyfikacyjnych na podstawie cech tych dokumentów (znaki wodne, fotografie, linie wrażliwe na promienie UV, układ graficzny dokumentu).

Ryzyko związane z walutami wirtualnymi

Milton Friedman zauważył, że: (…) *Internet stanie się jedną z głównych sił redukujących rolę rządów. Jedyną rzeczą, której nam brakuje, ale która z całą pewnością wkrótce zostanie rozwinięta, jest prawdziwa e-gotówka – metoda, dzięki której można przekazać poprzez Internet środki pomiędzy podmiotami A i B, przy czym zarówno podmiot A nie zna B, jak i podmiot B nie zna A*[43].

W płatniczym systemie finansowym można wyróżnić[44] następujące modele obrotu walutami:

---

[41] Zob. *Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process* (*Opinia o korzystaniu z innowacyjnych rozwiązań w procesie oceny profilu klienta przez instytucje kredytowe i finansowe*), https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf [dostęp: 2 XII 2019].

[42] Tamże, s. 5.

[43] Cyt. za A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, s. 7.

[44] Tamże, s. 19.

- scentralizowany: istnieje jeden podmiot odpowiadający za emisję i kontrolę obrotu określoną walutą. Transakcje są realizowane wyłącznie za pośrednictwem tego podmiotu, który prowadzi rejestr wszystkich transakcji,
- zdecentralizowany: podmiot centralny przekazuje podległym mu strukturom część kompetencji i zadań do wykonania,
- rozproszony: nie występuje hierarchizacja. Żadna z jednostek nie pozostaje wobec innej jednostki w relacji: nadrzędność–podrzędność. Nie ma również żadnej jednostki centralnej. Każdy uczestnik obrotu ma możliwość kontaktu z pozostałymi. Może on być również emitentem waluty, może uczestniczyć w kontroli i nadzorze obrotu oraz dysponować rejestrem wszystkich transakcji w systemie (będącym właściwym dla obrotu walutami wirtualnymi).

Na system płatniczy składa się określona grupa instytucji i procedur wykorzystywanych do zapewnienia sprawnego obiegu pieniądza na danym obszarze geograficznym[45].

W ramach systemu płatniczego należy wyróżnić cztery poziomy aktywności uczestników:

- poziom pierwszy – podmioty będące stronami dokonywanych transakcji płatniczych,
- poziom drugi – podmioty bezpośrednie obsługujące procesowanie transakcji pomiędzy uczestnikami poziomu pierwszego; są to dostawcy usług płatniczych, np. banki i instytucje płatnicze,
- poziom trzeci – podmioty uczestniczące w rozliczaniu transakcji pomiędzy uczestnikami poziomu drugiego (np. polska Krajowa Izba Rozliczeniowa),
- poziom czwarty – podmioty przechowujące środki pieniężne dostawców usług płatniczych lub papiery wartościowe (np. Narodowy Bank Polski oraz Krajowy Depozyt Papierów Wartościowych).

W systemie płatniczym należy wyróżnić[46]:

- system płatności wysokokwotowych;
- system płatności detalicznych (retailowych, ang. *retail* – handel detaliczny), na który składają się:
  - podsystem płatności kartowych,
  - podsystem płatności mobilnych,
  - podsystem płatności natychmiastowych;
- system rozrachunku papierów wartościowych.

Waluty wirtualne (ang. *virtual currencies*, VC) nie są regulowanymi produktami finansowymi w UE, co powoduje narażenie klientów na ryzyko, które często jest niemożliwe do przewidzenia, a ich katalog jest otwarty[47]. Z uwagi na brak regulacji

[45] Tamże, s. 79.

[46] Tamże.

[47] Zob. *EBA Opinion on 'virtual currencies'* (Opinia EBA o walutach wirtualnych, z 4 lutego 2014 r.), https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b-94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20

na szczeblu UE ochrona w tym zakresie powinna spoczywać na krajowych organach nadzorczych. Europejski Urząd Nadzoru Bankowego od lat publikuje raporty wskazujące na zagrożenia związane z obrotem walutami wirtualnymi[48].

Powszechnie przyjmuje się podział walut wirtualnych na[49]:

- żetony – akceptowane głównie przez członków wirtualnych społeczności, które są emitowane i kontrolowane przez jego twórców, np. autorów gier komputerowych (żetony: Facebook Credits, Amazon Coins, które są scentralizowanymi walutami wirtualnymi); w tym przypadku emitent jest instytucją kontrolującą sferę podażową (emisję) oraz autoryzuje i rozlicza transakcje,
- kryptowaluty.

Europejski Bank Centralny definiuje kryptowaluty jako: (…) *cyfrowo prezentowaną wartość, która nie została wyemitowana przez bank centralny, instytucję kredytową, jak i instytucję pieniądza elektronicznego, która w pewnych okolicznościach, może być wykorzystana jako alternatywa wobec pieniądza*[50].

Najbardziej znanym przykładem waluty wirtualnej jest bitcoin. Za jego twórcę uznaje się osobę (lub osoby) o pseudonimie Satoshi Nakamoto, w której zamyśle bitcoin miał pozwalać na realizowanie bezpośrednich i anonimowych transakcji w handlu elektronicznym[51]. Ten system miał być niezależny od tradycyjnych instytucji finansowych, a operacje finansowe miały się odbywać w całkowitej separacji od ogólnoświatowych systemów finansowych oraz centralnych systemów rozliczeniowych.

David Chaum jest postrzegany jako „ojciec pieniądza cyfrowego" i „ojciec anonimowości w Internecie"[52]. Przedstawił on scentralizowany system anonimowych płatności zwiększających bezpieczeństwo i prywatność użytkowników w stosunku do innych systemów istniejących w tym czasie. W 1982 r. opublikował pracę *Blind signatures for untraceable payments*, w której opisał naruszanie prywatności przez istniejące systemy rozliczeń[53]. Podstawą założeń Chauma była konieczność ograniczenia wiedzy pośrednika finansowego na temat czasu, wartości i przedmiotu płatności,

Currencies.pdf?retry=1 [dostęp: 2 XII 2019].

[48] http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf; https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD; https://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf [dostęp: 2 XII 2019].

[49] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 15.

[50] Tamże, s. 25.

[51] Tamże, s. 34–37. Założenia bitcoina zostały przedstawione w pracy *Bitcoin: A Peer-to-Peer Electronic Cash System*, autorstwa anonimowego autora o pseudonimie Satoshi Nakamoto. Uważa się jednak, że pod tym pseudonimem kryją się korporacje technologiczne: SAmsung, TOSHIba, NAKAmichi, MOTOrola.

[52] Tamże, s. 30.

[53] Tamże.

a także możliwości analizy zbyt wielu metadanych (ang. *big data*[54]). Dla pośrednika finansowego zbędne – z punktu widzenia płatności – są dane dotyczące: lokalizacji osoby, jej stylu życia (m.in. informacje o podróżach, opłacanych hotelach, rachunkach z restauracji, drobnych wydatkach, żywności, lekach, prasie, wsparciu instytucji politycznych i religijnych). Chum opracował tzw. ślepy podpis (podpis cyfrowy, nowy rodzaj kryptografii). To rozwiązanie prowadziło do uzyskania tzw. asymetrycznej anonimowości, w której płatnik był nieznany, ale osoba przyjmująca płatność mogła zostać zidentyfikowana, jeżeli zaszła taka potrzeba. Wadą tego rozwiązania była podatność na tzw. *double-spending*, tj. możliwość podwójnego wydatkowania tych samych środków[55].

W rozwoju kryptowalut nie można pominąć także tzw. ruchu *cypherpunk*[56], dla którego zwolenników prywatność była podstawą nowoczesnego i cyfrowego społeczeństwa. Nie wierzono, że zostanie ona zapewniona przez rządy. Mogła zostać zachowana wyłącznie dzięki zastosowaniu narzędzi szyfrujących i zdecentralizowanemu systemowi komunikacji. Pod wpływem tego ruchu jeden z jego członków przedstawił w 1998 r. projekt anonimowej waluty cyfrowej *b-money*. Podstawą dobrze funkcjonującego społeczeństwa cyfrowego było istnienie sprawnie działającego środka wymiany (pieniądza) oraz efektywnych sposobów egzekwowania umów. Najważniejszym elementem ruchu *cypherpunk* był projekt zasad dokonywania transakcji płatniczych bez udziału pośredników. Założono w nim, że wszystkie transakcje będą zapisywane w rejestrze, którego kopię ma każdy z jego uczestników. Dzięki temu taki rejestr jest niemożliwy do sfałszowania[57]. Powyższe koncepcje doprowadziły do powstania w 2008 r. kryptowaluty bitcoin, która została uruchomiona w 2009 r.

Waluty wirtualne a pieniądz elektroniczny[58]

Waluty wirtualne są często błędnie utożsamiane z tzw. pieniądzem elektronicznym[59]. Różnica między nimi poza sferą regulacyjną sprowadza się do tego, że waluta

[54] Używanie zaawansowanych technik w celu analizowania dużych zasobów zdywersyfikowanych danych, które mogą nie być ustrukturyzowane i mogą pochodzić z różnych źródeł, https://www.ibm.com/analytics/hadoop/big-data-analytics [dostęp: 2 XII 2019].

[55] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 30–31.

[56] *Cypherpunks* – działacze propagujący powszechne stosowanie silnej kryptografii jako drogi do zmian społecznych i politycznych. Pierwotnie tworzyli oni nieformalną grupę komunikującą się za pośrednictwem list dyskusyjnych, która za cel stawiała siebie osiągnięcie prywatności i bezpieczeństwa przez aktywne wykorzystanie kryptografii, za: https://pl.wikipedia.org/wiki/Cypherpunk [dostęp: 17 II 2010] – przyp. red.

[57] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 32–33.

[58] Komisja Nadzoru Finansowego w piśmie do banków z 10 lipca 2015 r. dokonała analizy prawnej emisji pieniądza elektronicznego, https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 2 XII 2019].

[59] W rozumieniu *Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych* (t.j.: DzU z 2019 r.

wirtualna jest sztuczną jednostką rozliczeniową, podczas gdy jednostka rozliczeniowa pieniądza elektronicznego jest wyrażona w jednostce mającej status prawnego środka płatniczego. Waluty wirtualne natomiast nie muszą mieć związku z pieniądzem tradycyjnym (ang. *fiat currency*, FC), nie musi on też być ich podstawą.

Czynnikiem wyróżniającym kryptowaluty pod względem technologicznym jest dostępność kodu źródłowego oraz otwarte oprogramowanie (ang. *open source*)[60]. Za zakwalifikowaniem danego instrumentu do kryptowalut przemawia zastosowanie rozproszonego systemu transakcji oraz oparcie konstrukcji na kryptografii. Musi też istnieć globalna, publiczna oraz rozproszona baza danych obejmująca zrealizowane transakcje przy użyciu kryptowaluty.

Podstawą bitcoina było otwarte oprogramowanie, czyli ogólnie dostępny kod źródłowy, dzięki czemu wszyscy mogli go na bieżąco analizować i ulepszać. Bitcoin umożliwiał również procesowanie bezpośrednich transakcji pomiędzy użytkownikami Internetu, wykorzystując protokół komunikacyjny osoba do osoby (ang. *peer-to-peer*, także: *person-to-person*, P2P[61]). To oznacza brak konieczności funkcjonowania centralnego serwera (repozytorium informacji o transakcjach) oraz brak potrzeby korzystania z pośrednika transakcji[62]. Nie występuje zatem pośrednictwo tzw. zaufanej trzeciej strony.

Transakcje bitcoinami są zapisywane w blokach, które następnie łączą się w łańcuch bloków, tj. zapis zatwierdzonych transakcji (ang. *blockchain*[63]). Te zapisy składają się na publiczną księgę (ang. *public ledger*), bazę danych, przechowywaną przez wszystkie komputery użytkowników sieci bitcoin. Nowatorstwo tego systemu polega na utworzeniu łańcucha bloków funkcjonujących w ramach publicznego rozproszonego rejestru transakcji dokonywanych bitcoinami, w którym niemożliwe jest wycofanie transakcji. Jest to korzystne dla akceptantów płatności (np. sklepu przyjmującego płatność w kryptowalucie), ale może być ryzykowne dla płatnika[64].

W systemie bitcoin nie funkcjonuje żadna jednostka centralna ani organy nadzorcze. Struktura użytkowników systemu bitcoin składa się z dwóch poziomów: poziom

poz. 659, ze zm.) oraz *Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE* (Dz. Urz. UE L 267 z 10 X 2009 r., s. 7).

[60] Oprogramowanie, które zezwala na używanie ich kodu źródłowego, https://pl.wikipedia.org/wiki/Otwarte_oprogramowanie [dostęp: 2 XII 2019].

[61] Oznacza on równorzędność uczestników sieci, tj. każdy komputer podłączony do sieci może wysyłać i odbierać dane w sieci, co umożliwia pobieranie plików oraz ich udostępnienie komputerom podłączonym do tej sieci, https://poradnikprzedsiebiorcy.pl/-peer-to-peer-definicja-historia-powstania-i-wplyw-na-rozwoj-internetu-cz-1 [dostęp: 2 XII 2019].

[62] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 35.

[63] https://blockgeeks.com/guides/what-is-blockchain-technology/ [dostęp: 2 XII 2019]; https://pl.wikipedia.org/wiki/Blockchain [dostęp: 2 XII 2019].

[64] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 51–53.

pierwszy obejmuje użytkowników – akceptantów, drugi – podmioty wspomagające procesowanie transakcji, jak pośrednicy płatności oraz platformy obrotu kryptowalutami.

Wszystkie platformy obrotu kryptowalutami są na liście ostrzeżeń publicznych Komisji Nadzoru Finansowego[65]. Do czasu objęcia ich przepisami AMLD4 nie musiały one stosować żadnych środków AML/CTF (w tym identyfikować i weryfikować klienta). Niejednokrotnie prowadziło to do sytuacji, w której środki pochodzące z tzw. nieautoryzowanych transakcji płatniczych wskutek przywłaszczenia danych dostępowych do rachunku bankowego (tzw. credentiali, ang. *credential* – poświadczenie) były przez systemy płatności natychmiast transferowane na te platformy i następnie lokowane w bitcoiny. Dzięki takiemu zabiegowi w zasadzie nie jest możliwe ustalenie sprawców przywłaszczeń i pociągniecie ich do odpowiedzialności karnej, dlatego postępowania były umarzane na etapie postępowań przygotowawczych w sprawie.

Bitcoin – przetwarzanie transakcji i wymiar prawny

Jednym z większych problemów transakcji w systemie bitcoin jest jego przepustowość. Szacuje się ją na poziomie jednej transakcji na sekundę lub maksymalnie siedmiu transakcji na sekundę. Dla porównania, średnia liczba transakcji na sekundę w usłudze PayPal wynosi 100, w Visie – 2 tys., przy czym maksymalna wydajność tego systemu wynosi 56 tys. transakcji na sekundę. Wykonywanie jednej transakcji w systemie bitcoin trwa od kilkunastu minut do godziny. Zarzutem kierowanym pod adresem tego systemu jest jego duża energochłonność. Funkcjonowanie systemu wymaga bowiem nieustannego dostarczania energii do urządzeń, a zapotrzebowanie na energię wzrasta wraz z rozwojem sieci. Szacunki wskazują, że jedna transakcja w systemie bitcoin pochłania średnie dzienne zapotrzebowanie na energię elektryczną półtora gospodarstwa domowego w USA, a dzienne koszty energii zużywanej przez ten system sięgają 15 mln dolarów. System bitcoina cechuje także pseudoanonimowość, którą należy wiązać z publicznym udostępnieniem zapisu o zrealizowanych transakcjach. Umożliwia to śledzenie i analizowanie transakcji oznaczonych konkretnym adresem IP komputera. Istotnym mankamentem jest protokół kryptograficzny. Dotychczas nie został on złamany, jednak teoretycznie jest to możliwe. Taka sytuacja może wystąpić, gdy ktoś uzyska więcej niż 50 proc. mocy obliczeniowej systemu. Może to doprowadzić do zmiany aktualnego stanu równowagi blockchain[66] i wielokrotnego wydawania tych samych jednostek wartości[67].

Aktywa (prawa) kryptograficzne są definiowane[68] jako wartości oparte na kryptografii i technologii rozproszonych rejestrów (ang. *distributed ledger technology*, DLT),

[65] Lista jest dostępna pod linkiem https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne [dostęp: 2 XII 2019].

[66] Zob. szerzej: https://www.bbva.com/en/difference-dlt-blockchain/, https://101blockchains.com/blockchain-vs-distributed-ledger-technology/ [dostęp: 2 XII 2019].

[67] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 123–127.

[68] Zob. *EBA reports on crypto-assets* (Raport EBA o kryptoaktywach, z 9 stycznia 2019 r.),

której jednym z przykładów jest blockchain. DLT to rozproszona baza danych z rejestrami, które można replikować. Są one współdzielone i zsynchronizowane wśród użytkowników[69].

Technologia blockchain (rozumiana jako jeden z rodzajów DLT) jest używana przede wszystkim do transferu bitcoinów pomiędzy osobami, przy użyciu kluczy prywatnych (służących do kontroli własności jednostek bitcoin) i publicznych. Do rejestrowania transferu jednostek bitcoin jest wykorzystywana DLT. W przypadku wygenerowania transakcji jest ona rozpowszechniana w całej sieci DLT, co – przy użyciu klucza prywatnego – pozwala zweryfikować, czy zbywca jest właścicielem jednostek bitcoin. DLT umożliwia przechowywanie, aktualizowanie i weryfikowanie informacji w sposób zdecentralizowany[70].

Obrót walutami wirtualnymi jest narażony na ryzyko prania brudnych pieniędzy i finansowania terroryzmu, czemu można zaradzić, uznając podmioty prowadzące taką działalność gospodarczą za instytucje obowiązane[71]. Dotyczy to świadczenia usług w zakresie:

- wymiany walut wirtualnych na środki płatnicze,
- wymiany pomiędzy walutami wirtualnymi,
- pośrednictwa w wymianach, o których mowa powyżej,
- prowadzenia rachunków w formie elektronicznej jako zbioru danych identyfikacyjnych, zapewniających osobom uprawnionym możliwość korzystania z jednostek walut wirtualnych, w tym przeprowadzania transakcji ich wymiany.

W dyrektywie AMLD5 za instytucje obowiązane uznano dostawców kont waluty wirtualnej[72] (ang. *included custodian wallet provider*). Wprowadzono tu także definicję legalną walut wirtualnych. Określono je jako cyfrowe wyznaczniki wartości, które nie są emitowane ani gwarantowane przez bank centralny lub organ publiczny i nie muszą być powiązane z walutą prawnie obowiązującą, a także nie mają prawnego statusu waluty lub pieniądza, ale są akceptowane przez osoby fizyczne lub prawne jako środek wymiany i mogą być przekazywane, przechowywane lub sprzedawane drogą elektroniczną. W Polsce pod pojęciem „waluty wirtualne" rozumie się cyfrowe odwzorowanie wartości, którymi nie są[73]:

- prawne środki płatnicze emitowane przez NBP, zagraniczne banki centralne lub inne organy administracji publicznej,

https://eba.europa.eu/eba-reports-on-crypto-assets [dostęp: 2 XII 2019].

69 https://pl.wikipedia.org/wiki/Technologia_rozproszonego_rejestru [dostęp: 2 XII 2019].

70 A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, s. 51–53.

71 Art. 2 ust. 1 pkt 12 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

72 Art. 3 pkt 19 AMLD5. Przez dostawcę kont waluty wirtualnej rozumie się podmiot świadczący usługi polegające na przechowywaniu prywatnych danych uwierzytelniających w imieniu swoich klientów na potrzeby posiadania, przechowywania i przekazywania walut wirtualnych.

73 Art. 2 ust. 1 pkt 26 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

- międzynarodowe jednostki rozrachunkowe, ustanawiane przez organizację międzynarodową i akceptowane przez poszczególne kraje należące do tej organizacji lub z nią współpracujące,
- pieniądze elektroniczne, w rozumieniu ustawy o usługach płatniczych[74],
- instrumenty finansowe, w rozumieniu ustawy o obrocie instrumentami finansowymi[75],
- weksle lub czeki wymienialne w obrocie gospodarczym na prawne środki płatnicze i akceptowane jako środek wymiany.

Waluty wirtualne zalicza się do tzw. wartości majątkowych[76], do których należą także prawa majątkowe, inne mienie ruchome lub nieruchomości, środki płatnicze, instrumenty finansowe w rozumieniu ustawy o obrocie instrumentami finansowymi, inne papiery wartościowe oraz wartości dewizowe.

Europejski Urząd Nadzoru Bankowego oraz Europejski Urząd Nadzoru Giełd i Papierów Wartościowych (European Securities and Markets Authority, ESMA[77]) opublikowały raport na temat zastosowania prawa UE do kryptoaktywów majątkowych (ang. *crypto-assets*)[78]. Na podstawie powyższego raportu można wymienić następujące zagrożenia związane z walutami wirtualnymi:

- brak wiedzy na temat funkcjonowania dostawców walut wirtualnych oraz ich produktów,
- rosnąca liczba transakcji online ze znikomą identyfikacją i weryfikacją klienta.

W 2018 r. FATF przyjął rekomendację (Rekomendacja 15[79]) mającą na celu włączenie do Rekomendacji definicji „*virtual assets*" i „*virtual assets service providers*". W konsekwencji w stosunku do tych aktywów i podmiotów obowiązuje obecnie prawodawstwo UE w zakresie przeciwdziałania praniu pieniędzy i zwalczania finansowania terroryzmu. Kryptoaktywa oznaczają:

- aktywa oparte na kryptografii i DLT lub zbliżonych technologiach,
- aktywa, które nie są używane i gwarantowane przez bank lub władze publiczne,
- aktywa, które mogą być wymieniane i stosowane w celach inwestycyjnych lub ułatwiających dostęp do dóbr i usług.

Przyjmuje się, że waluty wirtualne mogą spełniać prawne kryteria dla pieniądza elektronicznego i podlegać wszystkim wymogom regulacyjnym dotyczącym pieniądza tego rodzaju, w przypadku gdy:

---

[74] *Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych* (t.j.: DzU z 2019 r. poz. 659, ze zm.).

[75] *Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi* (t.j.: DzU z 2018 r. poz. 2286, ze zm.).

[76] Art. 2 ust. 2 pkt 27 ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu.

[77] https://www.esma.europa.eu/about-esma/esma-in-short/whos-who [dostęp: 2 XII 2019].

[78] Zob. *Advice: initial coin offerings and crypto-assets*, ESMA50-157-1391, z 9 I 2019 r., https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf [dostęp: 2 XII 2019].

[79] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html [dostęp: 2 XII 2019].

- są przechowywane elektronicznie,
- mają wartość pieniężną,
- zawierają w sobie określone roszczenia do wydawcy walut wirtualnych,
- są wydawane w zamian za otrzymane środki,
- są wydawane w celu dokonywania płatności,
- są akceptowane przez inne podmioty, niebędące tylko wydawcą.

Waluty wirtualne są definiowane przez EBA jako[80]:

- mające wymiar cyfrowy swojej wartości (ang. *digital representation of value*), co nie wyłącza możliwości istnienia fizycznego odpowiednika,
- nieemitowane przez bank centralny lub inny organ władzy publicznej,
- niemające związku z tradycyjną walutą,
- akceptowalne przez osoby prawne i fizyczne jak środek płatniczy,
- te, które można przekazywać, przechowywać lub zbywać elektronicznie.

W *Opinii…* EBA zidentyfikowano około 70 szczegółowych rodzajów ryzyka związanych z walutami wirtualnymi, m.in.:[81]

- ryzyko dla użytkowników (ang. *risks to users*),
- ryzyko dla innych uczestników (ang. *risks to other market participants*),
- ryzyko dla integralności finansowej (ang. *risks to financial integrity*),
- ryzyko dla systemów płatności w walutach tradycyjnych (ang. *risks to payment systems in fiat currencies*),
- ryzyko dla regulatorów i organów nadzorczych (ang. *risks to regulators*).

Ryzyko związane z rozbieżnością legislacyjną państw UE oraz odmiennymi praktykami organów nadzorczych

To ryzyko wynika z zasady minimalnej harmonizacji[82] uwzględnionej w dyrektywach UE. Jest ono też zwiększane przez odmienną implementację[83] dyrektyw AMLD do prawnych porządków państw członkowskich.

Różnice w spójnym stosowaniu aktów prawnych dotyczących przeciwdziałania praniu pieniędzy dodatkowo są pogłębiane przez rozbieżne praktyki organów nadzorczych w państwach członkowskich w odniesieniu do tych samych zagadnień. Różnice w tych praktykach mogą wynikać z:

- innego podejścia opartego na ryzyku,
- odmiennego rozumienia ryzyka ML/TF przez organy nadzorcze,

[80] Zob. *EBA Opinion on 'virtual*…, s. 11; *EBA reports on crypto-assets*…

[81] Tamże, s. 5.

[82] Minimalna harmonizacja oznacza, że prawodawca unijny wyznacza wspólny i minimalny standard regulacji danego obszaru, https://www.eversheds-sutherland.com/documents/global/poland/articles_pdf/pl/2011-12-01_eps_prawo_konsumenckie_ue_dyrekywy_oparte_na_harmonizacji_minimalnej_akunkiel.pdf, s. 46 [dostęp: 2 XII 2019].

[83] Wprowadzenie dyrektywy UE do krajowego porządku prawnego.

- różnych środków zaangażowanych w nadzór ML/TF w poszczególnych państwach członkowskich.

Zagrożenia płynące z odmienności w zakresie legislacji powodują, że niektóre podmioty uzyskują zezwolenia w krajach podchodzących bardziej liberalnie do tego procederu, co wiąże się ze świadczeniem przez te podmioty usług w innych państwach członkowskich UE.

W pewnych krajach przepisy AML zostały w taki sposób implementowane, że organy nadzorcze nie mogą działać dopóty, dopóki nie znajdą dowodu działalności przestępczej. Z uwagi na obowiązującą zasadę jednolitego paszportu takie praktyki organów nadzorczych są szczególnym zagrożeniem, ponieważ jeżeli podmiot raz uzyska zezwolenia, może on swoją działalnością zagrażać innym rynkom państw członkowskich.

Na gruncie poprzednich dyrektyw AML nie było wprost wyartykułowanego obowiązku współpracy pomiędzy organami informacji finansowej poszczególnych państw w zakresie wymiany informacji. Z tego też powodu istniało ryzyko, że te organy mają tylko częściowy ogląd sytuacji ML/TF. Inaczej zostało to przedstawione w AMLD5. Te przepisy będą uzupełnione wytycznymi co do współpracy oraz wielostronnych umów o wymianie informacji.

Ryzyko wynikające z rozbieżnych praktyk nadzorczych[84]

Komitet Moneyval[85] i FATF od dłuższego czasu kwestionowały niektóre praktyki AML/CTF wybranych państw odnośnie ich adekwatności do występujących zagrożeń prania pieniędzy i finansowania terroryzmu. Europejski Urząd Nadzoru Bankowego sformułował przeciwko jednemu z nadzorców zarzuty dotyczące naruszenia prawa UE[86] w związku z niewywiązywaniem się z wymagań przeciwdziałania praniu pieniędzy.

Odmienne podejścia organów nadzoru do podmiotów nadzorowanych wynikają z:

- różnic w poziomach ryzyka,
- bezkrytycznego przyjmowania podejścia organów innych państw członkowskich w określonych sektorach do szacowanego ryzyka,
- różnic w wyszkoleniu personelu zwalczającego ML/FT.

---

[84] *Joint Opinion of the European Supervisory Authorities*…, s. 17 [dostęp: 2 XII 2019].

[85] Działający przy Radzie Europy komitet do oceny środków przeciwdziałających praniu pieniędzy i finansowaniu terroryzmu, https://www.coe.int/en/web/moneyval/ [dostęp: 2 XII 2019].
Pełna nazwa: Komitet Specjalny Ekspertów Rady Europy ds. Oceny Środków Przeciwdziałania Praniu Pieniędzy w Krajach Europy Środkowej i Wschodniej funkcjonujący w ramach Rady Europy, będący tzw. ciałem regionalnym FATF, za: https://www.kic.gov.pl/pl/documents/764034/1002265/20120911_MONEYVAL_inf.pdf [dostęp: 18 II 2020] – przyp. red.

[86] Rekomendacja dotyczyła maltańskiej jednostki analityki finansowej, https://www.eba.europa.eu/-/eba-issues-recommendation-to-the-maltese-financial-intelligence-analysis-unit-in-relation-to-its-supervision-of-pilatus-bank [dostęp: 2 XII 2019].

Ryzyko związane ze słabością kontroli wewnętrznej[87]

To ryzyko wynika ze słabej implementacji środków identyfikacji i weryfikacji klienta korzystającego z systemu bankowego. Jednym z głównych założeń AMLD4 było wprowadzenie przez instytucje obowiązane systemów kontroli wewnętrznej dopasowanych do ryzyka, na które jest narażony dany podmiot w związku ze swoją działalnością.

Jakkolwiek organy nadzorcze stoją na stanowisku, że w podmiotach nadzorowanych wprowadzono odpowiednie systemy kontroli wewnętrznej, szczególnie w zakresie rejestrowania transakcji, identyfikacji i weryfikacji klienta oraz raportowania transakcji podejrzanych, to dane otrzymywane przez Europejskie Organy Nadzorcze prowadzą do wniosku, że funkcjonowanie w praktyce tych polityk jest nieefektywne[88].

Kolejnym mankamentem są niewystarczające środki organizacyjne instytucji nadzorowanych w zakresie AML/CFT. Organy nadzorcze identyfikują najczęstsze naruszenia wymagań prawnych AML/CFT polegające na:

- niewystarczającej kontroli wynikającej z niewłaściwej identyfikacji i weryfikacji klienta, także beneficjentów rzeczywistych,
- nieadekwatnej do zagrożeń kontroli wewnętrznej, spowodowanej niewłaściwymi politykami i procedurami AML/CFT oraz nieprawidłową oceną ryzyka klienta.

Ryzyko wynikające ze zjawiska de-riskingu[89]

Przyczyną zjawiska deriskingu jest niewłaściwe podejście instytucji obowiązanych na podstawie ustawodawstwa AML/ CTF do zarządzania ryzykiem ML/TF, polegające na odmowie wchodzenia w relacje biznesowe z klientami ocenionymi jako stwarzającymi podwyższone ryzyko z punktu widzenia polityk ML/TF instytucji obowiązanych. Takie podejście prowadzi do „wypchnięcia" tych podmiotów do sfer, w których pozostają poza jakąkolwiek kontrolą. To z kolei powoduje, że sektor finansowy jest narażony na ryzyko ML/TF. Brak dostępu podmiotów wykluczonych do systemu finansowego prowadzi do dokonywania przez nie transakcji poza systemami kontroli AML/CFT. Schodzą one do nieformalnych kanałów płatniczych w celu zaspokojenia swoich potrzeb (głównie dokonując transakcji gotówkowych, co powoduje, że śledzenie tego rodzaju transakcji staje się niemożliwe)[90].

Europejskie Organy Nadzorcze stoją na stanowisku, że przy metodzie *risked-based approach* nie wymaga się od instytucji obowiązanych wypowiadania umów bądź kończenia relacji biznesowej tylko z powodu ustalenia wyższego ryzyka prania pieniędzy i finansowania terroryzmu. Takie podejście, zamiast zapobiegać tym zjawiskom, wzmagałoby to ryzyko.

---

[87] *Joint Opinion of the European Supervisory Authorities*…, s. 20 [dostęp: 2 XII 2019].

[88] Tamże, s. 20.

[89] Tamże, s. 25.

[90] Tamże.

Ryzyko finansowania terroryzmu[91]

Organy nadzorcze raportują, że największym problemem związanym z ryzykiem finansowania terroryzmu jest słabość systemu kontroli w zakresie monitoringu transakcji. Osoby finansujące terroryzm niekonieczne mogą chcieć ukryć swoją tożsamość, mogą również posługiwać się środkami z legalnych źródeł (np. finansowanie społecznościowe). Z tego powodu identyfikacja i weryfikacja klienta schodzą na plan dalszy, ustępując miejsca właściwemu monitorowaniu transakcji[92].

Walkę z finansowaniem terroryzmu utrudnia brak dostępu do istotnych informacji, często będących w posiadaniu organów ścigania, które pomogły na wczesnym etapie zidentyfikować zagrożenie. Dlatego tak ważne jest podjęcie współpracy organów ścigania z organami nadzorczymi, ponieważ każdy z tych podmiotów ma ogląd tej samej sytuacji z innej perspektywy.

Ryzyko specyficzne dotyczące sektora usług finansowych

Ryzyko specyficzne sektorowe zostanie zaprezentowane wspólnie dla instytucji: kredytowych[93], płatniczych, pieniądza elektronicznego – jako instytucji najbardziej podatnych na zagrożenia ML/TF. Można wyróżnić następujące podstawowe problemy w tym obszarze:

- ryzyko charakterystyczne dla danego sektora,
- jakość kontroli i najczęstsze naruszenia przepisów w sektorze finansowym, m.in.:
  - niewłaściwy poziom identyfikacji i weryfikacji klienta przez instytucje finansowe, ryzyko powiązane z modelami biznesowymi klientów,
  - monitorowanie współpracy, w tym monitorowanie transakcji,
  - ocena całościowego profilu ryzyka sektora.

Do symptomów wskazujących na podwyższone ryzyko ML/TF zaliczono następujące zachowania klienta:

- podejmowanie decyzji niezrozumiałych pod względem ekonomicznym, brak zainteresowania korzystniejszymi warunkami finansowymi produktu,
- wypłacanie dużych kwot z bankomatów,
- częste dokonywanie transakcji o podobnej wartości,
- brak orientacji w cechach produktu,
- sposób zachowania lub obecność osoby towarzyszącej wskazujące na to, że klient jest kontrolowany i nie podejmuje samodzielnie decyzji,

[91] Tamże, s. 24.

[92] Tamże.

[93] Art. 4 ust. 1 pkt 17 *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (t.j.: DzU z 2019 r. poz. 2357).

- odmowa wykonania czynności związanych z jego identyfikacją i weryfikacją,
- rezygnacja z dokonania transakcji w przypadku, gdy dana instytucja okazuje zainteresowanie klientem,
- propozycja wręczenia korzyści majątkowej osobie dokonującej identyfikacji w zamian za nieprzeprowadzenie tej czynności lub wadliwe jej przeprowadzenie,
- posługiwanie się dokumentami wątpliwymi co do ich autentyczności.

Instytucje kredytowe oraz banki [94]

Instytucje kredytowe[95] (ang. *credit institutions*, CI) oraz banki są wykorzystywane przez klientów objętych ryzykiem ML/TF jako instytucje wejścia do systemu finansowego[96]. Jest to szczególnie widoczne w przypadku otwierania rachunków bankowych na podstawie przelewu weryfikacyjnego[97]. Komisja Nadzoru Finansowego uznała, że zawieranie umowy rachunku bankowego z wykorzystaniem przelewu weryfikacyjnego z innego rachunku płatniczego jako sposobu potwierdzania tożsamości klienta jest dopuszczalne, w przypadku gdy nie będzie możliwe kolejne zawarcie umowy rachunku płatniczego u innego dostawcy usług płatniczych, z wykorzystaniem przelewu z otwieranego rachunku dla potwierdzania tożsamości u tego dostawcy.

Również transakcje gotówkowe są czynnikiem powodującym rozwój zagrożenia ML/TF, zwłaszcza że większość instytucji kredytowych to instytucje retailowe, tj. konsumenckie i masowe. Występuje wówczas narażenie tych instytucji na transakcje transgraniczne, zwłaszcza tam, gdzie państwo członkowskie jest postrzegane jako centrum finansowe.

Na podstawie danych zawartych w wykresie 1 zamieszczonym na następnej stronie można zaobserwować roczny wzrost liczby naruszeń przepisów dotyczących zwalczania prania pieniędzy.

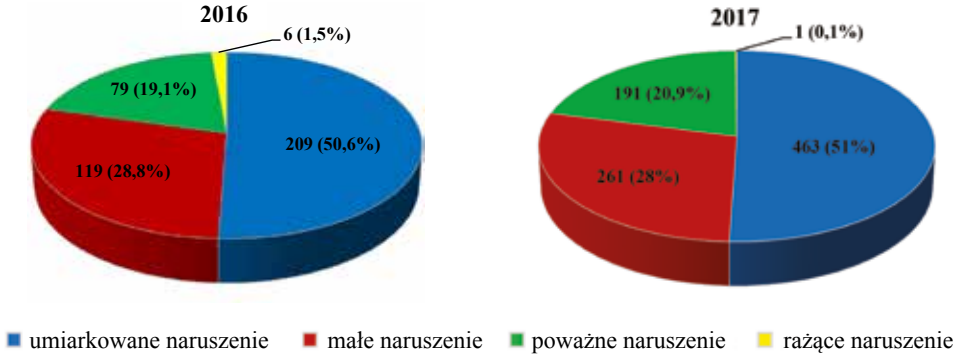
---

[94] *Joint Opinion of the European Supervisory Authorities*…, s. 30 i nast. [dostęp: 2 XII 2019].

[95] Art. 4 ust. 1 pkt 17 ustawy prawo bankowe.

[96] D. Chodziński, *Pranie pieniędzy jako jedna z form działania zorganizowanych grup przestępczych*, Legionowo 2012, s. 19, http://www.csp.edu.pl/download/6/16760/PraniepieniedzyjakojednazformdzialaniazorganizowanychgrupprzestepczychDChodzinsk.pdf [dostęp: 4 XII 2019].

[97] Zob. wytyczną nr 6 do *Rekomendacji KNF dotyczącej bezpieczeństwa transakcji płatniczych wykonywanych w Internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe*, z listopada 2015 r., https://zarabiajnabankach.pl/wp-content/uploads/2016/07/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf, s. 16 [dostęp: 2 XII 2019].



Wykres 1. Naruszenia przepisów dotyczących zwalczania prania pieniędzy.

Źródło: *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector* (Wspólna opinia Europejskich Organów Nadzorczych na temat ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu wpływającego na sektor finansowy UE, z 4 października 2019 r.), https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, s. 34 [dostęp: 2 XII 2019].

Wydawcy pieniądza elektronicznego (ang. electronic money issuers, EMI)[98]

Poziom ryzyka związanego z wydawaniem pieniądza elektronicznego zależy przede wszystkim od: metod dostępu do produktów e-money (np. zdalny on-boarding klientów[99]), cech produktów e-money, stopnia, w jakim EMI korzystają z innych podmiotów do dystrybucji i umarzania e-money w ich imieniu.

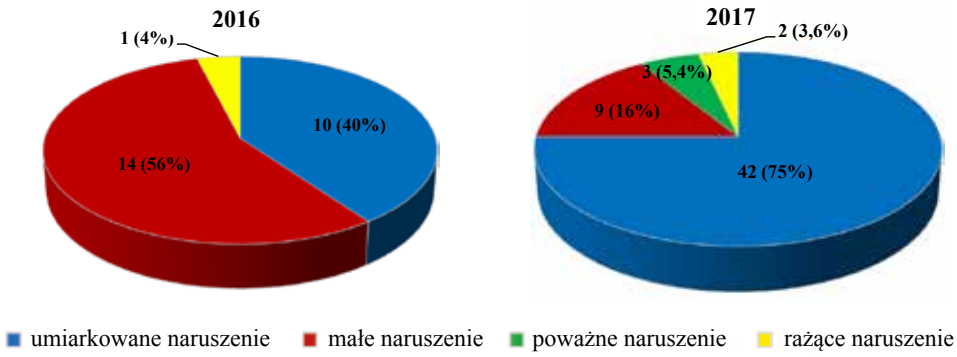
Im więcej wprowadza się restrykcji dotyczących użycia produktu e-money, tym mniejsza podatność na ML/TF. Wśród stosowanych restrykcji należy wymienić m.in.: limity płatności, brak możliwości dokonywania transakcji ATM (bankomatowych), akceptacja e-money możliwa w ograniczonej sieci akceptantów[100], brak transakcji osoba do osoby (P2P) oraz brak transakcji transgranicznych. Jednocześnie wymienione powyżej restrykcje sprawiają, że zastosowanie e-money jest ograniczone[101]. Do najczęstszych naruszeń w sektorze EMI zalicza się niewystarczające monitorowanie polityki i procedur, niska świadomości ML/TF, a także brak skuteczności raportowania transakcji podejrzanych (ang. *suspicious transaction reporting*, STR). W sektorze EMI obserwuje się wzrost liczby „naruszeń poważnych" oraz znaczny wzrost liczby „naruszeń umiarkowanych" (ang. *moderate breaches*), co zostało przedstawione na wykresie 2.

[98] *Joint Opinion of the European Supervisory Authorities*…, s. 46.

[99] To jest zdalne zawieranie umów z klientem.

[100] W rozumieniu art. 2 pkt 1b ustawy o usługach płatniczych.

[101] KNF do 2019 r. udzieliła tylko jednego zezwolenia na wydawanie pieniądza elektronicznego. Otrzymała je spółka Billon Solutions, https://businessinsider.com.pl/finanse/billon-solutions-licencja-e-money/xjb6be1, https://billongroup.com/pl/ [dostęp: 2 XII 2019].



Wykres 2. Naruszenia przepisów związanych z używaniem pieniądza elektronicznego.

Źródło: *Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector* (Wspólna opinia Europejskich Organów Nadzorczych na temat ryzyka związanego z praniem pieniędzy i finansowaniem terroryzmu wpływającego na sektor finansowy UE, z 4 października 2019 r.), https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, s. 50 [dostęp: 2 XII 2019].

Instytucje płatnicze (ang. payment institutions, PI)[102]

Ryzyko prania pieniędzy i finansowania terroryzmu w sektorze instytucji płatniczych[103] wiąże się głównie z rodzajem świadczonych usług oraz typem klienta. Największe ryzyko niosą za sobą przekazy pieniężne[104], zwłaszcza rozliczenia gotówkowe.

Podwyższony stopień wprowadzonych restrykcji ML/TF, dotyczący tego sektora, doprowadził do praktyk de-riskingu, stosowanych przez banki wobec dostawców usług przekazu pieniężnego działających w regionach o podwyższonym ryzyku ML/TF.

Przekazy pieniężne mają szczególne znaczenie w przypadku usług oferowanych klientom niemającym dostępu do regulowanych usług finansowych albo mającym ograniczony do nich dostęp. Wśród takich usług zaobserwowano używanie systemu hawala[105] do celów ML/TF przez dokonywanie niskokwotowych transferów pieniężnych[106].

[102] *Joint Opinion of the European Supervisory Authorities*…, s. 52.

[103] W rozumieniu art. 2 pkt 11 ustawy o usługach płatniczych.

[104] W rozumieniu art. 3 ust. 3 ustawy o usługach płatniczych.

[105] Pojmowany jako nieformalny transfer środków bez zaangażowania podmiotów autoryzowanych (jak banki). Zob. *System Hawala i finansowanie terroryzmu*, http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu/ [dostęp: 2 XII 2019].

[106] Zob. *Krajowa Ocena Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu*, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu, s. 125 [dostęp: 2 XII 2019].

Najczęstsze naruszenia w sektorze instytucji płatniczych

Organy nadzorcze obserwują, że polityka instytucji płatniczych w odniesieniu do identyfikacji i weryfikacji klienta, rejestru transakcji i STR jest dostosowana do obowiązujących przepisów. Problematyczna jest jednak efektywność zastosowanych praktyk. Obawy rodzi również niska świadomość instytucji płatniczych dotycząca zagrożeń ML/TF, która wynika z niewłaściwej oceny ryzyka klienta oraz jego działalności biznesowej (powodem może być m.in. konieczność szybkiego procesowania transakcji).

Podsumowanie

Analiza powyższych regulacji prawnych oraz stanowisk poszczególnych organów nadzorczych prowadzi do wniosku, że z uwagi na bardzo szybki postęp digitalizacji płatności elektronicznych te przepisy już w momencie wydania lub implementacji do krajowego systemu prawnego nie są adekwatne do zmieniającej się rzeczywistości. Pociąga to za sobą zwiększoną podatność systemu na ryzyko prania pieniędzy i finansowania terroryzmu.

Liczba wprowadzanych regulacji prawnych, zarówno w Unii Europejskiej, jak i w Polsce, oraz stopień ich skomplikowania pozwalają na wyciągnięcie wniosku, że ilekroć mamy do czynienia z innowacjami, to Amerykanie je wymyślają, Chińczycy kopiują, a Europejczycy regulują przepisami prawnymi. Dobitnie świadczy o tym to, że pomimo istniejącej od wielu lat możliwości wydawania pieniądza elektronicznego, pierwsze zezwolenie w tym zakresie zostało w Polsce udzielone dopiero w 2019 r.

Rynek płatności elektronicznych, a także organy nadzorcze stoją przed wyzwaniami związanymi z rozwojem FinTech oraz RegTech oraz śledzeniem trendów w obszarze walut wirtualnych. Instytucje finansowe i organy nadzorcze muszą współpracować ze sobą, m.in. przy wymianie informacji, oraz przeciwdziałać praktykom de-riskingu.

Bibliografia

Chodziński D., *Pranie pieniędzy jako jedna z form działania zorganizowanych grup przestępczych*, Legionowo 2012, Centrum Szkolenia Policji, http://www.csp.edu.pl/download/6/16760/PraniepieniedzyjakojednazformdzialaniazorganizowanychgrupprzestepczychDChodzinsk.pdf [dostęp: 4 XII 2019].

EBA Opinion on 'virtual currencies', https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20Opinion%20on%20Virtual%20Currencies.pdf?retry=1 [dostęp: 2 XII 2019].

EBA reports on crypto-assets, https://eba.europa.eu/eba-reports-on-crypto-assets [dostęp: 2 XII 2019].

Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention, https://www.fsb.org/wp-content/uploads/R270617.pdf [dostęp: 2 XII 2019].

Informacja o kartach płatniczych. I kwartał 2019 r., Narodowy Bank Polski, https://www.nbp.pl/systemplatniczy/karty/q_01_2019.pdf [dostęp: 4 XII 2019].

Informacja o kartach płatniczych. II kwartał 2019 r., Narodowy Bank Polski, https://www.nbp.pl/systemplatniczy/karty/q_02_2019.pdf [dostęp: 4 XII 2019].

Joint Opinion of the European Supervisory Authorities on the risks of money laundering and terrorist financing affecting the European Union's financial sector, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [dostęp: 2 XII 2019].

Krajowa Ocena Ryzyka Prania Pieniędzy oraz Finansowania Terroryzmu, Ministerstwo Finansów, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu [dostęp: 2 XII 2019].

Kunkiel-Kryńska A., *Prawo konsumenckie UE – dyrektywy oparte na metodzie harmonizacji minimalnej – wprowadzenie i wyrok TS z 16.05.1989 r. w sprawie 382/87 R. Buet i SARL Educational Business Services (EBS) v. Ministère public*, „Europejski Przegląd Sądowy" 2011, nr 12, s. 46–48; także: https://www.eversheds-sutherland.com/documents/global/poland/articles_pdf/pl/2011-12-01_eps_prawo_konsumenckie_ue_dyrekywy_oparte_na_harmonizacji_minimalnej_akunkiel.pdf [dostęp: 2 XII 2019].

Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process, https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf [dostęp: 2 XII 2019].

Piotrowska A., *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, CeDeWu.

Raport „Płatności cyfrowe" 2019, Izba Gospodarki Elektronicznej, https://eizba.pl/wpcontent/uploads/2019/11/PLATNOSCI_CYFROWE_2019.pdf?fbclid=IwAR1ol9GL6K85vybNy5iwjoctd4k7YPFuT1rki_OpLjTwSqw1DFpGNkBoXBk [dostęp: 2 XII 2019].

Rekomendacja KNF dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe, Warszawa, listopad 2015 r., Komisja Nadzoru Finansowego, https://zarabiajnabankach.pl/wp-content/uploads/2016/07/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf [dostęp: 2 XII 2019].

Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities, Komisja Europejska, https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf [dostęp: 4 XII 2019].

Stanowisko w sprawie wydawania kart przepłaconych, z 10 lipca 2015 r., Komisja Nadzoru Finansowego, https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [dostęp: 2 XII 2019].

System hawala i finansowanie terroryzmu, http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu [dostęp: 2 XII 2019].

UK FinTech. State of the Nation, T. Helm, A. Low, J. Townson (red.), 2019, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf [dostęp: 2 XII 2019].

Umowa międzynarodowa i memorandum of understanding – charakterystyka i terminologia, https://pressto.amu.edu.pl/index.php/cl/article/viewFile/6437/6458 [dostęp: 2 XII 2019].

Akty prawne

Dyrektywa PE i Rady (UE) 2018/843 z dnia 30 maja 2018 r. zmieniająca dyrektywę (UE) 2015/849 w sprawie zapobiegania wykorzystywaniu systemu finansowego do prania lub finansowania terroryzmu oraz zmieniająca dyrektywy 2009/138/WE i 2013/36/UE (Dz. Urz. UE L 156 z 19 VI 2018 r., s. 43).

Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/849 z dnia 25 maja 2015 w sprawie zapobiegania wykorzystywania systemu finansowego do prania pieniędzy lub finansowania terroryzmu, zmieniająca rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 648/2012 i uchylająca dyrektywę Parlamentu Europejskiego i Rady 2005/60/WE oraz dyrektywę Komisji 2006/70/WE (Dz. Urz. UE L 141 z 5 VI 2015 r., s. 73).

Dyrektywa Parlamentu Europejskiego i Rady 2009/110/WE z dnia 16 września 2009 r. w sprawie podejmowania i prowadzenia działalności przez instytucje pieniądza elektronicznego oraz nadzoru ostrożnościowego nad ich działalnością, zmieniająca dyrektywy 2005/60/WE i 2006/48/WE oraz uchylająca dyrektywę 2000/46/WE (Dz. Urz. UE L 267 z 10 X 2009 r., s. 7).

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j: DzU z 2019 r. poz. 1115, ze zm.).

Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych (t.j.: DzU z 2019 r. poz. 659, ze zm.).

Ustawa z dnia 29 lipca 2005 r. o obrocie instrumentami finansowymi (t.j.: DzU z 2018 r. poz. 2286, ze zm.).

Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe (t.j.: DzU z 2019 r. poz. 2357).

*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 XII 2010 r., s. 12).

Abstrakt

Badania pokazują, że najpopularniejszymi instrumentami płatniczymi są: karta płatnicza, rachunek bankowy z dostępem internetowym oraz konto w serwisie PayPal. Szybki rozwój techniki i digitalizacji płatności elektronicznych powodują, że już w momencie wydania aktów prawnych regulujących funkcjonowanie rynku finansowego w tym sektorze są one nieadekwatne do zmieniającej się rzeczywistości. Powoduje to podatność tego saktora na ryzyko wynikające z działalności przestępczej, w tym terrorystycznej. Wyzwania dla rynku płatności elektronicznych oraz organów nadzorczych w najbliższych latach będą się koncentrowały wokół przystosowania działalności do nowych trendów cyfrowych, implikacji związanych z rozwojem FinTech oraz RegTech, śledzeniu trendów i wyzwań w obszarze walut wirtualnych, wspieraniu wymiany informacji oraz współpracy pomiędzy instytucjami finansowymi a organami nadzorczymi, a także przeciwdziałaniu praktykom de-riskingu.

Słowa kluczowe: FinTech, RegTech, przeciwdziałanie praniu pieniędzy, przeciwdziałanie finansowaniu terroryzmu, AMC, CFT, EBA, KNF.

Abstract

Research shows that the most popular payment instrument is a payment card, then a bank account with Internet access and then a PayPal account. The progress and increase in the digitization of electronic payments means that when legislation is issued in these areas, they are no longer adequate to the changing reality. This makes them vulnerable to the risks associated with criminal activities, including terrorist activities. Challenges for the entire electronic payments market and supervisory authorities in the coming years will focus on adaptation to new digital challenges, implications related to the development of FinTech and RegTech, tracking trends and challenges in the area of virtual currencies, supporting information exchange

and cooperation between financial institutions and supervisory authorities and counteracting de-risking practices.

Keywords: FinTech, RegTech, anti money laundering, counter terrorist financing, AML, CFT, EBA, KNF.

Monika G. Bartoszewicz

Siła czy przesilenie?
Działalność i znaczenie Państwa Islamskiego

To, co wiemy o Państwie Islamskim[1], przypomina przedziwną mieszaninę propagandy wojennej oraz informacji zaczerpniętych z mediów społecznościowych i materiałów operacyjnych służb specjalnych. Naszą niepełną wiedzę można częściowo wytłumaczyć tym, że prowadzenie badań naukowych na ten temat było i jest niemożliwe, a większość analiz jest oparta na spekulacji lub ekstrapolacjach. Wiemy, że organizacja o nazwie Islamskie Państwo w Iraku i Lewancie (arab. Dawlat al-Islamijja fi al-Irak waasz-Szam) istniała jako jedna z wielu grup islamskich działających na Bliskim Wschodzie, na długo przed tym, zanim skoncentrowała na sobie uwagę światowych mediów i polityków. Samozwańczy kalif Abu Bakr al-Baghdadi[2] został liderem organizacji w maju 2010 r. Latem 2014 r. ugrupowanie zajęło rozległe terytorium, w tym miasta Mosul i Ramadi, a (…) *mimo tego, że nikt nie spodziewał się, że przetrwa dłużej niż trzy miesiące, w krótkim czasie kontrolowało już terytorium wielkością zbliżone do Wielkiej Brytanii*[3]. Doskonale przygotowana analiza Graeme'a Wooda sugeruje, że PI (…) *z zasady odrzuca pokój; łaknie ludobójstwa; jego poglądy religijne sprawiają, że jest konstytucyjnie niezdolne do pewnego rodzaju zmian,*

---

[1] Jak przypomina Janusz Danecki, nazwa „Państwo Islamskie" stała się niemal nazwą oficjalną, chociaż przymiotnik „islamski" jest neologizmem. Został on utworzony pod wpływem języków zachodnich w latach 70. XX w. i wyparł rodzime określenie, jakim jest przymiotnik „muzułmański" (a zatem zgodnie z regułami języka polskiego powinno się posługiwać nazwą „Państwo Muzułmańskie"). W literaturze anglojęzycznej najczęściej spotykanymi nazwami są „ISIS" (Islamic State of Iraq and Syria; Islamic State of Iraq and al-Sham) oraz „ISIL" (Islamic State of Iraq and Levant). Spotyka się również określenia czerpiące bezpośrednio z języka arabskiego: „Al Dawlah" (Państwo) lub „Da'esh/Da'ish", będący akronimem arabskich słów: *ad-Dawlah al-Islāmiyah fī 'l-Irāq wa-sh-Shām*, tzn. tych samych, które składają się na angielską nazwę ISIS: Państwo Islamskie Iraku i Syrii. W literaturze, ale także w dyskursie publicznym, często spotyka się frazę „tak zwane", która poprzedza nazwę. Ma ona wskazywać na samozwańczy i nieusankcjonowany prawem międzynarodowym status grupy. Ponieważ jednak w niniejszym artykule rozważania dotyczące prawnego statusu grupy nie są celem analizy, dla wygody czytelnika autorka używa skrótu PI (Państwo Islamskie) na przemian z nazwą „Kalifat".

[2] Zginął 26 X 2019 r. w wyniku wieloletniej operacji wywiadowczej amerykańskich sił specjalnych.

[3] G. Wood, *What ISIS really wants*, „The Atlantic", marzec 2015. Pełny tekst jest dostępny na: http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/ [dostęp: 13 IV 2019].

nawet jeśli mogą one zapewnić jego przetrwanie; i że uważa się za głównego gracza oraz zwiastuna nadchodzącej apokalipsy[4]. Innymi słowy, religia stanowiła esencję i oś tej organizacji, była zarówno *modus vivendi*, jak i *modus operandi*[5] oraz wpływała na zamierzenia grupy do tego stopnia, że można twierdzić, że PI było wyjątkowym przypadkiem wykorzystywania polityki do realizacji celów religijnych, a nie na odwrót (co jest o wiele bardziej typowe w polityce międzynarodowej[6]). Wynika to z tego, że – jak zauważył Artur Wejkszner – kalifat jest systemem rządów monokratycznych, w ramach których kalif jako osoba rządząca wymusza przestrzeganie owych norm przy użyciu wszystkich dostępnych środków, a jedną z tych norm jest stosowanie siły i przemocy[7]. Wejkszner przychyla się do stwierdzenia, że PI powinno być traktowane przede wszystkim jako grupa o charakterze paramilitarnym, dysponująca siłą, tj. sprzętem i zasobami ludzkimi, relatywnie jednak niewielkimi w odniesieniu do celów strategicznych i taktycznych, jakie sobie postawiła[8].

Państwo Islamskie, jak pisze Jürgen Todenhöfer, było pokłosiem wojny w Iraku[9], a jego członkowie, dodaje Patrick Cockburn, pragnęli zmieniać świat siłą i przemocą[10]. Olivier Hanne i Thomas Flichy de La Neuville przypisują powstanie PI wielu czynnikom, począwszy od problemów społecznych Iraku przez współzawodnictwo energetyczne na tym obszarze, inwazję amerykańską i rozpad Iraku w latach 2003–2011 aż po impas, w jakim kraj znalazł się w czasie rządów szyickiego premiera Nuri al-Malikiego (2006–2014)[11]. Nie można wprawdzie winić Al-Malikiego za całe zło, ale należy przyznać, że odegrał on główną rolę w doprowadzeniu do zbliżenia pomiędzy irackimi sunnitami a PI[12]. Do utworzenia Państwa Islamskiego przyczyniła się również wojna w Syrii trwająca w latach 2011–2014, która rozpoczęła się jako rewolta przeciw dyktaturze, ale szybko stała się częścią konfliktu pomiędzy sunnitami i alawitami, powiązanego z kolei z walkami pomiędzy sunnitami i szyitami (oraz związanych z tymi konfliktami wojen zastępczych, tzw. *proxy wars*). Nie należy też zapominać o renesansie starcia pomiędzy Zachodem a Moskwą w tym regionie, przypominającym zatargi z okresu zimnej wojny. Można więc pokusić się o tezę, że samo PI było

---

4 Tamże, brak numeracji stron.

5 Więcej o teologii politycznej Państwa Islamskiego zob. M.G. Bartoszewicz, *Reconciliation in the Shadow of ISIS*, w: *Oblicza pojednania*. *Faces of Reconciliation*, J. Kulska (red.), Opole 2016, s. 241–256.

6 Dobrze sporządzone omówienie instrumentalnego podejścia do religii w stosunkach międzynarodowych można znaleźć w: W. Cavanaugh, *The Myth of Religious Violence*, Oxford 2009.

7 A. Wejkszner, *Państwo Islamskie. Narodziny nowego kalifatu?*, Warszawa 2016, s. 85–86.

8 Tamże, s. 172.

9 J. Todenhöfer, *ISIS od środka. 10 dni w „Państwie Islamskim"*, Kraków 2015, s. 9.

10 P. Cockburn, *The Rise of the Islamic State*, New York–London 2015, s. 8.

11 O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie. Geneza nowego kalifatu*, Warszawa 2015, s. 13–35.

12 P. Cockburn, *The Rise of the Islamic*…, s. 47.

zaangażowane w pięć różnych konfliktów, które wzajemnie się napędzały i stanowiły niemalże bliskowschodnią wersję wojny trzydziestoletniej[13].

W wyniku nałożenia się na siebie tych czynników do czerwca 2014 r. PI było typową organizacją terrorystyczną organicznie związaną z Al-Kaidą. Po kryzysie wywołanym śmiercią Abu Musaba az-Zarkawiego dzięki nowemu przywódcy organizacja nie tylko przetrwała w Iraku, lecz także rozszerzyła działalność na Syrię targaną wewnętrznym konfliktem. W początkach 2014 r. PI ostatecznie zerwało związki z Al-Kaidą[14] i dokonało spektakularnej ekspansji, awansując do roli globalnego mocarstwa terrorystycznego. W czerwcu 2014 r. przywódca PI ogłosił powstanie kalifatu, który latem 2015 r. obejmował połowę Syrii oraz dość dużą część obszaru Iraku, a zatem terytorium wielkości mniej więcej Wielkiej Brytanii zamieszkałe przez ok. 8 mln ludzi[15]. Wraz z rozbiciem jego głównej siedziby w Rakce w październiku 2017 r. pojawiła się pokusa, aby Państwo Islamskie włożyć do lamusa historii i zaprzestać rozważań nad jego istnieniem i oddziaływaniem. Ale to właśnie teraz jest dobry czas na rzetelne analizy i refleksje nad tym fenomenem. Jak pisze Krzysztof Strachota, Państwo Islamskie jest zarówno zjawiskiem wyjątkowym, jak i bardzo typowym dla regionu, gdyż jest przejawem głębokiego kryzysu politycznego i społecznego, a także kryzysu bezpieczeństwa[16].

W niniejszym artykule autorka stawia sobie za cel przeanalizowanie źródeł siły Państwa Islamskiego. Podstawą rozważań jest teza, że PI było jednocześnie graczem rozgrywającym swoje strategiczne założenia za pomocą rozwiązań siłowych oraz instrumentem, za którego pomocą inne podmioty stosunków międzynarodowych realizowały politykę siły. Aby odpowiedzieć na pytanie, z jakich czynników płynęła siła tego fenomenu, w pierwszej części artykułu autorka przyjrzała się funkcjonowaniu PI, biorąc pod uwagę jego status i cele, sojuszników oraz zasięg terytorialny, a także analizując zasoby zarówno twardej, jak i miękkiej siły jego oddziaływania. W drugiej części artykułu, pozostając w optyce geopolitycznej, przeanalizowała głównych uczestników wydarzeń bliskowschodnich, którzy często wykorzystywali Kalifat (lub walkę z nim) do osiągnięcia własnych partykularnych interesów za pomocą rozwiązań siłowych. Porównując podejście do PI zarówno podmiotów lokalnych (państwa arabskie, Iran, Turcja), jak i międzynarodowych (Stany Zjednoczone wraz z zachodnimi sojusznikami oraz Rosja), można określić, jak wysoko w hierarchii ich celów strategicznych znajdowało się wyeliminowanie Kalifatu, oraz ocenić politykę prowadzoną za pomocą siły militarnej i potęgi ekonomicznej.

---

[13] Tamże, s. 94.

[14] K. Strachota, *Bliski Wschód w cieniu Państwa Islamskiego*, seria: Punkt Widzenia OSW, nr 52, Warszawa 2015, s. 8.

[15] P. Ramsauer, *Pokolenie dżihadu. Europo, czeka cię apokalipsa*!, Warszawa 2016, s. 15.

[16] K. Strachota, *Bliski Wschód w cieniu*…, s. 17.

Siła Państwa Islamskiego

W lecie 2014 r., po założeniu baz w Syrii i błyskawicznym zajęciu północnego Iraku, Państwo Islamskie położyło fundamenty pod utworzenie protopaństwa, czy też, jak pisze Artur Wejkszner, państwa (…) *in statu nascendi,* (…) *z własną administracją, ludnością, terytorium, ideologią i represyjnymi działaniami*[17], czyli pierwszego we współczesnych czasach, rozwiniętego muzułmańskiego systemu totalitarnego[18]. Petra Ramsauer zauważyła, że: (…) *wcześniej istniały już wprawdzie protopaństwa radykalnych islamistów – na przykład w postaci panowania talibów w Afganistanie w latach 1996–2001 – jednak plan budowy kalifatu był czymś wyjątkowym. Od likwidacji kalifatu osmańskiego w marcu 1924 roku potrzeba odbudowania wspólnego państwa wszystkich muzułmanów stanowiła credo wielu ruchów politycznych islamizmu, aż do dżihadyzmu włącznie*[19]. Co ciekawe, w opublikowanym w internecie w 2004 r. tekście *Idarat at-Tauahhusz* (*Rządy barbarzyństwa*), będącego jednocześnie instruktażem i manifestem ustanowienia kalifatu, jego autor, Abu Bakr Nadżi, obmyślił plan bitwy polegający na osłabieniu wrogich państw za pomocą czegoś, co nazywał „potęgą rozdrażnienia i wyczerpania". Jak wyjaśniają Michael Weiss i Hassan Hassan (…) *chodziło o to, żeby wciągnąć Stany Zjednoczone do otwartej, a nie „zapośredniczonej" wojny na Bliskim Wschodzie*[20].

Zgodnie z tym myśleniem Państwo Islamskie nie uznawało żadnej konwencji dotyczącej jeńców ani cywilów; nie istniały dla niego ani ONZ, ani prawo międzynarodowe. To, że nie było uznawane za państwo, nie miało żadnego znaczenia, ponieważ jedyną ambicją tego tworu *sui generis* było stanie się kalifatem, a nie zasiadanie na forum Zgromadzenia Ogólnego albo przystąpienie do OPEC. Polityka PI była oparta wyłącznie na zasadach dżihadu, którego celem jest rozszerzenie obecności islamu (arab. *dar al-islam*) za cenę wprawienia świata w stan wojny (arab. *dar al-harb*). Ta logika siły dopuszczała rokowania z niewiernymi (arab. *kuffar*) i akceptowała zawieranie taktycznych sojuszy oraz zawieszenia broni, ale jedynie w wymiarze oportunistycznym. Kalifowi, który nie ogłosił świętej wojny przynajmniej raz w roku, groziła dymisja. Zawarcie pokoju z PI było więc złudne, gdyż nie istniały czynniki zdolne do ograniczenia lub wyeliminowania odwoływania się organizacji do rozwiązań siłowych[21].

Rozważając status i dążenia Kalifatu, należy pamiętać, że strategiczną koncepcją PI było „pozostanie i ekspansja" (arab. *bakijja wa tatamaddad*), podczas gdy plan prezydenta Baracka Obamy zakładał „poniżenie i zniszczenie" (ang. *degrade and destroy*)[22]. Podstawą strategii Kalifatu była ekspansja terytorialna w regionie, stanowiąca

[17] A. Wejkszner, *Państwo Islamskie. Narodziny*…, s. 41.

[18] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 47.

[19] P. Ramsauer, *Pokolenie dżihadu. Europo*…, s. 31.

[20] M. Weiss, H. Hassan, *ISIS. Wewnątrz armii terroru*, Warszawa 2015, s. 77.

[21] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 138.

[22] P. Cockburn, *The Rise of the Islamic*…, s. 152.

jego immanentną cechę, oraz utrzymanie kontroli nad zajętym już terytorium[23], którego obszar podlegał stałym fluktuacjom, trudnym do śledzenia ze względu na częstość zmian oraz napływ dużej ilości informacji, nierzadko sprzecznych ze sobą[24].

Zdaniem Strachoty PI aspirowało do przejęcia skutecznej kontroli nad terytorium, zwłaszcza nad miastami, w których udzielano im pomocy (np. Faludża). Wiązało się to z koniecznością działań militarnych, a nie tylko stricte terrorystycznych[25]. Państwo Islamskie nie funkcjonowało na obszarze jednego państwa[26], ale scaliło terytoria dwóch krajów dotychczas pozostających ze sobą w konflikcie (warto przypomnieć, że dla tych dwóch państw wojna jest rzeczywistością od 18 lat). Poza zaletą, jaką było działanie po obu stronach granicy syryjsko-irackiej[27] (odrzucenie istniejących granic), była możliwa także próba utworzenia zupełnie nowego porządku, co realizowano na siłę. Kształtowanie się alternatywnej mapy regionu było zatem częściowo pochodną siły PI, a częściowo wynikało ze słabości danego państwa i prowadziło do powstania parapaństwa – organizmu o cechach nowoczesnego państwa (ośrodek decyzyjny, instytucje, społeczeństwo, siły zbrojne, samodzielnie prowadzona polityka), ale nim niebędącego[28]. To właśnie sprawiło, że PI stało się modelem budowy i konsolidacji wpływów na określonym terenie, aspirującym do pozycji państwa, skoncentrowanym na działaniach w skali lokalnej i regionalnej, obecnym także w skali międzynarodowej jako ośrodek przyciągający istniejące już grupy oraz jednostki identyfikujące się z jego ideologią i strategicznymi założeniami. Granice ustalone w 1920 r. były negowane nie tylko przez bojowników PI, lecz także przez nacjonalistów panarabskich i pansunnickich z partii Baas. To powodowało, że te tak różniące się grupy połączyła chęć ponownego zjednoczenia obszarów podzielonych przez Zachód[29].

Sukces Państwa Islamskiego w pierwszej kolejności miał charakter militarny, a dopiero potem polityczny[30]. Ten drugi aspekt wynikał przede wszystkim z inkluzywności Kalifatu, gdzie wokół „twardego jądra", jakim byli radykalni wyznawcy islamu, skupiły się siły świeckie (byli baasiści), plemiona irackie, a także ugrupowania sufickie. Kolejnym czynnikiem wzmacniającym PI byli ochotnicy przybywający ze wszystkich stron świata na teren przez nie opanowany. Oprócz liczby 20 tys. zagranicznych bojowników, o jakiej mówiły siły bezpieczeństwa w Europie i Stanach Zjednoczonych, pojawiały się także inne, dużo wyższe szacunki. Ramsauer cytuje Abda ar-Rahmana, który twierdził, że po stronie PI walczy 50 tys. cudzoziemców, oraz wywiad rosyjski,

[23] A. Wejkszner, *Państwo Islamskie. Narodziny*…, s. 88–90.

[24] Tamże, s. 129–130.

[25] K. Strachota, *Bliski Wschód w cieniu*…, s. 10–11.

[26] Tamże, s. 15.

[27] P. Cockburn, *The Rise of the Islamic*…, s. 46.

[28] K. Strachota, *Bliski Wschód w cieniu*…, s. 21.

[29] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 60.

[30] Tamże, s. 35.

szacujący tę liczbę nawet na 70 tys.[31] Tak więc podanie prawdziwej liczby jest nierealne, gdyż nie ma żadnych możliwości zbadania tego zagadnienia. Prawdą jest, że nie są nawet znane dokładne liczby dotyczące poszczególnych krajów, z których pochodzili ochotnicy, można się jedynie posłużyć szacunkami. Podczas gdy Kalifatowi zależało na podawaniu jak najwyższej liczby ochotników, jego przeciwnicy starali się zaniżyć szacunki – w ten sposób siła militarna stawała się elementem wojny propagandowej. Szeregi PI zasiliło ponadto ok. 20 ugrupowań terrorystycznych z różnych krajów[32], a od końca lata 2014 r. można było zaobserwować wzrost poparcia dla Kalifatu zarówno w rejonie ich działania (Liban, Półwysep Arabski), jak i na dalej położonych obszarach (Libia, Nigeria). Ten wzrost wynikał z rozpowszechniania na tych terenach idei kalifatu. Państwo Islamskie nie ukrywało swoich aspiracji do zwierzchnictwa nad całym Bliskim Wschodem oraz Afryką Północną, a w wymiarze symbolicznym – nad całym „światem islamu".

Przedmiotem fascynacji sympatyków Państwa Islamskiego na całym świecie, a zarazem źródłem jego potęgi i fundamentem działania, była jego armia[33]. Były to regularne siły zbrojne będące w stanie rozbić silniejszą, profesjonalną i dobrze uzbrojoną armię iracką, odnieść wiele taktycznych sukcesów nad dość trudnym przeciwnikiem, jakim są paramilitarne oddziały irackich Kurdów (peszmergowie), zdobyć wiele miast, w tym drugie co do wielkości – Mosul, oraz kilkakrotnie zagrozić samemu Bagdadowi. Armia PI była złożoną, skuteczną w działaniu strukturą, dowodzoną zarówno przez weteranów wojskowych (rekrutujących się spośród byłych oficerów Saddama Husajna), jak i weteranów dżihadu, takich jak Ali Kiffa czy gruziński Czeczen Abu Umar asz-Sziszani (właśc. Tarchan Batiraszwili). Dzięki umiejętności przystosowania się do warunków geograficznych, armia PI stała się przeciwnikiem nie tylko profesjonalnym, lecz także bardzo zdeterminowanym. Tę determinację PI zawdzięczało obozom szkoleniowym, w których przekazywano i elementy wiedzy wojskowej, i elementy ideologiczne (wykłady poświęcane dżihadowi i znaczeniu męczeństwa, tj. oddania życia za wiarę, co gwarantuje miejsce w raju). W zestawieniu z wszechobecną korupcją w armii irackiej[34] kolejnym elementem wyróżniającym siły zbrojne PI była dyscyplina oraz to, że po zakończonym szkoleniu żołnierze dostawali żołd (według Samuela Laurenta pobory ochotników z Zachodu były wyższe, co stanowiło kolejny element strategii rekrutacyjnej i wojny propagandowej)[35].

Najliczniejszą formacją była piechota (30 tys. osób). Nie była to struktura monolityczna, gdyż tworzyły ją oddziały działające niezależnie, dopóki nie dostały rozkazu przegrupowania się do bitwy[36]. Odwrotnie funkcjonowały z kolei oddziały pancerne –

[31] P. Ramsauer, *Pokolenie dżihadu. Europo*…, s. 40.

[32] Tamże, s. 15.

[33] S. Laurent, *Kalifat terroru. Kulisy działania Państwa Islamskiego*, Warszawa 2015, s. 37.

[34] P. Cockburn, *The Rise of the Islamic*…, s. 11.

[35] S. Laurent, *Kalifat terroru. Kulisy*…, s. 39.

[36] Tamże, s. 43.

miały one scentralizowane dowództwo, a każdy region dysponował pewną liczbą czołgów w zależności od wyznaczonych celów strategicznych i zagrożeń. Jakość sprzętu, którym dysponowało PI, była różna, brakowało natomiast wykwalifikowanej kadry, co powodowało, że bojownicy Kalifatu nie mogli używać całego swojego arsenału[37]. Także artyleria (5 tys. osób) dysponowała nowoczesnym uzbrojeniem pozyskanym od Wolnej Armii Syrii (WAS), którą dozbrajał Zachód w ramach wspierania „umiarkowanych rebeliantów" (m.in. pociskami przeciwpancernymi Milan)[38]. Kolejną formacją, liczącą 700 członków, byli strzelcy wyborowi (Al-Kanz). Był to niewielki oddział, ale o bardzo dużym znaczeniu strategicznym, rekrutujący się z najlepszych żołnierzy innych oddziałów. Przechodzili oni trudne i wyczerpujące szkolenie, w którym wykorzystywano umiejętności żołnierzy z innych krajów (ang. *know-how*), byli także przygotowywani na śmierć[39]. Razem z siłami specjalnymi (600 osób), podlegającymi bezpośrednio głównemu dowództwu, stanowili wizytówkę Kalifatu[40]. Należy także wspomnieć o wojsku przygranicznym, które nie tylko chroniło terytorium przed agresją z zewnątrz, lecz także nie pozwalało mieszkańcom opuszczać obszaru Kalifatu. Czuwało ono również nad sprawnym przemytem, będącym stałym źródłem dochodu.

Ponad 11 lat po wkroczeniu Stanów Zjednoczonych do Iraku śmiertelnie groźny ruch partyzancki wykazał się biegłością w wielu aspektach sztuki wojennej, łatwością dostosowywania się do sytuacji i wytrwałością w boju[41]. Daniel Estulin uważa, że przypadkowej zbieraninie terrorystów nie udałoby się samodzielnie zdobyć dużego miasta i terytorium ani ustanowić nad nimi kontroli (dla porównania podaje przykład amerykańskiej ofensywy na Faludżę)[42]. Swoje sukcesy militarne PI zawdzięczało przede wszystkim uzbrojeniu, którego miało zaskakująco dużą ilość. Trzeba doliczyć 30 radzieckich czołgów T-55 przejętych od armii Baszszara al-Asada, wozy opancerzone produkcji amerykańskiej[43], pojazdy typu humvee (3 tys.), działa M-198 155 mm oraz pociski SCUD i pociski przeciwlotnicze krótkiego zasięgu SA-18, SA-24 oraz FN-6 (w nieznanej liczbie). Dżihadyści przejęli także trzy samoloty myśliwskie, których mogli używać dzięki pilotom z dawnej armii Saddama Husajna szkolonym we Francji[44]. Nie bez znaczenia było także obranie hybrydowej taktyki walki, łączącej konwencjonalne działania wojenne, walkę partyzancką i akcje terrorystyczne. Te działania miały na celu ustanowienie kontroli nad terenami miejskimi zdominowanymi przez sunnitów

[37] S. Laurent, *Kalifat terroru. Kulisy*…, s. 44–45.

[38] Tamże, s. 47, 150. S. Laurent jest zdania, że PI uzyskało te pociski bezpośrednio od WAS zbrojonej przez Zachód.

[39] Tamże, s. 48–50.

[40] Tamże, s. 56.

[41] M. Weiss, H. Hassan, *ISIS. Wewnątrz armii terroru*…, s. 372.

[42] D. Estulin, *W imię Allaha*, Katowice 2016, s. 210.

[43] O. Hanne i T. Flichy de La Neuville określali ich liczbę na co najmniej 50, S. Laurent pisał natomiast o 400.

[44] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 97–98.

w Iraku i Syrii, przejęcie kontroli nad infrastrukturą krytyczną na tym obszarze oraz nad granicami zewnętrznymi Kalifatu, zniszczenie lub osłabienie potencjału wojskowego reżimu irackiego i syryjskiego, a także dalszą ekspansję terytorialną[45]. Z kolei taktyka obronna miała charakter adaptacyjny i była realizowana z wykorzystaniem wielu działań: od fortyfikacji przez obronę terytorialną i strefową, zamrożenie działań czy ekspansję[46]. Cywilów natomiast traktowano jako ludzkie tarcze, mające zapobiec nalotom sił międzynarodowych[47].

Znane są także plany Państwa Islamskiego dotyczące broni masowego rażenia (broń CBRN). Jak zauważa Wejkszner, taka broń niosłaby za sobą konsekwencje raczej psychologiczne niż faktyczne ryzyko związane z możliwością jej użycia[48]. Jeśli chodzi o broń nuklearną, to po zajęciu Mosulu PI oświadczyło, że dysponuje materiałami rozszczepialnymi, z których nie zawaha się skorzystać. Natomiast zdaniem ekspertów wartość uranu posiadanego przez PI czyniła go bezużytecznym w kontekście jego zastosowania operacyjnego. O wiele większe było prawdopodobieństwo użycia broni radiologicznej, szczególnie tzw. brudnej bomby (ang. *radiological dispersal device*, RDD), urządzenia mało praktycznego, ale skutecznego pod kątem wojny psychologicznej. Próby wejścia w posiadanie broni chemicznej (m.in. gazu musztardowego) zdawały się potwierdzać przesłanki o rozwijaniu takiego arsenału przez PI; nie bez znaczenia były przy tym wcześniejsze doświadczenia Al-Kaidy, z których mogło czerpać PI. Ponadto broń biologiczna, łatwa do pozyskania na czarnym rynku, zwiększała ryzyko bojowego wykorzystania patogenów. Miał na to wskazywać m.in. laptop przejęty przez wojska zachodnie, w którym znajdował się instruktaż dotyczący produkcji takiej broni i jej użycia, np. na wybrane obiekty w Turcji czy do zatrucia ujęć wody pitnej w pobliżu niektórych aglomeracji.

Według Daniela Estulina siłę ekonomiczną Kalifatu stanowiły dochody PI, które u szczytu potęgi ugrupowania wynosiły 3–6 mln dolarów dziennie. Łączna wartość jego aktywów sięgała 1,3–2 mld dolarów, co nie tylko stawiało PI na pierwszym miejscu najlepiej finansowanych grup terrorystycznych na świecie, lecz także pozwalało wyprzedzić kilka państw[49]. Państwo Islamskie korzystało także z pieniędzy, które regularnie otrzymywało od prywatnych darczyńców, a także z podatków i haraczy (arab. *dżizja*), które ściągano od niemuzułmanów zamieszkujących podbite tereny. Zajmowało również rachunki bankowe i majątki poszczególnych osób, wymuszało okupy za porwanych ludzi oraz zawłaszczało i sprzedawało na czarnym rynku zabytki skradzione ze starożytnych pałaców i stanowisk archeologicznych.

Ale Państwo Islamskie to nie tylko „twarda" siła wojska i ekonomii. Nie mniej ważnymi rezerwami, z których umiejętnie czerpano, były siła w wersji *soft*, czyli siła

[45] A. Wejkszner, *Państwo Islamskie. Narodziny*…, s. 173.

[46] Tamże, s. 174.

[47] Tamże, s. 175.

[48] Tamże, s. 198–203.

[49] D. Estulin, *W imię Allaha*…, s. 272–273.

idei, machiny propagandowej, a także wojna psychologiczna prowadzona za pomocą strachu. Strachota podkreśla, że myślą przewodnią była próba odtworzenia wzorowego państwa islamskiego[50]. To obraz prawdziwej utopii, państwa, w którym, według słów Abu Bakra al-Baghdadiego: *Arab i nie-Arab, czarny i biały, człowiek Zachodu i człowiek Wschodu – wszyscy są braćmi*[51]. Ważny był nie tylko ów ideał, lecz także sposób, w jaki ku niemu dążono. Hanne i Flichy de La Neuville zauważają, że salafizm dżihadystyczny uznaje się za rewolucyjny, a więc stosujący przemoc[52]. Wynika z niego coś więcej niż tylko konfliktowy stosunek do sąsiadów i niemożność nawiązania oraz utrzymania z nimi jakichkolwiek relacji. Płynie z niego także agresywność sankcjonująca stosowanie siły i zmuszająca do jej użycia wobec wszystkich wrogów – wewnętrznych i zewnętrznych. Salafizm dżihadystyczny oznacza bowiem odrzucenie reguł gry dyktowanych przez społeczność międzynarodową, odmowę działania pod jej dyktando. W przypadku Kalifatu nie miało się przecież do czynienia z procesem państwowotwórczym sankcjonowanym przez ONZ, ale z wyzwaniem rzuconym całemu systemowi międzynarodowemu.

Dyrektor amerykańskiej Centrali Wywiadu Robert James Woolsey mówił o terrorystach, że nie chcieli zasiąść przy stole do rozmów, raczej pragnęli zniszczyć tych, którzy przy nim siedzą – i to są słowa najbardziej odpowiadające prawdzie w odniesieniu do PI. Krzysztof Strachota twierdzi wręcz, że PI było siłowym wyzwaniem rzuconym reżimom istniejącym w regionie, wyznaczonym wcześniej granicom, koncepcji narodu jako suwerena (który PI zastąpiło *ummą* – wspólnotą wiernych), wpływom oraz roli Zachodu (jako bezalternatywnego punktu odniesienia cywilizacyjnego), a także pewnemu modelowi społeczno-politycznemu (demokracji, rządom prawa, wolnemu rynkowi itp.)[53]. Przywódca Kalifatu Ibrahim al-Badri, który przyjął *nom de guerre* (pseudonim – przyp. red.) „Abu Bakr al-Baghdadi", zdawał się to dobrze rozumieć. Postać Al-Baghdadiego z powodu przemyślanej nieobecności stała się czymś w rodzaju idei, być może przerastającej jego osobę. Jego śmierć była nieunikniona, ale śmierć ruchu, który stworzył – niekoniecznie, ponieważ PI jest tylko symbolem i nośnikiem pewnej idei, która już na dobre się zakorzeniła – i to nie tylko na obszarze Bliskiego Wschodu[54].

Można pokusić się o tezę, że cała polityka międzynarodowa PI sprowadzała się do współpracy z podobnymi do niego radykalnymi ośrodkami i ugrupowaniami na świecie oraz do propagandy[55]. Ta ostatnia zajmowała bardzo ważne miejsce w Kalifacie

[50] K. Strachota, *Bliski Wschód w cieniu*…, s. 10–11.

[51] P. Cockburn, *The Rise of the Islamic*…, s. XI.

[52] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 120.

[53] K. Strachota, *Bliski Wschód w cieniu*…, s. 20, 40.

[54] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 55.

[55] Obszerne omówienie propagandy stosowanej przez PI można znaleźć u W. McCantsa (zob. W. McCants i in., *The Islamic State's Ideology & Propaganda*, The Brookings Project on „U.S. Relations with the Islamic World" 2015) oraz D.B. Skillicorna (tenże, *Empirical Assessment of al Qaeda, ISIS, and Taliban Propaganda*, materiały konferencyjne, [bmw] 2015).

i podlegała bezpośrednio Al-Baghdadiemu[56]. Propaganda Kalifatu skupiała się na: upowszechnianiu informacji pomocnych przy rekrutacji bojowników, pozyskiwaniu zwolenników (radykalizacji społeczności) oraz zdobywaniu funduszy[57]. Tym celom służyły agencje informacyjne, czasopisma internetowe (m.in. „Dabiq", „Rumiyah") oraz profesjonalnie przygotowane materiały wideo, publikowane zarówno po arabsku, jak i w językach obcych, m.in. po rosyjsku, angielsku, francusku. Nie sposób odmówić Kalifatowi skuteczności także w tej dziedzinie. Hanne i Flichy de La Neuville oceniają, że połowę bojowników armii PI rekrutowano poza granicami Kalifatu, a ich liczbę oceniono jesienią 2014 r. na ok. 50 tys.[58] Bojownikom Kalifatu miała stawić czoła armia iracka (350 tys. żołnierzy), która była wspomagana przez policjantów (kolejne 500 tys.) oraz prorządowe milicje sunnickiego Przebudzenia (As-Sahwa). Skoro jednak prawie milion żołnierzy nie było w stanie pokonać PI, to znaczy, że w przypadku Kalifatu siła przekazu i propaganda strachu powinny być brane pod uwagę tak samo jak jego siła militarna. Ucieczkę żołnierzy armii irackiej z Mosulu spowodowała między innymi panika, jaką wywołała właśnie kampania propagandowa prowadzona równolegle do działań militarnych. Trzeba jednak pamiętać, że jeśli chodzi o świat wirtualny, to Kalifat dysponował siłą, ale nie wszechmocą – nie był w stanie prowadzić wojny w cyberprzestrzeni. To oznacza, że upowszechniał swoje materiały, lecz nie potrafił włamać się do ośrodków transmisji danych; wykorzystywał Internet, ale nie umiał go kontrolować, uprawiał jedynie lokalne piractwo[59].

Dbanie o własny wizerunek wymagało zdecydowanych działań, podejmowanych nie tylko poza granicami PI. Jednym z nich było zatrzymywanie uciekinierów. Laurent pisał: (…) *rozczarowanych kalifatem jest wielu, ale niewielu wraca* (do krajów pochodzenia). *Niewygodni świadkowie mogliby zepsuć tę doskonale działającą machinę propagandową, przedstawiającą Państwo Islamskie jako eldorado muzułmanów i przyciągającą tak wielu Europejczyków*[60]. Jednak najpowszechniej znanym sposobem wykorzystywania środków przekazu i mediów społecznościowych przez PI było upublicznianie aktów przemocy i pokazów brutalnej siły. Od momentu swojego powstania PI umiejętnie korzystało z serwisów społecznościowych, takich jak YouTube i Twitter, jako ważnego narzędzia propagandowego w wojnie psychologicznej. Publikowane materiały (biczowanie, odcinanie członków, ukrzyżowania, dekapitacje, egzekucje i inne

[56] C. Winter, *The Virtual "Caliphate": Understanding Islamic State's Propaganda Strategy*, „Quilliam Report" 2015, http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [dostęp: 13 IV 2019].

[57] L. Shamieh, Z. Szenes, *The Propaganda of ISIS/DAESH through the Virtual Space*, „Defence Against Terrorism Review" 2015, nr 1, s. 7–31.

[58] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 93.

[59] Tamże, s. 78–79.

[60] S. Laurent, *Kalifat terroru. Kulisy*…, s. 53.

formy wymierzania kary) pozwalały szerzyć strach (terror) zarówno w sercach wrogów, jak i mieszkańców obszarów znajdujących się już pod kontrolą Kalifatu[61].

Państwo Islamskie to eksperci od strachu, pisał Cockburn[62]. Rzeczywiście, dżihadyści wiedzieli, jak siać terror. Nawet w miejscach, które musieli opuścić, rozmieszczali miny przeciwpiechotne, zaminowywali też domy i meczety, a nawet zwłoki ludzkie, aby nadal zabijać[63]. Według Strachoty stosowali oni terroryzm indywidualny, spektakularne zamachy bombowe (samobójcze, z użyciem samochodów), widowiskowe egzekucje indywidualne i zbiorowe, a ich celem były zarówno siły bezpieczeństwa oraz armia, jak i ludność cywilna[64]. Wejkszner także pisze o systemie przemocy terrorystycznej skierowanej przeciw wrogowi wewnętrznemu i zewnętrznemu, na który składały się: wywiad, kontrwywiad, policja religijna, a także pełna kontrola środków społecznej komunikacji i kontrola gospodarki[65]. Strachota zwrócił również uwagę na to, że działania i sukcesy PI świadczyły nie tylko o sile ugrupowania, lecz także o słabości i ograniczonych możliwościach Iraku, Syrii oraz całej międzynarodowej koalicji[66]. Twierdził wręcz, że powołanie koalicji złożonej z kilkudziesięciu państw pod przywództwem Stanów Zjednoczonych było uznaniem siły Kalifatu i jego nobilitacją. Napoleońskie zwycięstwa PI tylko częściowo można wytłumaczyć słabością irackiej armii. Podobnie poczynań uczestników konfliktu bliskowschodniego nie sposób pojąć bez analizy tego, jak oni sami postrzegali PI oraz jak jego siła i działalność odnosiły się do ich własnej polityki międzynarodowej.

Państwo Islamskie jako element polityki siłowej innych podmiotów

Bliskiego Wschodu nie można zrozumieć bez polityki, a polityki bliskowschodniej nie sposób z kolei pojąć bez wzięcia pod uwagę rozwiązań siłowych, tym bardziej że niemal wszystkie zaangażowane strony stosują przemoc. W tym kontekście Państwo Islamskie jawiło się jako jeden z podstawowych instrumentów siłowej polityki prowadzonej od dekad przez obecne na tym obszarze podmioty międzynarodowe. Aktualny konflikt ma swoje korzenie w wydarzeniach z 1948 r., a nawet jeszcze

---

[61] S. Stalinsky (M. Khayat i R. Sosnow – współpraca), *ISIS's Use Of Twitter, Other U.S. Social Media To Disseminate Images, Videos Of Islamic Religious Punishments – Beheading, Crucifixion, Stoning, Burning, Drowning, Throwing From Buildings – Free Speech?*, „Middle East Media Research Institute" 2016, Inquiry & Analysis Series, nr 1218, https://www.memri.org/reports/isiss-use-twitter-other-us-social-media-disseminate-images-videos-islamic-religious [dostęp: 13 IV 2019].

[62] P. Cockburn, *The Rise of the Islamic*…, s. XIV.

[63] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 99.

[64] K. Strachota, *Bliski Wschód w cieniu*…, s. 9–11.

[65] A. Wejkszner, *Państwo Islamskie. Narodziny*…, s. 44, 85.

[66] K. Strachota, *Bliski Wschód w cieniu*…, s. 16, 20, 35.

wcześniejszych[67]. Analizując je z krótszej perspektywy czasowej, można uznać, że gdyby nie próba obalenia reżimu Al-Asada (2011 r.) przez dozbrajanie, finansowanie i szkolenie paramilitarnych syryjskich ugrupowań, PI nie miałoby możliwości przeprowadzenia swojego blitzkriegu w czerwcu 2014 r. To właśnie Zachód wraz ze swoimi regionalnymi aliantami – Turcją, Arabią Saudyjską, Katarem, Kuwejtem oraz Zjednoczonymi Emiratami Arabskimi – stworzył warunki do powstania i działalności Kalifatu[68]. W syryjskie powstania od początku było uwikłanych wiele rządów Środkowego Wschodu i Zachodu zainteresowanych obaleniem rządu Al-Asada. David Cameron, premier Wielkiej Brytanii, Francois Hollande, prezydent Francji, oraz Barack Obama, prezydent Stanów Zjednoczonych, połączyli swoje siły już w 2011 r., aby odsunąć od władzy legalnie wybranego prezydenta Syrii i zadać cios Rosjanom i Irańczykom, którzy go popierali. Arabia Saudyjska, Katar, Stany Zjednoczone, Francja, Anglia oraz inne kraje usiłowały wesprzeć działania przeciwników Al-Asada[69] pieniędzmi, dostawami broni, a także kampaniami medialnymi, zwłaszcza stacji telewizyjnych Al-Dżazira i Al-Arabija, które pod wieloma względami przypominały dezinformacyjną zachodnią propagandę sprzed wojny w Iraku w 2003 r. Także prywatni sponsorzy i organizacje z Arabii Saudyjskiej i Kuwejtu dostarczały na wielką skalę pieniądze, broń i bojowników[70]. Jednak sztuczny podział na rebeliantów i grupy ekstremistyczne się nie sprawdził. „The Washington Post" ujawnił, że członkowie Wolnej Armii Syrii zostali przeszkoleni w Arabii Saudyjskiej przez siły sojusznicze, przy wykorzystaniu prywatnych firm o charakterze wojskowym, a po zakończeniu finansowania i szkolenia ich przez Zachód zasilili szeregi PI[71]. W ten sposób zemściła się polityka wspierania frakcji „umiarkowanych". Ponadto rozgrywanie jednych fundamentalistów przeciw drugim oznaczało, że nawet wygrana wojna nie przyniesie rozwiązania politycznego, co ostatecznie znalazło potwierdzenie po 2017 r.

Należy jednocześnie pamiętać, że destabilizacja i podziały polityczne towarzyszące „zmianie reżimu" były jedynie elementem większej całości[72]. Estulin sugeruje: (…) *jeśli jakieś państwo ma niezależny rząd, ropę naftową, finanse, rolnictwo albo strategiczne zasoby, a jeszcze nie znajduje się w strefie wpływów międzynarodowych korporacji, to prędzej czy później zostanie zorganizowana pod przywództwem Stanów*

[67] Geneza problemów będących podstawą wszystkiego, co obecnie dzieje się na Bliskim Wschodzie, została opisana w: D. Fromkin, *A Peace to End All Peace: The Fall of the Ottoman Empire and the Creation of the Modern Middle East*, London 2001.

[68] P. Cockburn, *The Rise of the Islamic*…, s. 9.

[69] Tamże, s. 71.

[70] J. Todenhöfer, *ISIS od środka. 10 dni*…, s. 15, 16.

[71] M. Souad, *The terrorists fighting us now? We just finished training them*, „The Washington Post", 18 VIII 2014 r., https://www.washingtonpost.com/posteverything/wp/2014/08/18/the-terrorists-fighting-us-now-we-just-finished-training-them/?utm_term=.f59f2cc2a47f [dostęp: 13 IV 2019].

[72] Washington's Blog, W. Masden, Syrian Girl Partisan, J.P. Leonard, *ISIS IS US: The Shocking Truth Behind the Army of Terror*, San Diego 2015, s. 21, 44.

Zjednoczonych kampania prowadząca do jego zniszczenia[73]. Według Estulina wzniecanie wojen domowych to typowa polityka „dziel i rządź" oparta na modelu konfliktu, w którym Kalifat był tylko jednym z narzędzi realizowania tej strategii. Otrzymywał on pieniądze i broń od tych samych sił (będących pod wodzą Stanów Zjednoczonych), które potem zrzucały bomby na Irak i Syrię. Można się z nim zgodzić, że metody kontroli nad światem islamskim przy wykorzystywaniu historycznych różnic między sunnitami i szyitami to polityka prowadzona już od czasów umowy Sykes–Picot[74]. Z taką argumentacją zgadza się także Cockburn, według którego zaangażowanie Zachodu pogłębiło istniejące różnice i zmieniło bieg wydarzeń, co spowodowało wybuch wojny domowej[75]. Ma to sens, jeśli uznamy, że zaangażowanie państw zachodnich w regionie sprowadza się do ochrony interesów naftowych oraz dbania o to, aby kraje regionu nadal były słabe i podzielone, co jest gwarantem niezmienności tamtejszej sytuacji. W tym kontekście straszenie PI było jedynie instrumentem mającym usprawiedliwić wykorzystanie tej groźby jako pretekstu do interwencji zbrojnej[76].

Przyglądając się sytuacji na Bliskim Wschodzie, można w niej odnaleźć odbicie powiązań zależnych od siebie potęg światowych i regionalnych. Cockburn podkreśla, że państwa tego regionu mają inne cele strategiczne oraz różne priorytety i nie zawsze na szczycie tej hierarchii znajdowało się pokonanie Kalifatu[77]. Warto zatem przyjrzeć się najważniejszym podmiotom.

Analizując bliskowschodnie *proxy wars*, czyli zaangażowanie poszczególnych państw we wspieranie (politycznie, finansowo, logistycznie) i tworzenie sił biorących udział w konflikcie, Strachota wyróżnia następujące jego strony: reżim w Damaszku oraz opozycję. Reżim w Damaszku, wspierany przez Iran, Hezbollah, Rosję, widział w PI głównego wroga, zagrażającego terytorialnej integralności państwa[78]. Niezbyt silne oddziały Al-Asada musiały jednak unikać strat i mogły angażować się tylko na jednym froncie[79]. Z kolei dla syryjskiej opozycji, wspieranej przez państwa arabskie i zachodnie oraz Turcję, nadrzędnym celem było obalenie Al-Asada. Państwo Islamskie było wówczas drugą co do wielkości siłą w Syrii, co oznaczało, że jeżeli Al-Asad upadnie, to nic nie powstrzyma Kalifatu przed zapełnieniem pustki po nim[80]. Rząd Iraku oraz iraccy Kurdowie byli wspierani przez koalicję państw zachodnich, przy czym Kurdów wspomagał również Iran. Cele Bagdadu nie były dalekie od celów Damaszku, Kurdowie natomiast prowadzili zupełnie inną politykę. Pozbawieni prawa do samostanowienia, mają oni względną autonomię w Iraku (od 2003 r.) i w Syrii (od 2012 r.).

[73] D. Estulin, *W imię Allaha*…, s. 5–7.

[74] Tamże, s. 242.

[75] P. Cockburn, *The Rise of the Islamic*…, s. 111.

[76] D. Estulin, *W imię Allaha*…, s. 258–259.

[77] P. Cockburn, *The Rise of the Islamic*…, s. 156.

[78] K. Strachota, *Bliski Wschód w cieniu*…, s. 28.

[79] P. Cockburn, *The Rise of the Islamic*…, s. 33.

[80] Tamże, s. 34.

Natomiast w Turcji ich sytuacja systematycznie się pogarsza. Udział Kurdów w koalicji utworzonej przez prezydenta Obamę gwarantował im zatem nie tylko finansowanie i zaopatrzenie w broń, lecz także możliwość zaistnienia na scenie międzynarodowej oraz wsparcie dla ich sprawy. Wynikało ono często z popularnego (aczkolwiek niekoniecznie prawdziwego) przekonania, że peszmergowie to jedyna siła dająca odpór armiom Kalifatu. Kurdowie oportunistycznie skorzystali z trwającego konfliktu i zabezpieczyli sporne terytoria. Massoud Barzani wykorzystał załamanie armii irackiej i zagarnął wszystkie ziemie (wraz z miastem Kirkuk), o które od 2003 r. Kurdowie toczyli spory z Arabami[81]. Należy pamiętać również o oportunizmie politycznym irackich sunnitów, szczególnie plemion z terenów będących pod kontrolą PI. Dodatkowo do PI ciągnęli zdegradowani byli oficerowie oraz odsunięci od władzy członkowie elity baasistowskiej, którzy chcieli odzyskać choćby namiastkę dawnego Iraku. Także dla nich Kalifat stanowił jedynie środek do osiągnięcia zupełnie innego celu[82].

Arabia Saudyjska zagrała w Syrii oraz Iraku kartą salafizmu politycznego, aby przeciwstawić się zbliżeniu między Iranem, Irakiem Al-Malikiego i Syrią Al-Asada, do którego doszło po 2003 r. Ta koalicja powstała przy milczącym zaangażowaniu Rosji, a nawet Chin. Arabia Saudyjska uzyskała poparcie Turcji, Izraela i krajów Zatoki, a więc całego bloku proamerykańskiego. To przeciw Iranowi Arabia Saudyjska subwencjonowała Sadddama Husajna podczas wojny toczonej w latach 1980–1988, a przeciw Al-Asadowi wspierała dżihadyzm w Syrii, jednocześnie wysyłając za granicę rodzimych potencjalnych *troublemakerów*[83]. Obietnica udziału Ar-Rijadu w międzynarodowej koalicji skierowanej przeciw PI, ogłoszona 11 września 2014 r. przez prezydenta Obamę, dotyczyła jedynie sfery humanitarnej i logistycznej, bez angażowania wojska oraz sprzętu wojskowego. Arabia Saudyjska miała prawo czuć się zagrożona, ponieważ PI było wrogie dynastii Saudów, uważanej przez nich za skorumpowaną i pozostającą na usługach Amerykanów. Innymi słowy, instrument, który miał być wygodnym narzędziem polityki zagranicznej, wymknął się spod kontroli[84]. Podobnie Katar, sprzymierzony ze Stanami Zjednoczonymi, jest państwem, którego głównym celem jest obalenie reżimu Al-Asada, bliskiego Iranowi, i osłabienie Teheranu. Tym należy tłumaczyć finansowe i zbrojne wspieranie przez Katar rebeliantów[85] i organizowanie przerzutu dżihadystów z Maghrebu i Libii do Syrii przez Turcję, a do Iraku – przez iracki Kurdystan[86].

Te obawy podzielała również Turcja, która od samego początku wspierała rebeliantów przeciw Al-Asadowi. Zdaniem Hanne'a i Flichy de La Neuville'a to wsparcie wiązało się ze strategią wywierania wpływów, zmierzającą do odbicia południowych

[81] Tamże, s. XIV, 32.

[82] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 34–35, 63.

[83] Ang. *troublemaker* – 'wichrzyciel, awanturnik' (przyp. red.).

[84] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 121–122.

[85] P. Cockburn, *The Rise of the Islamic*…, s. 105–106.

[86] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 125.

rubieży kraju utraconych w 1920 r., które niegdyś stanowiły część Imperium Osmańskiego[87]. Także szkolenie żołnierzy WAS przez oficerów tureckich w bazie w Hatay było odpowiedzią na wsparcie, jakiego Damaszek udzielał Partii Pracujących Kurdystanu (kurd. Partiya Karkerên Kurdistanê, PKK), walczącej o niepodległość i podejmującej akcje terrorystyczne na wschodzie Turcji. Strategia oparta na dążeniach Kurdów do autonomii jest bardzo niebezpieczna dla Ankary, stąd Ankara także wykorzystywała dążenia salafitów.

Wielokrotnie pojawiały się zarzuty o to, że Turcja finansowała i wspierała Kalifat[88], a jednocześnie oskarżała Waszyngton o robienie tego samego[89]. Zarówno prezydent Recep Tayyip Erdoğan, jak i premier Ahmet Davutoğlu stanowczo zaprzeczali informacjom o jakiejkolwiek współpracy z PI. Jednak w ramach programu badawczego prowadzonego na uniwersytecie Columbia zespół naukowców ze Stanów Zjednoczonych, Europy i Turcji dokonał analizy mediów tureckich oraz międzynarodowych, aby zweryfikować zapewnienia polityków i ocenić wiarygodność zarzutów. Raport zawierający podsumowanie ich prac opublikowano w 2014 r., a zaktualizowano w 2015 r.[90] Można w nim znaleźć dane świadczące o tym, że twierdzenie rosyjskiego prezydenta Władimira Putina, jakoby Turcja była „wspólnikiem terrorystów"[91], nie było wyssane z propagandowego palca. Zarzuty obejmują wiele udokumentowanych działań, począwszy od dostaw sprzętu wojskowego dla PI przez pomoc transportową dla bojowników i ich wsparcie logistyczne, w tym pomoc przy rekrutacji nowych członków, opiekę medyczną oraz organizowanie szkoleń aż po ich finansowanie (przez zakup ropy). W raporcie można też znaleźć informacje o siłach tureckich walczących u boku dżihadystów, szczególnie w walkach o Kobani (Ajn al-Arab). Ponadto Turcja nie tylko bezpośrednio wspierała PI, lecz także od 2011 r. ułatwiała przemyt broni i gotówki oraz przejście przez granicę nowych rekrutów (mogli oni spokojnie przekraczać długą, wynoszącą 510 mil, granicę turecko-syryjską)[92]. Co prawda w późniejszym czasie Turcy poprawili szczelność granic, ale również potrzeby PI w tym zakresie uległy zmianie[93].

---

87 Tamże, s. 127–128.

88 D. Graeber, *Turkey could cut off Islamic State's supply lines. So why doesn't it?*, „The Guardian", 18 XI 2015 r., https://www.theguardian.com/commentisfree/2015/nov/18/turkey-cut-islamic-state-supply-lines-erdogan-isis [dostęp: 13 IV 2019].

89 T. O'Connor, *Does the US Fund Terror? Erdogan Says Turkey Has Evidence Washington Supports ISIS, Kurds*, „International Business Times", 27 XII 2016 r., http://www.ibtimes.com/does-us-fund-terror-erdogan-says-turkey-has-evidence-washington-supports-isis-kurds-2465915 [dostęp: 13 IV 2019].

90 D.L. Phillips, *Research Paper: ISIS-Turkey Links*, „The Huffington Post", 11 VIII 2014 r., http://www.huffingtonpost.com/david-l-phillips/research-paper-isis-turke_b_6128950.html [dostęp: 13 IV 2019].

91 R. Sidway, *Putin: Turkish leadership purposefully supports Islamization of country*, „Jihad Watch", 27 XI 2015 r., https://www.jihadwatch.org/2015/11/putin-turkish-leadership-purposefully-supports-islamization-of-country [dostęp: 13 IV 2019].

92 P. Cockburn, *The Rise of the Islamic*…, s. 7, 72.

93 Tamże, s. 156.

Niemiecka stacja Deutsche Welle jeszcze w 2016 r. informowała, że każdego dnia jeździ do Syrii kilkaset ciężarówek załadowanych towarami wartymi miliardy dolarów oraz że te towary trafiają prosto w ręce Kalifatu. Z wyemitowanego materiału jasno wynikało, że kanały zasilające PI wiodą prosto do Turcji[94].

Jako spadkobierca Imperium Osmańskiego, które było ostatnim sunnickim kalifatem rządzącym światem islamskim (i nie tylko) od XIV w. aż do 1924 r., Turcja ma ogromne możliwości propagowania islamu. Podręczniki historii w tureckich szkołach od dziesięcioleci apologetycznie opisują historię Imperium, w tym wszystkie jego wojny i podboje. Również islam odgrywa dużą rolę w społeczeństwie tureckim, chociaż konstytucja tego kraju czyni je wciąż oficjalnie świeckim. Według sondażu przeprowadzonego w 2014 r. aż 89 proc. tureckiego społeczeństwa uważa, że tym, co definiuje naród, jest przynależność do określonej religii[95].

Na tureckiej scenie politycznej nie ma opozycji na tyle silnej, aby zatrzymać lub przynajmniej skutecznie zakwestionować politykę Erdoğana. Dla Partii Sprawiedliwości i Rozwoju (tur. Adalet ve Kalkinma Partisi, AKP), której przewodniczył Erdoğan, reislamizacja Turcji jest priorytetem. Erdoğanowi może jednak zaszkodzić inny wróg, który może okazać się ważniejszy od PI. Sümeyye Erdoğan Bayraktar, córka tureckiego prezydenta, broniąc reżimu ojca, stwierdziła, że organizacja kierowana przez Fethullaha Gülena, który mieszka w Stanach Zjednoczonych, jest „właściwie bardziej niebezpieczna" od PI[96]. Te słowa padły podczas przemówienia wygłoszonego na 15. dorocznej konwencji *Muslim American Society-Islamic Circle of North America*, na której Sümeyye była jednym z głównych gości[97]. Można się zatem pokusić o postawienie

---

[94] *IS supply channels through Turkey*, Deutsche Welle, 26 XI 2016 r., http://www.dw.com/en/is-supply-channels-through-turkey/av-18091048 [dostęp: 13 IV 2019].

[95] Por. U. Bulut, *Churches in Turkey on the Verge of Extinction*, The Gatestone Institute, 19 IV 2015 r., https://www.gatestoneinstitute.org/5584/turkey-churches [dostęp: 13 IV 2019]. Ersin Kalaycioglu z uniwersytetu Sabanci oraz Ali Carkoglu z Koc University w ramach badania „Nacjonalizm w Turcji i na świecie" przeprowadzili wywiady z Turkami w wieku od 18 do 64 lat. Według nich „Turek to muzułmanin". Więcej na: E. Atalay, *Cihan devletinde yabancıya yer yok*, Agos, 26 VI 2014 r., http://www.agos.com.tr/tr/yazi/7434/cihan-devletinde-yabanciya-yer-yok [dostęp: 13 IV 2019].

[96] C. Ross, *Erdogan's Daughter Tells US Muslims That Gulen Movement Is 'More Dangerous' Than ISIS*, „The Daily Caller", 27 XII 2016 r., http://dailycaller.com/2016/12/27/erdogans-daughter-tells-us-muslims-that-gulen-movement-is-more-dangerous-than-isis-video/#ixzz4Xddy3va4 [dostęp: 13 IV 2019].

[97] Recep T. Erdoğan oskarżył gulenistów o próbę dokonania zamachu stanu (15 VII 2016 r.), skierowaną przeciw tureckiemu rządowi. Stwierdził wówczas, że to właśnie Fethullah Gülen był inspiratorem i mózgiem operacji przeprowadzonej przez członków tureckiej armii, w wyniku której życie straciło ponad 240 cywilów. Gulenistą miał być także Mevlut Mert Altintas, który w grudniu 2016 r. zamordował ambasadora Rosji Andrieja Karłowa. Nie wiadomo jedynie, dlaczego dokonał morderstwa, wznosząc palec wskazujący w geście, który stał się symbolem lojalności wobec PI (gest *tawhid* symbolizujący jedność Boga), i krzyczał: „Pamiętaj o Aleppo! Pamiętaj o Syrii!". Rola Rosji, która pomogła reżimowi Al-Asada wyprzeć rebeliantów z tego miasta, jest nie do przecenienia, rola gulenistów zaś pozostaje tajemnicą. Ostatecznie można przyjąć, że gest Altintasa był tylko celowym kamuflażem, nie wiadomo jednak, czemu miałby służyć.

tezy, że powodem, dla którego reżim Erdoğana wykazywał taką opieszałość w walce z PI, mogło być to, że chce on dokooptować Kalifat dżihadystów do własnego, tworzonego krok po kroku, neoottomańskiego kalifatu, którego centrum znajdowałoby się w Stambule. Konsekwentne i zdecydowane wysiłki Erdoğana nakierowane na zniszczenie świeckości państwa tureckiego są znane od lat. Równie często odnotowywano jego „neoosmańskie tendencje", czyli mówiąc wprost – chęć przywrócenia kalifatu. Jest zatem bardzo możliwe, że Erdoğan postrzegał Państwo Islamskie mniej jako wroga, a bardziej jako szansę na osiągnięcie tego celu. Wyobrażał sobie, że przy pomocy PI uda mu się pokonać innych wrogów Turcji, takich jak Kurdowie czy alawicki reżim w Damaszku[98], a przynajmniej utrzymać ich na dystans, dopóki nie nadarzy się okazja do tego, aby wykonać zdecydowany ruch i zebrać plony działalności PI. Przeniósłby przy tym siedzibę kalifatu nad Bosfor, sam zaś przyjąłby godność kalifa.

Ten scenariusz wyjaśniałby, dlaczego Ankara dystansuje się od polityki Zachodu i odmówiła podpisania we wrześniu 2014 r. dokumentu zobowiązującego kraje regionu Zatoki Perskiej do zwalczania PI, mimo że ta deklaracja była na tyle dyplomatyczna, że każde z podpisujących ją państw obiecywało walczyć z samozwańczym Kalifatem jedynie w takim stopniu, jaki uznało za „właściwy". Minister spraw zagranicznych Turcji Mevlüt Çavuşoğlu nie podpisał wspólnego komunikatu po spotkaniu 11 września w Dżuddzie i nie wydał zgody na wykorzystanie bazy lotniczej w İncirlik przez amerykańskie myśliwce. Mniej więcej w tym samym czasie Barackowi Obamie oraz Johnowi Kerry'emu nie udało się przekonać tureckiego rządu do działań przeciw PI, które handlowało ropą na czarnym rynku[99]. Tureckie władze wówczas wyjaśniały, że PI przetrzymuje 49 tureckich dyplomatów jako zakładników i grozi, że jeśli Turcja uderzy w PI, ich życie będzie zagrożone[100]. Turecki rząd wskazywał także na kurdyjskich uchodźców, których zwiększająca się liczba obciążała państwo, a jednocześnie zwiększała ryzyko wystąpienia przez Kurdów z żądaniami rewindykacji[101]. Pentagon nie reagował w obawie przed dalszym osłabieniem sojuszu, który już wtedy był jedynie „na papierze", a dziś jest jeszcze słabszy.

O ile państwa arabskie boją się Iranu i aspirowania przez Turcję do bycia regionalnym hegemonem, o tyle dla Iranu to PI było demonicznym tworem zbrojonym przez Stany Zjednoczone za pośrednictwem Arabii Saudyjskiej oraz Kataru, dążącym do zdestabilizowania reżimu Baszszara al-Asada, podzielenia Iraku oraz podporządkowania sobie szyitów. Celem nadrzędnym tych działań było sprawowanie kontroli nad złożami

[98] P. Cockburn, *The Rise of the Islamic*…, s. 37.

[99] D.E. Sanger, J. Hirschfeld Davis, *Turkey fails to cut Islamic State oil revenue despite US pressure*, „Sydney Morning Herald", 14 IX 2014 r., http://www.smh.com.au/world/turkey-fails-to-cut-islamic-state-oil-revenue-despite-us-pressure-20140914-10gpaq.html [dostęp: 13 IV 2019].

[100] Według O. Hanne'a i T. Flichy de La Neuville'a Rosja i Iran twierdzą, że więźniowie zostali wyzwoleni po negocjacjach, co czyniłoby z Turcji jedyne państwo świata utrzymujące tajne stosunki dyplomatyczne z PI. Zob. O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 131.

[101] Tamże, s. 130.

ropy naftowej[102]. To z kolei nie wykluczało nadziei Iranu na zwrócenie się przez Stany Zjednoczone do niego o pomoc w walce z Kalifatem, co pozwoliłoby Teheranowi na negocjowanie w sprawach arsenału nuklearnego oraz złagodzenia embarga ekonomicznego. W tym kontekście należy rozpatrywać podjęcie decyzji przez Teheran o zwiększeniu wydatków na cele wojskowe do 5 proc. budżetu[103]. Jednak wolta administracji prezydenta Donalda Trumpa w polityce bliskowschodniej położyła kres tym nadziejom. W tej geopolitycznej rozgrywce Iran nie ukrywa swojej współpracy z Rosją, aby przywrócić „pokój i bezpieczeństwo" na Bliskim Wschodzie[104].

Rosja Putina jest jednym z nielicznych państw konsekwentnie zachowujących swoją linię geopolityczną wobec Bliskiego Wschodu, którą Hanne i Flichy de La Neuville sprowadzają do trzech zasad: wspieranie Damaszku, traktowanie Teheranu jak partnera oraz odpowiadanie na terroryzm bezwzględną siłą (wynikające częściowo z doświadczeń afgańskich, a częściowo z doświadczeń czeczeńskich)[105]. Z perspektywy Rosji reakcja na siłę PI mogła być tylko jedna – okazanie jeszcze większej, bezwzględnej siły. Jednocześnie Rosja – w ramach prowadzonej polityki zagranicznej – nie traktowała instrumentalnie siły Kalifatu. Wydawałoby się zatem, że w tej sprawie Moskwa mogła osiągnąć porozumienie z Zachodem, jednak Stany Zjednoczone zdawały się dążyć do realizacji podobnych planów, ale z wykorzystaniem nieco innych środków.

Krótkowzroczna polityka Zachodu w zakresie sponsorowania syryjskiej rebelii przeciw Al-Asadowi zemściła się dosyć szybko. Już w sierpniu 2014 r. Stany Zjednoczone zostały zmuszone do przyznania, że nie są w stanie powstrzymać ekspansji dżihadystów bez współpracy z dyktatorem. Państwo Islamskie zdobyło Mosul 10 czerwca, Stany Zjednoczone natomiast zdecydowały się na użycie lotnictwa na terenie Syrii 23 września. Cockburn, zwracając uwagę na 105 dni dzielących te wydarzenia, sugeruje, że powodem zwłoki jest potraktowanie armii Kalifatu podobnie jak oddziałów beduińskich watażków wyłaniających się niespodziewanie na pustyni, zostawiających za sobą śmierć i zniszczenie, ale niezmieniających *status quo* regionu[106]. To z kolei budziło nadzieję, że Kalifat upadnie równie niespodziewanie i szybko, jak się pojawił. Tak się jednak nie stało. Priorytetami Zachodu były zatem powstrzymanie ekspansji terytorialnej Państwa Islamskiego oraz zmobilizowanie i wsparcie oponentów przy pomocy Stanów Zjednoczonych[107], które wyraźnie rozgraniczały dwie strefy interwencji: w Iraku dążono do osłabienia PI i zmuszenia go do wycofania się poza granicę syryjską, gdzie byłoby możliwe jego zniszczenie, w Syrii

[102] Tamże, s. 145.

[103] *Iran zwiększa budżet obronny*, Defence24, 9 I 2017 r., http://www.defence24.pl/523728,iran-zwieksza-budzet-obronny [dostęp: 13 IV 2019].

[104] *Iran, Russia reaffirm alliance in Syrian war*, „The Times of Israel", 3 XII 2016 r., http://www.timesofisrael.com/iran-russia-reaffirm-alliance-in-syrian-war [dostęp: 13 IV 2019].

[105] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 147.

[106] P. Cockburn, *The Rise of the Islamic*…, s. X, 28.

[107] K. Strachota, *Bliski Wschód w cieniu*…, s. 44.

natomiast skupiono się na trzech celach – PI, Dżabhat an-Nusra (paramilitarnej organizacji islamistycznej) oraz wojskowych obiektach reżimu. Według Hanne'a i Flichy de La Neuville'a naloty przeprowadzane w Syrii miały właśnie te trzy podstawowe cele[108]. Podkreślają oni także ironię sytuacji, w której działania Stanów Zjednoczonych bez rezolucji ONZ i zgody Rady Bezpieczeństwa stałyby się nielegalne z międzynarodowego punktu widzenia. Dla przykładu, między 8 sierpnia a 6 października 2014 r. przeprowadzono 250 nalotów na obiekty w Iraku i 90 w Syrii. Trzydzieści procent tych operacji dotyczyło dzielnic Ibrilu, Amerli i Bagdadu, czyli miast, o których się mówi, że nie uległy PI.

Zamierzeniem wielkiej koalicji powołanej podczas szczytu NATO w Newport (4–5 września 2014 r.), do której weszło 25 państw, było położenie kresu PI. W najsilniejszym składzie koalicja obejmowała ponad 60 państw, w tym wszystkie państwa Bliskiego Wschodu (bez Iranu, Izraela i Omanu). Jej część wojskową tworzyła armia amerykańska, francuska, brytyjska, kanadyjska, niemiecka, australijska i włoska; nie było natomiast kontyngentów żadnego państwa muzułmańskiego. Część humanitarną – najmniej kosztowną, ale najbardziej akceptowalną dla własnych obywateli – zapewniły Arabia Saudyjska, Kuwejt i Turcja. Za logistykę wzięły odpowiedzialność Zjednoczone Emiraty Arabskie oraz Katar[109]. Działało prawo siły, ale była to siła bezwładu, ponieważ działania koalicji bardzo przypominały działania prowadzone w czasie wojny w Zatoce w 1991 r. oraz podczas inwazji w 2003 r. – w dużej mierze winnej obecnej sytuacji. Słabości koalicji uwypuklało utworzenie jej w pośpiechu i niejako na siłę. Funkcjonowała ona przede wszystkim jako struktura wykorzystująca sprecyzowaną taktykę (naloty lotnicze oraz wsparcie irackich sił zbrojnych), ale bez jasno określonej strategii[110]. W ocenie Strachoty problemy koalicji były natury zarówno militarno-politycznej (brak prowadzonych i planowanych działań regularnych na lądzie), jak i strategicznej (brak strategii rozwiązania problemów w Syrii oraz Iraku, które to państwa dziś są utożsamiane z PI)[111]. Siłowe rozwiązanie problemu PI, argumentował Strachota, było z jednej strony zadaniem technicznie prostym, wymagającym zaangażowania sił zewnętrznych oraz konsolidacji lokalnych sił zwalczających Kalifat, z drugiej zaś – niemożliwym do zrealizowania właśnie z braku woli politycznej, wynikającej ze świadomości skutków wywołanych unicestwieniem PI. Rzeczywiście, jak można zaobserwować, rozbicie PI nie rozwiązało problemu terroryzmu ani nie zakończyło konfliktów w regionie, nie wyprowadziło go z kryzysu społeczno-gospodarczego ani z kryzysu wartości i tożsamości, nie poprawiło też bezpieczeństwa na Bliskim Wschodzie.

Sceptycyzm co do działań koalicji wypływał również z tego, że wojna prowadzona pod hasłem „zero zabitych" gwarantowała jedynie „zero zwycięstw"[112]. Wynikało to

[108] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 143.

[109] Tamże s. 140.

[110] Tamże, s. 141.

[111] K. Strachota, *Bliski Wschód w cieniu*…, s. 38–39.

[112] S. Laurent, *Kalifat Terroru. Kulisy*…, s. 141.

z taktyki rozpraszania swoich sił stosowanej przez PI. To z kolei osłabiało skuteczność nalotów (np. brak dużych skupisk uzbrojenia, które mogłyby zostać namierzone przez samoloty). Do 23 października 2016 r. zrealizowano w ramach koalicji 6600 operacji, z których jedynie 632 (czyli ok. 10 proc.) zakończyły się atakami na cele naziemne[113]. Ciekawie wypada też porównanie ataków lotniczych w Iraku i Syrii z innymi interwencjami[114]. Okazuje się, że były one nie tylko krótsze, lecz także mniej intensywne. W Kosowie (1999 r.) koalicja przez 90 dni dokonała 19 484 uderzeń (ponad 200 dziennie), w Afganistanie (2001 r.) – 6500 nalotów między 7 października a 17 grudnia, w Libii (2011 r.) przez 215 dni przeprowadzono 9700 akcji, czyli 45 dziennie, w Iraku i Syrii zaś (w 2015 r., do 31 marca) zrealizowano ich 2796, co daje zaledwie 15 takich akcji każdego dnia. W tym samym czasie, kiedy trwały naloty koalicji, PI zdobywało tereny, na których albo mogło liczyć na wsparcie ludności, albo było w stanie zdominować miejscowych sunnitów[115].

Należy jednak przyznać, że interwencja lądowa pociągnęłaby za sobą trudne do oszacowania straty (co prawda Kurdowie odgrywali rolę piechoty Stanów Zjednoczonych, ale okazało się to niewystarczające)[116]. W operacjach naziemnych najważniejszy jest teren, lud Iraku zaś to społeczeństwo plemienne, a plemiona są przywiązane do konkretnego terytorium. To zadecydowało o formie walki prowadzonej przez PI[117], szczególnie że plemiona były skupione na terenach wiejskich, na których bojownikom PI było dużo łatwiej się przemieszczać i rozbijać obóz[118]. Nie bez znaczenia było także to, że PI zawsze miało strategiczną inicjatywę, np. członkowie Kalifatu wykazywali większą aktywność w jednym miejscu kosztem działań w innym[119]. Nieefektywność nalotów wynikała nie tylko z tego, że przeciwnik skutecznie wykorzystywał swoją mobilność, rozproszenie i kamuflaż, lecz także z czynników normatywnych, np. niestosowania się przez niego do konwencji genewskich. Laurent przytoczył w tym kontekście słowa Abu Marjama:

> Nigdy nie zrzucicie tylu bomb, co Baszszar al-Asad, nigdy nie będziecie systematycznie bombardować meczetów, szkół ani szpitali, tylko dlatego, że dżihadyści często chronią się w takich miejscach. Nie użyjecie śmiertelnego gazu w mieście, mając nadzieję, że oprócz kobiet i dzieci ta operacja zabije również kilku bojowników. Nie wyślecie własnych ludzi na rzeź, by bronić rękami i nogami każdej uliczki w każdej wiosce, wiedząc, że większość z nich straci głowy. Nie zrobicie

[113] P. Cockburn, *The Rise of the Islamic*…, s. 160.

[114] D. Kilcullen, *Blood Year: Terror and the Islamic State*, Quarterly Essay 2015, t. 58, https://www.quarterlyessay.com/essay/2015/05/blood-year [dostęp: 13 IV 2019].

[115] M. Weiss, H. Hassan, *ISIS. Wewnątrz armii terroru*…, s. 367.

[116] S. Laurent, *Kalifat terroru. Kulisy*…, s. 152.

[117] M. Weiss, H. Hassan, *ISIS. Wewnątrz armii terroru*…, s. 313.

[118] Tamże, s. 316.

[119] Tamże, s. 366.

> żadnej z tych rzeczy, a nawet gdybyście byli na to gotowi, inni przed wami już próbowali. I mimo to Państwo Islamskie przetrwało[120].

Tam, gdzie siła militarna dawała przewagę, słabość cywilizacyjna związywała ręce. Pomimo względnej słabości Państwa Islamskiego, szczególnie w kontekście połączonych sił wielu jego wrogów, sprzeczne często założenia geopolityczne koalicjantów i różne podejścia do PI sprawiły, że szybko stało się ono faktem politycznym na mapie Bliskiego Wschodu i było siłą, z którą trzeba było się liczyć w politycznych kalkulacjach.

Efekt przesilenia?

Na siłę Państwa Islamskiego składały się następujące elementy: złożona struktura armii i przyjęcie taktyki odmiennej od zachodniej, w tym dobrze określone kierunki działań wojennych, wysokie morale i wyszkolenie, dobre dowodzenie, a także inkluzywny charakter organizacji. Polityka Al-Kaidy zmierzała przede wszystkim do destabilizacji, PI skupiało się natomiast głównie na tworzeniu struktur państwowych na kontrolowanym przez siebie terytorium, z własną armią, aparatem bezpieczeństwa i sądowniczym, systemem edukacji i gospodarczym (podatki, przedsiębiorstwa, a nawet własna moneta)[121]. Co więcej, PI wykazało się ogromnymi zdolnościami adaptacyjnymi (podejmowanie działań o różnym charakterze), odpornością na straty (w ludziach, terytorialne), zdolnością do kumulacji doświadczeń i otwartością na nowe formy aktywności, a także akceptacją nowych sił i otwartością na nowe środowiska (np. uznające tych samych wrogów, a niekoniecznie podzielające radykalne islamskie hasła PI, byłych funkcjonariuszy partii Baas i oficerów Saddama Husajna), czyli wejściem na zupełnie nowy poziom działań wojskowych, politycznych, ideologicznych i terytorialnych[122]. Nie sposób nie zgodzić się z Ramsauer, że Państwo Islamskie było (…) *czymś więcej niż tylko kolejnym ugrupowaniem terrorystycznym*[123]. Było to państwo, ideologia i zarazem w dużej części ruch protestu, któremu nie chodziło o to, aby we wstrząsanej wojną domową Syrii oraz w ustawicznie niestabilnym Iraku zdobyć pozycję nowej władzy, zaprowadzającej porządek lub urzeczywistniającej utopię kalifatu, ponadnarodowego państwa wszystkich muzułmanów. Chodziło raczej o utworzenie struktur siły opartej zarówno na przemocy, jak i ideologii terroryzowania reszty świata.

W ewolucji od organizacji terrorystycznej do protopaństwa oraz od organizacji terrorystycznej do armii operacyjnej PI, stosując *soft power* i *hard power*, tworzyło świat równoległy do istniejącego systemu stosunków międzynarodowych. Głównym

[120] S. Laurent, *Kalifat terroru. Kulisy*…, s. 145.

[121] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 35.

[122] K. Strachota, *Bliski Wschód w cieniu*…, s. 9–11.

[123] P. Ramsauer, *Pokolenie dżihadu. Europo*…, s. 20, 24.

wrogiem byli *kuffar*, czyli niewierni. W podziale ludzi pomagało oddzielenie dżihadu od spraw religijnych (oraz lansowany przez Kalifat takfiryzm[124], dopuszczający atakowanie innych muzułmanów, jeśli na podstawie swojego zachowania zostaną uznani za niewiernych)[125]. Ma jednak rację Ramsauer, która pisze, że gotowość Kalifatu do stosowania przemocy, nienawiść i fanatyzm o nieporównywalnym poziomie okrucieństwa, nie wykluczają tego, że zbrodnie były popełniane zgodnie z zasadami bezlitosnej, ale jednak militarnej logiki[126]. Zasada siły i systematycznego stosowania przemocy dotyczyła nie tylko wrogów zewnętrznych, lecz także wewnętrznych, w tym ludności cywilnej. Przejawem tego było systematyczne dopuszczanie się przemocy wobec ludności cywilnej oraz sadyzm, zarówno milicji, jak i pojedynczych bojowników. Sadyzm był znakiem rozpoznawczym dżihadystów oraz motywem przewodnim w wydawanych przez nich materiałach propagandowych, epatujących brutalnością działań: eksterminacjami jeńców i ludności cywilnej, czystkami etnicznymi i religijnymi oraz masowymi gwałtami.

Dla Stanów Zjednoczonych i całego Zachodu istnienie i działania Państwa Islamskiego oznaczały fiasko prowadzonej dotychczas polityki, dla niektórych państw regionu (Irak, Syria) były zagrożeniem ich egzystencji, dla innych – nieco nieobliczalnym, ale użytecznym instrumentem przydatnym do rozwiązań siłowych (Arabia Saudyjska, Katar), dla jeszcze innych (Turcja) – czynnikiem, którego siłę można było wykorzystać do realizacji własnych zadań. Laurent postawił tezę, że rozwiązania siłowe były na rękę Państwu Islamskiemu, które złapało Zachód w pułapkę wojny będącej uzasadnieniem dżihadu zakrojonego na szeroką skalę[127]. To właśnie przez prowadzenie działań wojennych Zachód potwierdził status kalifa Al-Baghdadiego. Wojna była także wyrazem uznania dla Państwa Islamskiego, co pozwoliło na skupienie wokół niego wszystkich radykalnych muzułmanów przez przedstawienie tego konfliktu jako nowej „krucjaty". *Czy rzeczywiście główną troską Zachodu było powstrzymanie średniowiecznego barbarzyństwa* – pytał retorycznie Jürgen Todenhöfer[128], i postawił tezę, że w rozgrywce chodziło przede wszystkim o zabezpieczenie interesu ekonomicznego, a konkretnie – o swobodny dostęp do pól naftowych, kontrolę nad strategicznym rurociągiem do Turcji i transport ropy. Według niego terroryści postrzegali swoją politykę jako uprawnioną odpowiedź na agresywne i łupieżcze zachowanie Stanów Zjednoczonych, które traktują ich kraje wyłącznie jako stacje benzynowe. Jednak taka analiza przedstawia PI jedynie jako najbardziej radykalną reakcję na agresywną politykę Zachodu – i tym samym zdaje się ignorować jego swoistą podmiotowość.

[124] Arab. *takfir* – 'wyrzeczenie się wiary' (przyp. red.).

[125] M. Weiss, H. Hassan, *ISIS. Wewnątrz armii terroru*…, s. 78.

[126] P. Ramsauer, *Pokolenie dżihadu. Europo*…, s. 19, 31.

[127] S. Laurent, *Kalifat terroru. Kulisy*…, s. 153.

[128] J. Todenhöfer, *ISIS od środka. 10 dni*…, s. 21, 28.

Krzysztof Strachota[129] podkreślił, że samo istnienie PI rzuciło wyzwanie całemu porządkowi polityczno-społecznemu w regionie Bliskiego Wschodu, gdyż negując legitymację reżimów, podważyło przeniesioną z Zachodu hierarchię norm politycznych. Zasada republikańskiej formy rządów została zastąpiona monarchią teokratyczną (kalifatem) i konceptem narodu tworzącego państwo – *ummę* (wspólnotę wiernych), a prawo międzynarodowe regulujące procesy państwowotwórcze oraz instytucje stające na jego straży – szariatem. Jednocześnie Kalifat rzucił bezpośrednie wyzwanie regionalnemu systemowi bezpieczeństwa podporządkowanemu interesowi Stanów Zjednoczonych, ponieważ obecny porządek geopolityczny, który jest wynikiem dominacji Zachodu w wymiarze zarówno cywilizacyjnym, politycznym, ekonomicznym, jak i wojskowym, powoli się kończy.

W ocenie Richarda Berretta Państwo Islamskie było wpadką historii[130]. Olivier Hanne i Thomas Flichy de La Neuville zgadzają się, że jeśli już musi się postrzegać PI jako przypadek, to śmiertelny[131]. Ta ocena nie wydaje się aż tak kontrowersyjna, jeśli przypomni się, że sukces PI był oznaką słabości polityki państw regionu i koalicji, i to słabości nie tyle wojskowej czy ekonomicznej, ile ideowej. Plany PI były długofalowe, a wyrastały z koncepcji, które żyją życiem niezależnym, zarówno od sukcesów, jak i porażek tej organizacji. Organizacji, która – jak już wspomniano – na swoim czarnym sztandarze niosła idee. Przenosząc dżihad na poziom państwowy, legitymizowano siłę jako nieodzowny element rzeczywistości geopolitycznej na Bliskim Wschodzie (dotychczas dżihad był potocznie kojarzony z podmiotami niepaństwowymi, głównie organizacjami terrorystycznymi). Potęga militarna Kalifatu się zakończyła, ale duch symbolizujący Państwo Islamskie przerósł jego siłę wojskową, instytucjonalną, ekonomiczną i terytorialną. Może to miał na myśli B. Obama, który 24 września 2014 r. powiedział, że należy „wypowiedzieć wojnę wojnie"[132]. Jednak wojny nie wystarczy tylko wypowiedzieć, należy ją jeszcze wygrać. To wciąż przed nami.

Bibliografia

Atalay E., *Cihan devletinde yabancıya yer yok*, Agos, 26 VI 2014 r., http://www.agos.com.tr/tr/yazi/7434/cihan-devletinde-yabanciya-yer-yok [dostęp: 13 IV 2019].

Barrett R., *The Islamic State*, The Soufan Group, X 2014, http://soufangroup.com/wp-content/uploads/2014/10/TSG-The-Islamic-State-Nov14.pdf [dostęp: 13 IV 2019].

[129] K. Strachota, *Bliski Wschód w cieniu*…, s. 14–15, 23, 24.

[130] R. Barrett, *The Islamic State*, The Soufan Group, X 2014 r., http://soufangroup.com/wp-content/uploads/2014/10/TSG-The-Islamic-State-Nov14.pdf [dostęp: 13 IV 2019].

[131] O. Hanne, T. Flichy de La Neuville, *Państwo Islamskie*…, s. 151.

[132] Przemówienie wygłoszone podczas 69. sesji Zgromadzenia Ogólnego Organizacji Narodów Zjednoczonych. Pełny tekst jest dostępny na: http://www.independent.co.uk/news/world/americas/barack-obamas-speech-to-the-un-in-full-9753615.html [dostęp: 13 IV 2019].

Bartoszewicz M.G., *Reconciliation in the Shadow of ISIS*, w: *Oblicza pojednania: Faces of Reconciliation*, J. Kulska (red.), Opole 2016, Wydawnictwo Uniwersytetu Opolskiego, s. 241–256.

Bulut U., *Churches in Turkey on the Verge of Extinction*, The Gatestone Institute, 19 IV 2015 r., https://www.gatestoneinstitute.org/5584/turkey-churches [dostęp: 13 IV 2019].

Cavanaugh W., *The Myth of Religious Violence*, Oxford 2009, Oxford University Press.

Cockburn P., *The Rise of the Islamic State*, New York–London 2015, Verso.

DeJesus K.M. *ISIS: The Rise of the Islamic State*, Santa Barbara 2017, Praeger Security International.

Estulin D., *W imię Allaha*, Katowice 2016, Sonia Draga.

Fromkin D., *A Peace to End All Peace: The Fall of the Ottoman Empire and the Creation of the Modern Middle East*, London 2001, Macmillan.

Gerges F.A., *ISIS: A History*, Princeton 2016, Princeton University Press.

Graeber D., *Turkey could cut off Islamic State's supply lines. So why doesn't it?*, „The Guardian", 18 XI 2015 r., https://www.theguardian.com/commentisfree/2015/nov/18/turkey-cut-islamic-state-supply-lines-erdogan-isis [dostęp: 13 IV 2019].

Hanne O., Flichy de La Neuville T., *Państwo Islamskie. Geneza nowego kalifatu*, Warszawa 2015, Dialog.

Hénin N., *Jihad Academy: The Rise of Islamic State*, New Delhi 2015, Bloomsbury.

Iran, Russia reaffirm alliance in Syrian war, „The Times of Israel", 3 XII 2016 r., http://www.timesofisrael.com/iran-russia-reaffirm-alliance-in-syrian-war/ [dostęp: 13 IV 2019].

Iran zwiększa budżet obronny, Defence24, 9 I 2017 r., http://www.defence24.pl/523728,iran--zwieksza-budzet-obronny [dostęp: 13 IV 2019].

IS supply channels through Turkey, Deutsche Welle, 26 XI 2016 r., http://www.dw.com/en/is-supply-channels-through-turkey/av-18091048 [dostęp: 13 IV 2019].

Kilcullen D., *Blood Year: Terror and the Islamic State*, „Quarterly Essay" 2015, t. 58, https://www.quarterlyessay.com/essay/2015/05/blood-year [dostęp: 13 IV 2019].

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

McCants W. i in., *The Islamic State's Ideology & Propaganda*, The Brookings Project on U.S. Relations with the Islamic World Events 2015 (wideo), http://www.brookings.edu/events/2015/03/11-islamic-state-ideology-propaganda [dostęp: 13 IV 2019].

McCants W., *The ISIS Apocalypse: The History, Strategy, and Doomsday Vision of the Islamic State*, New York 2015, St. Martin's Press.

Nance M., *Defeating ISIS: Who they Are, How they Fight, What they Believe,* New York 2016, Skyhorse Publishing.

O'Connor T., *Does the US Fund Terror? Erdogan Says Turkey Has Evidence Washington Supports ISIS, Kurds*, „International Business Times", 27 XII 2016 r., http://www.ibtimes.com/does-us-fund-terror-erdogan-says-turkey-has-evidence-washington-supports-isis--kurds-2465915 [dostęp: 13 IV 2019].

Phillips D.L., *Research Paper: ISIS-Turkey Links*, „The Huffington Post", 11 VIII 2014 r., http://www.huffingtonpost.com/david-l-phillips/research-paper-isis-turke_b_6128950.html [dostęp: 13 IV 2019].

Ramsauer P., *Pokolenie dżihadu. Europo, czeka cię apokalipsa!*, Warszawa 2016, Muza.

Ross C., *Erdogan's Daughter Tells US Muslims That Gulen Movement Is 'More Dangerous' Than ISIS*, „The Daily Caller", 27 XII 2016 r., http://dailycaller.com/2016/12/27/erdogans-daughter-tells-us-muslims-that-gulen-movement-is-more-dangerous-than-isis-video/#ixzz4Xddy3va4 [dostęp: 13 IV 2019].

Sanger D.E., Hirschfeld Davis J., *Turkey fails to cut Islamic State oil revenue despite US pressure*, „Sydney Morning Herald", 14 IX 2014 r., http://www.smh.com.au/world/turkey-fails-to-cut-islamic-state-oil-revenue-despite-us-pressure-20140914-10gpaq.html [dostęp: 13 IV 2019].

Shamieh L., Szenes Z., *The Propaganda of ISIS/DAESH through the Virtual Space*, „Defence Against Terrorism Review" 2015, nr 1, s. 7–31.

Sidway R., *Putin: Turkish leadership purposefully supports Islamization of country*, „Jihad Watch", 27 XI 2015 r., https://www.jihadwatch.org/2015/11/putin-turkish-leadership-purposefully-supports-islamization-of-country [dostęp: 13 IV 2019].

Skillicorn D.B., *Empirical Assessment of al Qaeda, ISIS, and Taliban Propaganda* (szkic), [bmw] 2015, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2546478 [dostęp: 13 IV 2019].

Souad M., *The terrorists fighting us now? We just finished training them*, „The Washington Post", 18 VIII 2014 r., https://www.washingtonpost.com/posteverything/wp/2014/08/18/the-terrorists-fighting-us-now-we-just-finished-training-them/?utm_term=.f59f2cc2a47f [dostęp: 13 IV 2019].

Stalinsky S. (M. Khayat i R. Sosnow, współpraca), *ISIS's Use Of Twitter, Other U.S. Social Media To Disseminate Images, Videos Of Islamic Religious Punishments – Beheading, Crucifixion, Stoning, Burning, Drowning, Throwing From Buildings – Free Speech?*, „Middle East Media Research Institute" 2016, Inquiry & Analysis Series nr 1218, https://www.memri.org/reports/isiss-use-twitter-other-us-social-media-disseminate-images-videos-islamic-religious [dostęp: 13 IV 2019].

Strachota K., *Bliski Wschód w cieniu Państwa Islamskiego*, seria: Punkt Widzenia OSW, nr 52, Warszawa 2015.

Todenhöfer J., *ISIS od środka. 10 dni w „Państwie Islamskim”*, Kraków 2015, Wydawnictwo Uniwersytetu Jagiellońskiego.

Wasington's Blog, Masden W., Syrian Girl Partisan, Leonard J.P., *ISIS IS US: The Schocking Truth Behind the Army of Terror*, San Diego 2015, Progressive Press.

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

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

Winter C., *The Virtual "Caliphate": Understanding Islamic State's Propaganda Strategy*, „Quilliam Report" 2015, http://www.quilliamfoundation.org/wp/wp-content/uploads/publications/free/the-virtual-caliphate-understanding-islamic-states-propaganda-strategy.pdf [dostęp: 13 IV 2019].

Wood G., *What ISIS really wants*, „The Atlantic" 2015, marzec, http://www.theatlantic.com/magazine/archive/2015/03/what-isis-really-wants/384980/ [dostęp: 13 IV 2019].

Abstrakt

Po październiku 2017 r. pojawiła się pokusa, aby Państwo Islamskie włożyć do lamusa historii i zaprzestać rozważań nad jego istnieniem i oddziaływaniem. Ale to właśnie teraz nadszedł czas na rzetelne analizy i refleksje nad tym fenomenem. W niniejszym artykule omówiono funkcjonowanie PI przy uwzględnieniu jego statusu i celów, jego sojuszników oraz zasięgu terytorialnego, a także dokonano analizy zasobów zarówno twardej, jak i miękkiej siły jego oddziaływania. Na siłę PI składały się następujące elementy: złożona struktura jego armii i różnice taktyczne, w tym dobrze określone kierunki działań wojennych, wysokie morale i wyszkolenie jego żołnierzy, dobre dowodzenie, oraz inkluzyjny charakter organizacji. Państwo Islamskie wykazało się ogromnymi zdolnościami adaptacyjnymi (różne teatry działań), odpornością na straty (ludzkie, terytorialne), zdolnością do kumulacji doświadczeń i otwartością na nowe formy aktywności, ale także na nowe kręgi zwolenników, czy też raczej – wejściem na zupełnie nowy poziom działań wojskowych, politycznych, ideologicznych i terytorialnych.

W drugiej części artykułu autorka skupiła się na analizie głównych uczestników wydarzeń bliskowschodnich, którzy często wykorzystywali Kalifat (lub walkę z nim) do osiągnięcia własnych, partykularnych interesów za pomocą rozwiązań siłowych. Odnosi się zarówno do podmiotów lokalnych (państwa arabskie, Iran, Turcja), jak i międzynarodowych (Stany Zjednoczone wraz z zachodnimi sojusznikami, Rosja), porównując ich podejście do PI. Taka analiza pozwala na określenie, jak wysoko w hierarchii celów strategicznych tych państw znajduje się ostateczne wyeliminowanie Kalifatu oraz jak skuteczna jest polityka prowadzona za pomocą siły militarnej i potęgi ekonomicznej. Dla Stanów Zjednoczonych i całego Zachodu istnienie i działania PI oznaczały

fiasko prowadzonej dotychczas polityki; dla niektórych państw regionu (Irak, Syria) stanowiło ono zagrożenie dla ich egzystencji, dla innych – było nieco nieobliczalnym, ale użytecznym instrumentem przydatnym do rozwiązań siłowych (Arabia Saudyjska, Katar), dla jeszcze innych (Turcja) – czynnikiem, którego siłę można wykorzystać do własnych celów.

Słowa kluczowe: Państwo Islamskie, Kalifat, siła militarna, *soft power*, geopolityka.

Abstract

After October 2017, a temptation appeared to put the "Islamic State" in the junkyard of history and to stop pondering about its existence and impact. To the contrary, now the time has come for meticulous analyses and reflections concerning this phenomenon. This article discusses the functioning of IS based on its strength and taking into account its status and goals, allies and territorial coverage, as well as analyzing both hard and soft power of its impact. It is claimed that the strength of PI consisted of the following elements: the complex structure and tactical differences, including well-defined goals of military operations, high morale and training, good command, but also the inclusive nature of the organization. What is more, the Islamic State has shown a great adaptability (various theaters of activities), resistance to losses (human, territorial), the ability to accumulate experiences and an openness to new forms of activity. Furthermore, its inherent strength and the enabling milieu allowed it for achieving a completely new level of military, political, ideological and territorial activities.

In the second part of the article, the analysis focuses on the main actors of Middle Eastern events who often used the Caliphate (or the purported struggle against it) as an object of power play to achieve their own particular interests. Specifically, the reflections include local actors (the Arab states, Iran, Turkey) and international (US together with its Western allies and Russia). This comparative analysis allows to determine how high in the hierarchy of their strategic goals the ultimate elimination of the Islamic State could be placed. This is followed by an evaluation of policy effectiveness. The paper concludes that for America and the whole West, the existence and operation of the Islamic State meant the failure of the hitherto policies in the Middle East; for some countries in the region (Iraq, Syria) it was an existential threat, for others a somewhat unpredictable but useful instrument (Saudi Arabia, Qatar), or even (Turkey) a factor whose power can be used for its own purposes.

Keywords: Islamic State, Caliphate, hard power, soft power, geopolitics.

Leszek Wiszniewski

Rola i znaczenie analizy informacji wywiadowczej w zapewnianiu bezpieczeństwa państwa

W XXI w. ludzie są zmuszeni do odbioru coraz większej ilości informacji, mniej lub bardziej przydatnych. Jednym z głównych czynników wpływających na to zjawisko jest technologia rozwijająca się w zawrotnym tempie. Osoby korzystające z Internetu, w tym z portali społecznościowych (m.in. takich, jak Facebook, Twitter, YouTube) są adresatami 34 gigabajtów danych, co według naukowców z University of California w San Diego przekłada się na 100 tys. słów dziennie (ponad dwa razy tyle co na początku lat 80. poprzedniego stulecia)[1]. To powoduje konieczność szybkiego przetwarzania wiadomości i przyporządkowywania im odpowiednich stopni ważności. Z podobnymi problemami zmagają się politycy sprawujący w kraju funkcje kierownicze. Nadmiar informacji często utrudnia im podjęcie decyzji, od których może zależeć życie i zdrowie obywateli. Z tego względu, z uwagi na dynamicznie zmieniające się środowisko bezpieczeństwa państwa oraz mnogość wyzwań i zagrożeń wynikających z tego procesu, nastąpi wzrost znaczenia analizy informacji. Dla rządów szczególnie istotne będą materiały opracowane na podstawie danych pochodzących ze źródeł niejawnych. Tego rodzaju materiały umożliwiają właściwą ocenę sytuacji geopolitycznej (m.in. w przypadku działań hybrydowych prowadzonych przez przeciwnika, w tym dezinformacji) oraz podejmowanie działań wyprzedzających (np. zapobieganie zamachom terrorystycznym przez aresztowania osób zaangażowanych w ich przygotowania czy prewencyjne stosowanie środków bezpieczeństwa w przypadku nieprecyzyjnych sygnałów o potencjalnym zagrożeniu). Zwiększy się także rola służb specjalnych (wywiadu, kontrwywiadu) i formacji mundurowych, którym ustawodawca przyznał kompetencje do operacyjnego gromadzenia informacji oraz sporządzania na ich podstawie odpowiednio przygotowanych produktów analitycznych dla decydentów.

W pierwszej części opracowania zostanie omówiony problem analizy informacji w ujęciu teoretycznym, w tym kwestie definicyjne oraz cykl analityczny, ze szczególnym uwzględnieniem sposobów pozyskiwania informacji oraz rodzajów analizy. W drugiej części zostaną przedstawione uwarunkowania prawne dotyczące wybranych

[1] *The American Diet: 34 Gigabytes a Day*, https://bits.blogs.nytimes.com/2009/12/09/the-american-diet-34-gigabytes-a-day/?_r=0 [dostęp: 3 IX 2019].

polskich instytucji odpowiedzialnych za zapewnianie bezpieczeństwa państwa, które w ramach swoich kompetencji przygotowują analizy.

Kwestie definicyjne

Na początku rozważań nad problemem analizy informacji należy odwołać się do literatury naukowej, aby poprawnie rozumieć terminy używane w niniejszej pracy. W *Słowniku języka polskiego PWN* znajdują się definicje, zgodnie z którymi analiza to ‘myślowe wyodrębnienie właściwości lub składników badanego zjawiska czy też przedmiotu’[2], a informacja to ‘powiadomienie o czymś, zakomunikowanie czegoś; wiadomość, pouczenie’[3]. W materiałach akademickich pojawia się także sformułowanie, że „informacja” to (…) *zbiór faktów, zdarzeń, cech itp. określonych obiektów (rzeczy, procesów, systemów) zawarty w wiadomości (komunikacie), tak ujęty i podany w takiej postaci (formie), że pozwala odbiorcy ustosunkować się do zaistniałej sytuacji i podjąć odpowiednie działania umysłowe lub fizyczne*[4]. W literaturze specjalistycznej z dziedziny wojskowości i bezpieczeństwa można przeczytać, że (…) *analiza informacji w dziedzinie bezpieczeństwa państwa polega na nadawaniu sensu tej informacji, czyli (1) obejmuje poprawne wnioskowanie o konsekwencjach treści informacji i (2) maksymalizuje użyteczność informacji w podejmowaniu decyzji przez odbiorcę, dzięki sformułowaniu rekomendacji określonych działań*[5]. Istotne pozostaje także rozumienie pojęcia bezpieczeństwo informacyjne. W literaturze przedmiotu jest ono używane w dwóch kontekstach. Pierwszy z nich odnosi się bardziej do zagrożeń związanych z przetwarzaniem informacji, co potwierdzają Piotr Potejko (*bezpieczeństwo informacyjne stanowi zbiór działań, metod, procedur, podejmowanych przez uprawnione podmioty, zmierzających do zapewnienia integralności gromadzonych, przechowywanych i przetwarzanych zasobów informacyjnych, poprzez zabezpieczenie ich przed niepożądanym, nieuprawnionym ujawnieniem, modyfikacją, zniszczeniem*[6]) i Krzysztof Liedel (*bezpieczeństwo informacyjne bardzo często rozumiane jest jako ochrona informacji przed niepożądanym – przypadkowym lub świadomym – ujawnieniem, modyfikacją, zniszczeniem lub uniemożliwieniem jej przetwarzania*[7]). Nieco inne rozumienie tego terminu proponuje Leszek Korzeniowski, który uważa, że (…) *przez bezpieczeństwo informacyjne podmiotu (człowieka lub organizacji) należy*

[2] L. Drabik, E. Sobol, *Słownik języka polskiego,* Warszawa 2005, s. 14.

[3] Tamże, s. 277.

[4] P. Sienkiewicz, *10 wykładów,* Warszawa 2005, s. 62.

[5] J. Konieczny, *Analiza informacji w dziedzinie bezpieczeństwa państwa*, Warszawa 2014, s. 256.

[6] P. Potejko, *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), Warszawa 2009, s. 194.

[7] K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, s. 19.

rozumieć możliwość pozyskania dobrej jakości informacji oraz ochrony posiadanej informacji przed jej utratą[8]. Ten pogląd podzielają Krzysztof Liderman (*bezpieczeństwo informacyjne oznacza uzasadnione zaufanie podmiotu do jakości i dostępności pozyskiwanej oraz wykorzystywanej informacji*[9]) oraz Józef Janczak i Andrzej Nowak, którzy twierdzą, że (…) *kiedy mówi się o bezpieczeństwie informacyjnym, to zawsze dotyczy to podmiotu, który jest zagrożony poprzez brak informacji lub możliwość utraty zasobów informacyjnych*[10]. Próbę doprecyzowania terminu bezpieczeństwo informacyjne państwa podjęli eksperci Biura Bezpieczeństwa Narodowego. W projekcie *Doktryny bezpieczeństwa informacyjnego RP* z 2015 r. przedstawili „bezpieczeństwo informacyjne państwa" jako:

> (…) transsektorowy obszar bezpieczeństwa, którego treść odnosi się do środowiska informacyjnego (w tym cyberprzestrzeni) państwa; proces, którego celem jest zapewnienie bezpiecznego funkcjonowania państwa w przestrzeni informacyjnej poprzez panowanie we własnej, wewnętrznej, krajowej infosferze oraz efektywną ochronę interesów narodowych w zewnętrznej (obcej) infosferze. Osiąga się to poprzez realizację takich zadań, jak: zapewnienie adekwatnej ochrony posiadanych zasobów informacyjnych oraz ochrony przed wrogimi działaniami dezinformacyjnymi i propagandowymi (w wymiarze defensywnym) przy jednoczesnym zachowaniu zdolności do prowadzenia wobec ewentualnych przeciwników (państw lub innych podmiotów) działań ofensywnych w tym obszarze. Zadania te konkretyzowane są w strategii (doktrynie) bezpieczeństwa informacyjnego (operacyjnej i preparacyjnej), a do ich realizacji utrzymuje się i rozwija odpowiedni system bezpieczeństwa informacyjnego[11].

Na potrzeby pracy warto przyjąć szerszą – proponowaną przez Korzeniowskiego czy Lidermana – definicję terminu „bezpieczeństwo informacyjne", która odnosi się do możliwości pozyskiwania informacji pozwalających decydentom na zapewnienie bezpieczeństwa państwa.

Podrozdział poświęcony kwestiom definicyjnym jest także miejscem, w którym należy wytłumaczyć, czym jest propaganda (dezinformacja) oraz zjawisko szumu informacyjnego, które w ostatnim czasie stały się przedmiotem debaty w polskiej przestrzeni publicznej. „Dezinformacja" to komunikat sprzeczny z rzeczywistością, który może być (…) *elementem walki informacyjnej pomiędzy konkurującymi podmiotami*[12] (np. państwami czy przedsiębiorstwami). „Propaganda" i „dezinformacja" zostały szerzej zdefiniowane w projekcie *Doktryny bezpieczeństwa*

---

[8] L.F Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, s. 147.

[9] K. Liderman, *Bezpieczeństwo informacyjne*, Warszawa 2012, s. 22.

[10] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, s. 18.

[11] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 3 IX 2017].

[12] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 36.

informacyjnego RP. Jest to: (…) *rozpowszechnianie zmanipulowanych lub sfabrykowanych informacji (albo kombinacji jednych i drugich), w celu skłonienia ich odbiorców do określonych zachowań korzystnych dla dezinformującego, lub też w celu odwrócenia ich uwagi od faktycznie zaistniałych wydarzeń*[13]. Terminem „szum informacyjny" językoznawcy określają 'nadmiar informacji utrudniający wyodrębnienie informacji prawdziwych i istotnych'[14].

Cykl wywiadowczy

Analiza danych jest tylko jednym z wielu etapów procesu, którego celem jest wsparcie informacyjne władz danego państwa w podejmowaniu decyzji pozwalających zapewnić obywatelom szeroko rozumiane bezpieczeństwo. W literaturze przedmiotu ten proces tradycyjnie określa się mianem cyklu wywiadowczego, na który składa się przeważnie – w zależności od taksonomii przyjętej przez poszczególnych naukowców – od czterech do sześciu etapów. Na potrzeby niniejszej publikacji przyjęto cztery etapy tego cyklu, obejmujące:

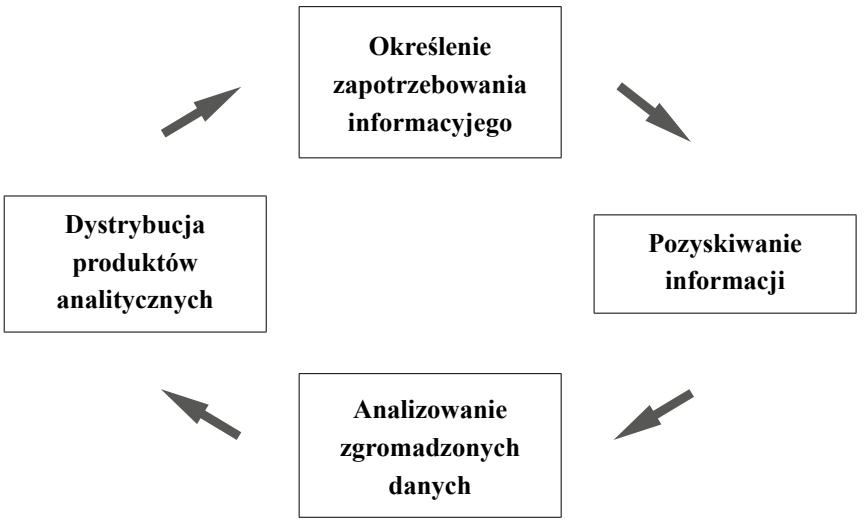
1) **określenie zapotrzebowania informacyjnego** przez organy państwowe, upoważnione do tego na podstawie obowiązującego prawa, oraz zlecenie zadań podległym im instytucjom (m.in. służbom bezpieczeństwa i porządku publicznego, agencjom wywiadowczym i kontrwywiadowczym). Ten etap jest ściśle skorelowany z bieżącymi wydarzeniami na świecie czy zjawiskami (np. konfliktami zbrojnymi, terroryzmem), które mogą negatywnie wpływać na bezpieczeństwo państwa. To na ich podstawie rząd określa kierunki działania służb. W tym kontekście jest konieczna umiejętność priorytetyzacji zagrożeń przez decydentów;
2) **pozyskiwanie informacji przez służby zgodnie z potrzebami władz**;
3) **analizowanie zgromadzonych danych**[15];
4) **przekazywanie odbiorcom** (zgodnie z właściwością rzeczową) **gotowych produktów analitycznych**. Tomasz Aleksandrowicz zauważa, że ten etap – w przypadku braku reakcji władz na otrzymany dokument – zamyka cykl wywiadowczy, a jeżeli pojawia się kolejne zlecenie, to mamy do czynienia z tzw. otwartym cyklem wywiadowczym[16].

[13] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP*…

[14] http://sjp.pwn.pl/sjp/;3067966 [dostęp: 13 V 2017].

[15] Problem pozyskiwania informacji oraz ich przetwarzania zostanie przedstawiony w dalszej części opracowania.

[16] T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie*, Warszawa 1999, s. 55–56.



Rysunek. Cykl wywiadowczy.

Źródło: Opracowanie własne.
Wykorzystane materiały: K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, s. 82–87.

Warto przedstawić kilka przykładów naruszeń cyklu wywiadowczego. Eksperci wyróżniają błędy popełniane zarówno przez decydentów, jak i analityków. Odbiorcy finalnych produktów mogą:

- w sposób nieprecyzyjny formułować swoje potrzeby, co może wynikać z braku umiejętności wykorzystania posiadanych sił i środków, w tym służb specjalnych;
- nie wykorzystywać wiedzy i konkluzji przekazywanych w dokumentach[17]. W tym kontekście warto wskazać na problem opisany w psychologii społecznej przez Irvinga Janisa, tj. syndrom grupowego myślenia (ang. *groupthink syndrome*, GTS). Definiuje się go jako (…) *nieracjonalny wzorzec myślenia i zachowania w grupie, który narzuca sztuczny konsensus i tłumi głosy sprzeciwu*[18]. To oznacza, że osoby podejmujące decyzje (czy to politycy, czy dowódcy wojskowi) jako członkowie większej grupy mogą jej ulec i – w obawie przed wykluczeniem – dobrowolnie ograniczyć swoje zdolności intelektualne do właściwej oceny sytuacji. Wśród przykładów GTS – wymienionych przez Janisa w artykule zatytułowanym *Groupthink*, opublikowanym w 1971 r. – znajdują się błędne decyzje podjęte przez Amerykanów, w tym brak właściwego przygotowania się na atak Japończyków na Pearl Harbor, przegrana

[17] J. Konieczny, *Analiza informacji w dziedzinie*…, s. 248.

[18] K. Albrecht, *Inteligencja praktyczna. Sztuka i nauka zdrowego rozsądku*, Gliwice 2009, s. 217.

podczas inwazji w Zatoce Świń oraz decyzja o zwiększeniu zaangażowania USA w wojnę w Wietnamie[19].

Błędy mogą powstać także na etapie opracowywania materiału analitycznego dla finalnego odbiorcy. Wśród najczęstszych należy wymienić[20]:

- przekonanie o wystarczającej ilości materiałów potrzebnych do sporządzania produktu analitycznego dla odbiorcy zewnętrznego oraz brak chęci do wykorzystania informacji, które wpływają na ocenę zagrożeń (np. tego rodzaju zachowanie może wynikać z tzw. lenistwa analityka, który ma już przygotowany i zatwierdzony projekt opracowania, a nowe dane diametralnie zmieniają przyjęte założenia, co wiąże się z koniecznością dalszej pracy nad tym samym dokumentem);
- brak odpowiedniej weryfikacji informacji dostarczanych przez źródło. Nieprawdziwe wiadomości mogą zniekształcać obraz rzeczywistości, co może doprowadzić do podjęcia przez polityków błędnych decyzji;
- tworzenie opracowań w sposób zgodny z oczekiwaniami adresatów materiałów czy przełożonych (np. osoby odpowiedzialne za przetwarzanie danych w obawie o karierę mogą umieszczać w analizach tezy i oceny zgodne ze sposobem postrzegania świata przez kierownictwo danej instytucji);
- spóźnione przekazywanie materiałów (brak informacji w odpowiednim czasie uniemożliwia podjęcie właściwej decyzji).

Sposoby pozyskiwania informacji

Analizę informacji poprzedza proces ich zdobywania. W literaturze przedmiotu wymienia się wiele sposobów gromadzenia wiedzy dotyczącej bezpieczeństwa państwa. Obecnie można wskazać co najmniej kilka takich sposobów. Wśród najpopularniejszych należy wymienić:

- **OSINT** (ang. *Open Source Intelligence*), zwany także białym wywiadem – pozyskiwanie informacji ze źródeł otwartych, tj. mediów tradycyjnych i elektronicznych, portali społecznościowych (np. Facebooka), oficjalnych rejestrów państwowych, dokumentów administracji publicznej udostępnianych obywatelom, wykładów, konferencji naukowych oraz materiałów, do których dostęp nie wymaga specjalnych upoważnień czy umiejętności. W ostatnich latach OSINT – w związku z postępującym zjawiskiem cyfryzacji, coraz szerszym dostępem ludzi do internetu oraz ich otwartością na dzielenie się szerokim spektrum informacji z życia prywatnego za pośrednictwem portali społecznościowych – staje się nieocenionym źródłem wiedzy;

[19] I. Janis, *Groupthink*, „Psychology Today" 1971, nr 6, s. 43–46, 74–76.

[20] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji*…, s. 112–115.

- **HUMINT** (ang. *Human Intelligence*), czyli zdobywanie wiedzy od tzw. osobowych źródeł informacji. Przez HUMINT należy rozumieć klasyczne działania wywiadowcze. Najczęściej instytucje państwowe (np. służby specjalne) uprawnione do prowadzenia działań operacyjno-rozpoznawczych starają się pozyskiwać materiały od osób posiadających informacje mogące mieć istotne znaczenie dla bezpieczeństwa zewnętrznego i wewnętrznego państwa, porządku konstytucyjnego, a także pozycji kraju na arenie międzynarodowej oraz jego potencjału militarnego i gospodarczego. W celu nawiązywania kontaktów oraz późniejszego werbunku funkcjonariusze służb korzystają z szerokiego spektrum narzędzi. W literaturze przedmiotu wskazuje się na różne motywacje osób, które godzą się na współpracę z organami bezpieczeństwa. Najpopularniejsza teoria zamyka się w angielskim skrócie **MICE** (tj. *money, ideology, coercion, ego*). Zgodnie z jej założeniami ludzie przekazują służbom informacje ze względu na m.in.: pieniądze otrzymywane w zamian, wyznawane poglądy, strach przed kompromitacją, zaspokojenie własnych ambicji;
- **SIGINT** (ang. *Signals Intelligence*)[21], na który składa się m.in. **COMINT** (ang. *Communication Intelligence* – informacje komunikacyjne, w tym pochodzące z rozmów telefonicznych, konwersacji przeprowadzanych za pomocą radiostacji oraz innych środków), **ELINT** (ang. *Electronic Intelligence* – dane pochodzące z rozpoznania sygnałów elektromagnetycznych nieużywanych w telekomunikacji) oraz **TELINT** (ang. *Telemetry Intelligence* – techniczne i wywiadowcze informacje pochodzące ze zgromadzonych i przetworzonych sygnałów świetlnych czy obcej telemetrii). Reasumując, SIGINT polega na pozyskiwaniu informacji za pomocą radarów, podsłuchów telefonicznych, mikrofonów kierunkowych oraz – być może przede wszystkim – kontroli przepływu danych w internecie. Obecnie, gdy weźmie się pod uwagę niską świadomość wielu użytkowników w zakresie zapewnienia bezpieczeństwa działań prowadzonych w cyberprzestrzeni, materiały pochodzące z tego typu źródeł stają się niezwykle cenne nie tylko dla hakerów czy grup przestępczych, lecz także dla służb państwowych, które w sposób niejawny i zgodnie z obowiązującym prawem powinny zdobywać interesującą je wiedzę. Jednocześnie ze względu na dużą liczbę informacji przesyłanych w sieciach teleinformatycznych, ich pozyskiwanie oraz analiza wymagają specjalistycznych umiejętności oraz programów komputerowych, które wspierają proces przetwarzania zgromadzonych materiałów;
- **IMINT** (ang. *Imagery Intelligence*) nazywany w literaturze także **PHOTINT** (ang. *Photo Intelligence*)[22] **–** pozyskiwanie wiedzy m.in. ze zdjęć wykonanych przez satelity wyposażone w wysokiej klasy aparaty fotograficzne lub przez

[21] Tłumaczenie własne za: *Global National Security and Intelligence Agencies Handbook*, Washington 2015, s. 279.

[22] Tamże.

funkcjonariuszy dzięki prowadzeniu obserwacji osób czy zainstalowaniu środków technicznych. Informacje zdobyte w ten sposób pozwalają wskazać czy też potwierdzić niepożądane zmiany w środowisku bezpieczeństwa (np. ruchy wojsk przeciwnika, budowanie nowych obiektów o przeznaczeniu militarnym);

- **MASINT** (ang. *Measurements and Signatures Intelligence*) – informacje wywiadowcze o charakterze naukowym i technicznym, otrzymywane przez jakościową i ilościową analizę danych (metryczną, kątową, przestrzenną, długości fal, zależności czasowych, modulacji, hydromagnetyczną), pochodzące z wyspecjalizowanych sensorów technicznych[23].

Typy analiz i techniki analityczne

Kolejnym etapem cyklu wywiadowczego jest analiza wiedzy zgromadzonej zgodnie z zapotrzebowaniem polityków pełniących funkcje kierownicze w państwie. Można wskazać co najmniej dwa główne **typy analiz** stanowiących wsparcie w procesie decyzyjnym. Są nimi:

- **analiza strategiczna** – rozumiana jako kompleksowa diagnoza wydarzeń z przeszłości i teraźniejszości, która umożliwia przygotowanie prognozy dotyczącej szeroko pojmowanych zagrożeń bezpieczeństwa oraz wniosków i rekomendacji. Ułatwiają one odbiorcom takiego materiału podjęcie decyzji przynoszących skutki długofalowe;
- **analiza sygnalna** – przygotowywana na podstawie bieżącej pracy służb. Zazwyczaj przybiera formę tzw. kostki informacyjnej jedno- lub dwuakapitowej. W materiale zawierającym tylko jeden akapit (formą przypomina depeszę prasową) znajdują się odpowiedzi na najbardziej podstawowe pytania (kto? co? gdzie? kiedy?). W przypadku analiz dwuakapitowych wskazuje się dodatkowo krótkie wnioski i ewentualne rekomendacje.

Osobnym zagadnieniem są **techniki analityczne** wykorzystywane w toku opracowywania dokumentów istotnych dla bezpieczeństwa państwa. Wśród ciekawszych można wskazać:

- **analizy zdarzeń o wysokim wpływie i niskim prawdopodobieństwie** (ang. *high impact*, *low probability events*). Ich autorzy opisują zdarzenia, które mogą implikować poważne konsekwencje dla bezpieczeństwa państwa, ale prawdopodobieństwo ich wystąpienia jest niewielkie. Ważnymi elementami takiego opracowania są: diagnoza, w jaki sposób może dojść do niepożądanej sytuacji, oraz wskaźniki (tzw. czerwone flagi) ostrzegające przed zbliżającym się niebezpieczeństwem;

[23] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji*…, s. 59.

- **analizy typu scenariusze możliwych zdarzeń**. Na podstawie zgromadzonych informacji, własnego doświadczenia oraz wiedzy o typowości przypadków analitycy przygotowują prognozę wydarzeń w perspektywie krótko-, średnio- i długookresowej. Zazwyczaj taka analiza składa się z trzech możliwych wariantów (scenariuszy): optymistycznego (najkorzystniejszego dla państwa), pesymistycznego (negatywnego) oraz najbardziej prawdopodobnego;
- **analizy typu „czerwony kapelusz"**. Ich celem jest odtworzenie sposobu myślenia przeciwnika (osób, organizacji terrorystycznych) oraz przewidywanie – z uwzględnieniem wszystkich zmiennych – jego możliwych zachowań w przyszłości (w tym potencjalnych decyzji np. godzących w bezpieczeństwo państwa).

Pozyskiwanie i przetwarzanie informacji przez wybrane instytucje państwowe

W polskim systemie bezpieczeństwa funkcjonuje wiele instytucji państwowych, które przygotowują decydentom produkty analityczne. Zakres informacji potrzebnych do przygotowania analiz, które są pozyskiwane i przetwarzane przez poszczególne podmioty, jest różny i wynika z ich ustawowych kompetencji. Inne dane gromadzą cywilne służby specjalne, inne wojskowe, a jeszcze inne służby o charakterze policyjnym.

Polski kontrwywiad i wywiad – działając na podstawie i w granicach prawa – odpowiadają odpowiednio za (…) *uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego*[24] (Agencja Bezpieczeństwa Wewnętrznego) oraz za (…) *uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej oraz jej potencjału ekonomicznego i obronnego*[25] (Agencja Wywiadu). Szefowie ABW i AW są jednocześnie zobligowani do niezwłocznego przekazywania prezydentowi Rzeczpospolitej Polskiej i Prezesowi Rady Ministrów informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczpospolitej Polskiej. Ponadto, jeżeli Prezes Rady Ministrów nie zdecyduje inaczej, szefowie ABW i AW przekazują te informacje także ministrom konstytucyjnym, zgodnie z ich właściwością rzeczową[26].

Na etapie gromadzenia informacji funkcjonariusze korzystają z uprawnień określonych w rozdziale 4. *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*. Wśród nich należy wymienić m.in.:

- kontrolę operacyjną (obejmującą m.in. uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą

[24] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: DzU z 2020 r. poz. 27), art. 5.

[25] Tamże, art. 6.

[26] Tamże, art. 18.

sieci telekomunikacyjnych, oraz obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne)[27];
- tajną współpracę z osobami niebędącymi funkcjonariuszami[28];
- pomoc organów administracji państwowej, które są zobowiązane do przekazywania do ABW i AW informacji istotnych dla bezpieczeństwa zewnętrznego i międzynarodowej pozycji Rzeczpospolitej Polskiej[29].

Przetwarzanie zgromadzonych informacji odbywa się w wyspecjalizowanych jednostkach organizacyjnych poszczególnych służb. Na podstawie otwartych źródeł informacji nie ma możliwości ustalenia szczegółowego zakresu ich kompetencji, gdyż te zagadnienia są regulowane przepisami o ochronie informacji niejawnych. O rosnącym znaczeniu analizy informacji w ABW świadczy jednak zmiana struktury organizacyjnej tej formacji. W listopadzie 2018 r. weszło w życie *Zarządzenie nr 163 Prezesa Rady Ministrów z 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego*[30]. Zgodnie z jego postanowieniami wyodrębniono – jak można przypuszczać z Biura Ewidencji i Analiz (zwanego także Biurem E) – nowy Departament Informacji, Analiz i Prognoz (Departament VIII). Obecnie to jego funkcjonariusze zapewne odpowiadają za przygotowywanie produktów analitycznych w ABW[31]. Ponadto można wnioskować – na podstawie wywiadu przeprowadzonego przez Krzysztofa Liedela z gen. Adamem Rapackim – że analizę dotyczącą zagrożeń terrorystycznych może prowadzić w pewnym zakresie Centrum Antyterrorystyczne, które zostało powołane do życia na mocy *Zarządzenia nr 102 Prezesa Rady Ministrów z dnia 17 września 2008 r. zmieniającego zarządzenie w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (akt uchylony – przyp. red.). Adam Rapacki wskazywał, że (…) *poza przetwarzaniem informacji o charakterze operacyjnym w Centrum będą opracowywane analizy dotyczące poszczególnych zagadnień po to, aby wiedza dystrybuowana z Centrum była jednolita dla wszystkich podmiotów*[32].

W przypadku AW nawet takie rozważania były do niedawna niemożliwe, gdyż statut tej instytucji nie ujawniał, która jednostka organizacyjna odpowiada za analizę informacji (prawie wszystkie nosiły nazwę „Biuro")[33]. Zmiana w tej materii również nastąpiła w 2018 r. Zgodnie z *Zarządzeniem nr 106 Prezesa Rady Ministrów z dnia*

[27] Tamże, art. 27.

[28] Tamże, art. 36.

[29] Tamże, art. 41.

[30] M.P. z 2018 r. poz. 927.

[31] Tamże, § 3.

[32] K. Liedel, *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa,* Warszawa 2010, s. 132.

[33] *Obwieszczenie Prezesa Rady Ministrów z dnia 14 września 2016 r. w sprawie ogłoszenia jednolitego tekstu zarządzenia Prezesa Rady Ministrów w sprawie nadania statutu Agencji Wywiadu* (M.P. z 2016 r. poz. 936), § 3.

3 lipca 2018 r. zmieniającym zarządzenie w sprawie nadania statutu Agencji Wywiadu[34] utworzono nową jednostkę – Departament Informacyjny, który – tak jak w przypadku ABW – zapewne przygotowuje opracowania analityczne dla władz RP[35].

Inny zakres informacji pozyskują i przetwarzają wojskowe służby specjalne. Służba Kontrwywiadu Wojskowego (SKW) jest zobowiązana do (…) *uzyskiwania, gromadzenia, analizowania, przetwarzania i przekazywania właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej Sił Zbrojnych RP czy pozostałych jednostek organizacyjnych MON*[36]. Z kolei Służba Wywiadu Wojskowego (SWW) uzyskuje, gromadzi, analizuje, przetwarza i przekazuje właściwym organom informacje, które mogą mieć istotne znaczenie dla potencjału obronnego Rzeczpospolitej Polskiej, bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP oraz warunków realizacji przez nie zadań poza granicami państwa. Ta służba rozpoznaje również i analizuje zagrożenia, które mogą wpływać na obronność państwa, występujące m.in. w rejonach konfliktów[37]. Zgromadzone i przetworzone informacje szefowie SKW i SWW przekazują niezwłocznie – po powiadomieniu ministra obrony narodowej – prezydentowi RP i Prezesowi Rady Ministrów. Ponadto, jeżeli te informacje dotyczą spraw objętych zakresem działania właściwego ministra, przekazują je również temu ministrowi, chyba że Prezes Rady Ministrów zadecyduje inaczej[38].

Na etapie gromadzenia informacji funkcjonariusze SKW i SWW korzystają z uprawnień określonych w rozdziale 3. *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*. Są one w wielu przypadkach zbieżne z uprawnieniami przewidzianymi dla ABW i AW (m.in. kontrola operacyjna czy tajna współpraca z osobami niebędącymi funkcjonariuszami). Jednocześnie trudno określić, które jednostki organizacyjne w SWW i SKW odpowiadają za analizę informacji, gdyż ich struktura pozostaje niejawna (prawodawca posługuje się określeniami: departament, zarząd, biuro[39]).

Centralne Biuro Antykorupcyjne, utworzone w 2006 r. na podstawie *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*[40] (…) *jako służba specjalna do spraw zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania*

[34] M.P. z 2018 r. poz. 660.

[35] Tamże, § 1.

[36] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (t.j.: DzU z 2019 r. poz. 687).

[37] Tamże, art. 6.

[38] Tamże, art. 19.

[39] *Zarządzenie Ministra Obrony Narodowej z dnia 21 kwietnia 2017 r. w sprawie nadania statutu Służbie Kontrwywiadu Wojskowego* (M.P. z 2017 r. poz. 431) oraz *Zarządzenie Ministra Obrony Narodowej z dnia 13 czerwca 2018 r. zmieniające zarządzenie w sprawie nadania statutu Służbie Wywiadu Wojskowego* (M.P. z 2018 r. poz. 694).

[40] Tekst jednolity: DzU z 2019 r. poz. 1921, ze zm.

działalności godzącej w interesy ekonomiczne państwa[41], zostało zobligowane (…) *do prowadzenia działalności analitycznej dotyczącej zjawisk występujących w obszarze właściwości CBA oraz przedstawiania w tym zakresie informacji Prezesowi Rady Ministrów, Prezydentowi Rzeczypospolitej Polskiej, Sejmowi oraz Senatowi*[42].

Na etapie gromadzenia informacji funkcjonariusze CBA korzystają z uprawnień określonych w rozdziale 3. ustawy o CBA. Również w przypadku CBA są one często zbieżne z uprawnieniami przewidzianymi dla ABW, AW, SKW oraz SWW (m.in. kontrola operacyjna, tajna współpraca z osobami, które nie są funkcjonariuszami). Za przetwarzanie i analizowanie informacji zgromadzonych w wyniku czynności operacyjno-rozpoznawczych odpowiada prawdopodobnie Departament Analiz[43].

Podczas realizacji swoich zadań ustawowych informacje o charakterze wywiadowczym pozyskują także Policja i Straż Graniczna (SG), które podlegają ministrowi spraw wewnętrznych i administracji. Charakter tych informacji determinuje katalog zadań wskazanych tym służbom przez ustawodawcę. Z tego względu Policja przetwarza dane związane z (…) *ochroną bezpieczeństwa i porządku publicznego, w tym zapewnieniem spokoju w miejscach publicznych oraz w środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania*[44]. Z kolei Straż Graniczna (…) *gromadzi i przetwarza informacje z zakresu ochrony granicy państwowej, kontroli ruchu granicznego, zapobiegania i przeciwdziałania nielegalnej migracji*[45]. Proces analizy informacji oraz ich przekazywania decydentom następuje w jednostkach organizacyjnych poszczególnych służb funkcjonujących w ramach odpowiednio Komendy Głównej Policji (KGP) oraz Komendy Głównej Straży Granicznej (KG SG). W KGP istnieje m.in.:

- Gabinet Komendanta Głównego Policji, do którego zadań należy (…) *koordynowanie przygotowywania materiałów na posiedzenia komisji i podkomisji parlamentarnych oraz udziału w ich pracach Komendanta Głównego Policji i jego zastępców, przygotowywanie analiz dotyczących funkcjonowania Policji na doraźne potrzeby kierownictwa KGP*[46];
- Główny Sztab Policji, którego zadaniem jest (…) *zarządzanie bieżącymi informacjami o stanie bezpieczeństwa i porządku* (…)*, w tym gromadzenie i analizowanie informacji o bieżących zdarzeniach i zagrożeniach na terenie kraju oraz podejmowanie działań służących ich zapobieganiu i eliminowaniu*[47].

---

[41] Tamże, art. 1.

[42] Tamże, art. 2.

[43] *Zarządzenie Nr 72 Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu* (M.P. z 2010 r. nr 76 poz. 953), § 3.

[44] *Ustawa z dnia 6 kwietnia 1990 r. o Policji* (t.j.: DzU z 2020 r. poz. 360), art. 1.

[45] *Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (t.j.: DzU z 2020 r. poz. 305), art. 1.

[46] http://www.policja.pl/pol/kgp/gabinet-komendanta-glo/ [dostęp: 3 IX 2019].

[47] http://www.policja.pl/pol/kgp/glowny-sztab-policji [dostęp: 3 IX 2019].

Z kolei w strukturze KG SG funkcjonuje:

- Zarząd do spraw Cudzoziemców, do którego zadań należy (…) *przygotowywanie cyklicznych i okresowych analiz i opracowań, w szczególności w zakresie powrotów cudzoziemców z terytorium RP*[48];
- Biuro Analityczno-Informacyjne, które odpowiada m.in. za (…) *zapewnienie Komendantowi Głównemu Straży Granicznej i jego zastępcom wsparcia w procesie decyzyjnym, w szczególności poprzez opracowanie i dostarczanie informacji i analiz oraz dokumentów o charakterze strategicznym dla działalności Straży Granicznej*[49].

Wymienienie zakresu kompetencji tylko kilku instytucji pokazuje, jak wiele podmiotów zajmuje się analizą informacji. Materiały zdobywane przez te podmioty oraz ich obszary zainteresowania – pomimo różnych zadań – często się pokrywają. Z tego względu prawodawca podjął w 2007 r. próbę usprawnienia systemu bezpieczeństwa państwa w zakresie przepływu danych pomiędzy jego poszczególnymi komponentami. *Ustawą z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[50] powołał do życia Rządowe Centrum Bezpieczeństwa (RCB) – podmiot, który koordynuje obieg informacji oraz pełni funkcję Krajowego Centrum Zarządzania Kryzysowego. Do podstawowych zadań RCB należą: (...) *analiza i ocena możliwości wystąpienia zagrożeń lub ich rozwoju, gromadzenie informacji o zagrożeniach i analiza zebranych materiałów, wypracowywanie wniosków i propozycji zapobiegania i przeciwdziałania zagrożeniom*[51]. O roli i znaczeniu informacji w działalności RCB świadczy wyodrębnienie w strukturze organizacyjnej tej instytucji osobnej komórki, tj. Biura Analiz i Reagowania, które składa się m.in. z Centrum Operacyjno-Analitycznego. Jego zadania to: (...) *monitorowanie i analizowanie sytuacji w obszarze stanu bezpieczeństwa narodowego oraz występujących w tym zakresie zagrożeń; sporządzanie sprawozdań, raportów i ocen: – z działań prowadzonych w sytuacjach kryzysowych przez Centrum – w zakresie powierzonym przez Radę Ministrów lub Prezesa Rady Ministrów, z działań prowadzonych w sytuacjach kryzysowych przez organy administracji publicznej właściwe w sprawach zarządzania kryzysowego*[52].

[48] http://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/zarzad-do-spraw-cudzozi/1909,Zarzad-do-Spraw-Cudzoziemcow-Komendy-Glownej-Strazy-Granicznej.html [dostęp: 3 IX 2019].

[49] https://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/biuro-analityczno-sytua/7895,Biuro-Analityczno-Sytuacyjne.html [dostęp: 9 XII 2019].

[50] Tekst jednolity: DzU z 2019 r. poz. 1398, ze zm.

[51] Tamże, art. 11.

[52] http://rcb.gov.pl/centrum-operacyjno-analityczne-2/ [dostęp: 3 IX 2019].

Wnioski

Autor opracowania jest świadomy, że nie wyczerpał tematu. Jego zamiarem było jedynie zasygnalizowanie kilku ciekawych aspektów pracy analitycznej oraz aktualnych rozwiązań systemowych w obszarze tworzenia dla władz RP produktów analitycznych, które wspomagają proces decyzyjny w sferze bezpieczeństwa państwa. Na tej podstawie można jednak, reasumując dotychczasowe rozważania oraz mając na uwadze, że pełne przedstawienie problemu wymagałoby przygotowania wielostronicowego opracowania, wyciągnąć pewne wnioski:

1. W związku z dużą liczbą informacji pojawiających się każdego dnia (potencjalnie istotnych dla życia, zdrowia i mienia polskich obywateli, porządku konstytucyjnego czy pozycji międzynarodowej RP) rola i znaczenie analizy danych będą rosły. Z tego względu na rynku pracy będą poszukiwani fachowcy, którzy potrafią priorytetyzować zagrożenia oraz opisywać niepożądane zjawiska w sposób syntetyczny.
2. Odrębnym wyzwaniem, wynikającym z coraz większej liczby danych, pozostaje tworzenie nowych narzędzi i bieżące usprawnianie już istniejących, w tym programów komputerowych, które pomagają analitykom sprawnie przetwarzać i porządkować zgromadzoną wiedzę.
3. W Polsce za przygotowywanie analiz na temat potencjalnych zagrożeń bezpieczeństwa państwa odpowiada wiele podmiotów. Często mają one podobne kompetencje, dlatego może dochodzić do niepotrzebnego dublowania się wysiłków w sferze rozpoznawania, gromadzenia i przetwarzania informacji. Z tego względu istotna wydaje się stała intensyfikacja współpracy pomiędzy nimi, w tym również polegającej na wymianie wiedzy, w celu osiągnięcia efektu synergii.
4. Warto rozpocząć dyskusję na temat zreformowania systemu bezpieczeństwa, w tym utworzenia jednego, centralnego podmiotu lub przekształcenia już istniejącego (np. Rządowego Centrum Bezpieczeństwa), który zajmowałby się analizowaniem informacji uzyskanych od służb specjalnych oraz urzędów. Następnie jego zadaniem byłoby przygotowanie każdego dnia jednego kompleksowego materiału, którego odbiorcami byłyby najważniejsze osoby w państwie. Ten wniosek wydaje się słuszny, jeśli weźmie się pod uwagę postulaty zgłaszane również przez byłego szefa Służby Wywiadu Wojskowego Andrzeja Kowalskiego (w 2013 r. wskazywał on na konieczność utworzenia przy koordynatorze służb specjalnych Centrum Analiz Strategicznych[53]), autorów *Białej Księgi Bezpieczeństwa Narodowego*[54] czy innych ekspertów

[53] *Plan zmian w służbach opracowywany od kilku lat*, http://niezalezna.pl/73124-plan-zmian-w-sluzbach-opracowywany-od-kilku-lat-znamy-szczegoly-wideo [dostęp: 13 V 2017].

[54] Twórcy tego dokumentu sygnalizowali konieczność budowy „(…) komórki (biura, centrum, departamentu itp.) odpowiedzialnej za dokonywanie strategicznych syntez informacji dostarczanych

zajmujących się problematyką bezpieczeństwa (np. z Fundacji im. Kazimierza Pułaskiego[55]).

Bibliografia

Albrecht K., *Inteligencja praktyczna. Sztuka i nauka zdrowego rozsądku*, Gliwice 2009, Helion.

Aleksandrowicz T.R., *Analiza informacji w administracji i biznesie*, Warszawa 1999, Wyższa Szkoła Handlu i Prawa.

Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej, Warszawa 2013, Biuro Bezpieczeństwa Narodowego.

Drabik L., Sobol E., *Słownik języka polskiego*, Warszawa 2005, Wydawnictwo Naukowe PWN.

Global National Security and Intelligence Agencies Handbook, Washington 2015, International Business Publications.

Janczak J., Nowak A., *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, AON.

Janis I., *Groupthink*, „Psychology Today" 1971, nr 6.

Konieczny J., *Analiza informacji w dziedzinie bezpieczeństwa państwa*, Warszawa 2014, ABW.

Korzeniowski L.F., *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, Difin.

Liderman K., *Bezpieczeństwo informacyjne*, Warszawa 2012, Wydawnictwo Naukowe PWN.

Liedel K., *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, Wydawnictwo Adam Marszałek.

Liedel K., *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa*, Warszawa 2010, Difin.

Liedel K., Piasecka P., Aleksandrowicz T.R., *Analiza informacji. Teoria i praktyka*, Warszawa 2012, Difin.

Obwieszczenie Prezesa Rady Ministrów z dnia 14 września 2016 r. w sprawie ogłoszenia jednolitego tekstu zarządzenia Prezesa Rady Ministrów w sprawie nadania statutu Agencji Wywiadu (M.P. z 2016 r. poz. 936).

przez służby specjalne i wypracowywanie zintegrowanych ocen na potrzeby kierowania bezpieczeństwem narodowym. Jej zadaniem byłoby zbieranie informacji od wszystkich służb państwa odpowiedzialnych za poszczególne sfery bezpieczeństwa, a następnie dokonywanie ich analizy i oceny na potrzeby najwyższych organów kierowania państwem". Zob. *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, s. 210.

[55] G. Małecki, *Reforma służb specjalnych z perspektywy 15 lat*, https://pulaski.pl/wp-content/uploads/2015/02/Raport_reforma_sluzb__FKP.pdf [dostęp: 13 V 2017].

Potejko P., *Bezpieczeństwo informacyjne*, w: *Bezpieczeństwo państwa*, K.A. Wojtaszczyk, A. Materska-Sosnowska (red.), Warszawa 2009, Oficyna Wydawnicza ASPRA.

Sienkiewicz P., *10 wykładów*, Warszawa 2005, AON.

Akty prawne

Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (t.j.: DzU z 2019 r. poz. 1398, ze zm.).

Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym (t.j.: DzU z 2019 r. poz. 1921, ze zm.).

Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego (t.j.: DzU z 2019 r. poz. 687).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j.: DzU z 2020 r. poz. 27).

Ustawa z dnia 12 października 1990 r. o Straży Granicznej (t.j.: DzU z 2020 r. poz. 305).

Ustawa z dnia 6 kwietnia 1990 r. o Policji (t.j.: DzU z 2020 r. poz. 360).

Zarządzenie nr 163 Prezesa Rady Ministrów z dnia 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (M.P. z 2018 r. poz. 927).

Zarządzenie nr 106 Prezesa Rady Ministrów z dnia 3 lipca 2018 r. zmieniające zarządzenie w sprawie nadania statutu Agencji Wywiadu (M.P. z 2018 r. poz. 660).

Zarządzenie Ministra Obrony Narodowej z dnia 13 czerwca 2018 r. zmieniające zarządzenie w sprawie nadania statutu Służbie Wywiadu Wojskowego (M.P. z 2018 r. poz. 694).

Zarządzenie Ministra Obrony Narodowej z dnia 21 kwietnia 2017 r. w sprawie nadania statutu Służbie Kontrwywiadu Wojskowego (M.P. z 2017 r. poz. 431).

Zarządzenie Nr 72 Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie nadania statutu Centralnemu Biuru Antykorupcyjnemu (M.P. z 2010 nr 76 poz. 953).

Źródła internetowe

http://niezalezna.pl/73124-plan-zmian-w-sluzbach-opracowywany-od-kilku-lat-znamy-szczegoly-wideo [dostęp: 3 IX 2019].

http:// https://rcb.gov.pl/centrum-operacyjno-analityczne-2/ [dostęp: 3 IX 2019].

http://sjp.pwn.pl/sjp/;3067966 [dostęp: 3 IX 2019].

http://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/zarzad-do-spraw-cudzozi/1909,Zarzad-do-Spraw-Cudzoziemcow-Komendy-Glownej-Strazy-Granicznej.html [dostęp: 3 IX 2019].

http://www.policja.pl/pol/kgp/gabinet-komendanta-glo/ [dostęp: 3 IX 2019].

http://www.policja.pl/pol/kgp/glowny-sztab-policji [dostęp: 3 IX 2019].

https://bits.blogs.nytimes.com/2009/12/09/the-american-diet-34-gigabytes-a-day/?_r=0 [dostęp: 3 IX 2019].

https://pulaski.pl/wp-content/uploads/2015/02/Raport_reforma_sluzb__FKP.pdf [dostęp: 3 IX 2019].

https://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/biuro-analityczno-sytua/7895,Biuro-Analityczno-Sytuacyjne.html [dostęp: 9 XII 2019].

https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [dostęp: 3 IX 2019].

Abstrakt

W tekście przedstawiono zagadnienia dotyczące analizy informacji i jej rolę w zapewnianiu bezpieczeństwa państwa. W pierwszej części zwrócono uwagę na teoretyczne aspekty przetwarzania wiadomości istotnych z punktu widzenia decydentów, w tym kwestie definicyjne, sposoby pozyskiwania informacji oraz rodzaje analizy danych. W głównej części tekstu wskazano na wiele podmiotów odpowiedzialnych za dostarczanie analiz politykom pełniącym funkcje kierownicze w państwie. We wnioskach postulowano zintensyfikowanie współpracy w zakresie przepływu informacji między poszczególnymi komponentami systemu bezpieczeństwa państwa oraz powołanie nowej instytucji odpowiedzialnej za koordynację i opracowywanie zbiorczych produktów analitycznych m.in. dla prezydenta RP i Prezesa Rady Ministrów.

Słowa kluczowe: analiza, informacja, bezpieczeństwo narodowe, służby specjalne, proces decyzyjny.

Abstract

The article presents the issue of data analysis in the process of providing national security. In the first part, there were highlighted theoretic aspects, including

definitions of terms data and analysis or means of collecting information. Moreover, there was shown types of analysis and the intelligence cycle. In the second part, the author pointed out legal frames in the field of Polish security institutions which are responsible for preparation of analytical products. In conclusion, the author suggested i.a. intensification of cooperation between those agencies.

Keywords: analysis, data, national security, intelligence services, decision making process.

Kamil Nowak

Wpływ sposobu prowadzenia postępowania przygotowawczego na zwalczanie działalności oszustów w zakresie podatku VAT – wybrane zagadnienia

Okolicznością, która ma istotne znaczenie dla skutecznego zwalczania działalności grup przestępczych trudniących się oszustwami podatkowymi związanymi z podatkiem VAT, jest sposób prowadzenia postępowania przygotowawczego. Ze spostrzeżeń autora artykułu wynika, że w praktyce organów ścigania – przede wszystkim do czasu wydania przez Prokuratora Generalnego 10 sierpnia 2017 r. *Wytycznych w sprawie zasad prowadzenia postępowań przygotowawczych w sprawach o przestępstwa związane z procederem wyłudzania nienależnego zwrotu podatku VAT oraz innych oszukańczych uszczupleń w tym podatku*[1] – były zauważalne, ukształtowane w okresie ostatnich kilkunastu lat, dwa odmienne sposoby prowadzenia postępowania przygotowawczego, które na podstawie ich metodyki można określić jako sposób defensywny i sposób ofensywny.

Defensywny sposób prowadzenia postępowania przygotowawczego

Defensywny (zachowawczy) sposób prowadzenia postępowania dotyczącego oszustw związanych z podatkiem VAT, zauważalny w przypadku części postępowań przygotowawczych, polegał przede wszystkim na stopniowym dokonywaniu – po wszczęciu postępowania przygotowawczego – zabezpieczenia dokumentacji finansowo-księgowej wszystkich podmiotów gospodarczych występujących w postępowaniu, a następnie – przed ewentualnym wydaniem postanowień o przedstawieniu zarzutów – na przeprowadzeniu oględzin całości tej dokumentacji w wersji papierowej oraz oględzin zabezpieczonych elektronicznych nośników informacji.

Należy przy tym zwrócić uwagę, że najczęściej każde takie postępowanie obejmuje swoim zakresem działalność od kilku do kilkudziesięciu (a czasem nawet kilkuset) podmiotów gospodarczych. Zależnie od długości okresu objętego postępowaniem – w najbardziej jaskrawych przypadkach – tylko w jednym podmiocie

[1] https://www.pk.gov.pl/wp-content/uploads/2018/01/c04ff96e25d267beeb4d5341305fcc16.pdf [dostęp: 7 IV 2019].

gospodarczym (najczęściej w przypadku podmiotów z poziomów bufora[2] lub brokera[3], rzadziej słupa[4]), może dojść do zabezpieczenia kilkudziesięciu, a niekiedy nawet kilkuset dowodów rzeczowych, zazwyczaj segregatorów lub plików dokumentacji finansowo-księgowej, z których każdy może zawierać od kilkudziesięciu do nawet kilkuset dokumentów (kart).

Trzeba również mieć świadomość tego, że czasem w praktyce śledczej dochodzi – wbrew intencjom organizatorów oszustw podatkowych – do zabezpieczenia dokumentacji firm słupów I rzędu (poziomu w schemacie oszustwa), czyli tzw. znikających podatników, niejako z wyprzedzeniem działań oszustów, którzy zmierzają do zniszczenia lub ukrycia tej dokumentacji. Reasumując, najczęściej dokumentacja zabezpieczona w ramach jednego postępowania jest zawarta w kilkuset (lub więcej) segregatorach. W przypadku dokonywania oględzin zgromadzonych dokumentów (w dużej mierze faktur VAT), polegających na spisywaniu do protokołów najistotniejszych danych zawartych w tych dokumentach – co łatwo sprawdzić – w sytuacji, gdyby tymi czynnościami miała się zajmować tylko jedna wyznaczona do tego osoba, która nie wykonuje w tym czasie innych czynności procesowych, oględziny najczęściej trwałyby kilka lat.

Osobną kwestią jest konieczność oględzin elektronicznych nośników informacji. Jeśli chodzi o firmy pełniące funkcje buforów lub brokerów w ramach karuzeli podatkowej, w przypadku uzyskania informacji o osobach, np. pracownikach tych firm, którzy mieli utrzymywać kontakt i współpracować z przedstawicielami grup przestępczych kontrolujących firmy słupy, trudno przeprowadzić rzetelne oględziny zabezpieczonego u nich sprzętu, m.in. laptopów, telefonów komórkowych, pendrive'ów, płyt CD, DVD lub dysków twardych z komputerów, bez zapoznania się z całością zawartej na nich dokumentacji w wersji elektronicznej, w tym ze skanami dokumentów, zdjęciami oraz korespondencją e-mailową.

---

[2] Podstawowym zadaniem b u f o r a jest zakup towarów od znikających podatników, słupów kolejnych poziomów lub innych buforów, a następnie ich sprzedaż brokerowi.

[3] B r o k e r – podmiot, czasem określany jako przedsiębiorstwo finansujące, najczęściej duża firma, która *prima facie* nie wzbudza zastrzeżeń organów skarbowych. Zazwyczaj jest głównym beneficjentem karuzeli podatkowej, a jego głównym zadaniem jest dokonywanie wewnątrzwspólnotowej dostawy towarów (WDT) nabytych wcześniej od bufora, opodatkowanej stawką 0% VAT, do tzw. spółki wiodącej, zarejestrowanej w innym państwie członkowskim.

[4] Wbrew poglądom spotykanym czasem w orzecznictwie, nie każdy słup spełnia kryteria bycia znikającym podatnikiem (ang. *missing trader*), którego definicja była zawarta w art. 2 pkt 1 *Rozporządzenia Komisji (WE) nr 1925/2004 z dnia 29 października 2004 r. ustanawiającego szczegółowe zasady wykonywania niektórych przepisów rozporządzenia Rady (WE) nr 1798/2003 w sprawie współpracy administracyjnej w dziedzinie podatku od wartości dodanej* (Dz. Urz. UE L 331 z 5 listopada 2004 r., s. 13), choć – rzecz jasna – zdecydowana większość słupów jest znikającymi podatnikami. Zgodnie z tym przepisem: „(…) »niewywiązujący się podmiot gospodarczy« oznacza podmiot gospodarczy zarejestrowany jako podatnik dla celów VAT, który, z potencjalnym zamiarem oszustwa, nabywa towary lub usługi, bądź symuluje ich nabywanie, nie płacąc podatku VAT, i zbywa je z uwzględnieniem podatku VAT, nie przekazując należnego podatku VAT właściwym władzom państwowym".

W jednym z postępowań prowadzonych przez Agencję Bezpieczeństwa Wewnętrznego zabezpieczono przenośny komputer, którego dysk twardy zawierał – co nie jest przecież niczym nadzwyczajnym – ponad 300 tys. e-maili, około 50 tys. skanów dokumentów i około 200 tys. zdjęć. Przy czym znaczna część zdjęć przedstawiała właśnie dokumentację finansowo-księgową i odręczne zapiski. W przypadku oględzin wymagało to wyjątkowo uważnej analizy. Autor artykułu pozostawia wyobraźni czytelnika odpowiedź na pytanie, jak długo mogą trwać oględziny tylko tego jednego wskazanego powyżej komputera. A co w przypadku, a ma to miejsce praktycznie w każdym postępowaniu dotyczącym oszustw związanych z podatkiem VAT, gdy zostanie zabezpieczonych kilkadziesiąt takich urządzeń i gdy zawierają one dokumenty oraz korespondencję w językach obcych, które nie są w Polsce powszechnie znane (np. w języku greckim, bułgarskim, węgierskim czy arabskim)?

Rzetelne przeprowadzenie oględzin powinno oznaczać przejrzenie każdego dokumentu. Pewnym ułatwieniem może być np. zmniejszenie liczby analizowanych e-maili przez rezygnację z dokładnego zapoznawania się z korespondencją typu spam. Jednak w odniesieniu do reszty dokumentów w wersji elektronicznej nie można z góry dyskwalifikować i pomijać żadnych materiałów, zwłaszcza ze względu na zasadę obiektywizmu zawartą w art. 4 kpk. Zgodnie z nią organy prowadzące postępowanie karne mają obowiązek badania okoliczności przemawiających zarówno na korzyść, jak i na niekorzyść oskarżonego (podejrzanego).

Czynności wskazane powyżej mogą być rzetelnie prowadzone jedynie przez osobę znającą akta sprawy i specyficzną terminologię stosowaną przez oszustów. Praktyka pokazuje, że oszuści podatkowi w rozmowach między sobą – przede wszystkim „ze względów bezpieczeństwa" – unikają lub ograniczają do minimum używanie określeń wskazujących wprost na dokonywanie oszustw podatkowych. Wychwycenie informacji, słów, zwrotów, które mogą wskazywać – najczęściej pośrednio – na świadomy udział tych osób w oszustwie podatkowym wymaga zatem spostrzegawczości, dobrej znajomości akt sprawy, charakteru, w jakim występują poszczególne podmioty uczestniczące w oszustwach, a także *modus operandi* oszustów. Prowadzenie czynności przez osobę niespełniającą tych wymagań jest obarczone ryzykiem pominięcia – nieświadomego niedostrzeżenia – części informacji istotnych z punktu widzenia oceny świadomości uczestniczenia w oszustwie (lub jej braku).

Wartościowym materiałem dowodowym są zestawienia zawierające wykaz wszystkich uczestników karuzeli podatkowej – niekiedy nawet ze wskazaniem cen (w tym na przykład tzw. złamanej ceny[5]), które mają być przyjmowane na określonym etapie oszustwa[6] – zabezpieczane czasem w trakcie przeszukań. Znalezienie takiego

[5] Tak zwana złamana cena zakłada dokonanie przez firmę słupa sprzedaży w cenie niższej od ceny netto, którą uiszczono na poprzednim etapie obrotu, a która jest możliwa do osiągnięcia z uwagi na niezapłacenie przez słupa należnego podatku VAT.

[6] Szerzej na temat mechanizmu oszustw VAT-owskich: A.A. Aronowitz, D.C.G. Laagland, G. Paulides, *Value-Added Tax Fraud in the European Union*, Amsterdam–New York 1996, s. 58 i nast.; *Intra-Community VAT Fraud*, Den Haag, Bonn, Brussel 2009, s. 5 i nast.; D. Pauch, *Transakcja*

dokumentu np. u osoby powiązanej z firmą buforem lub brokerem może być jedną z ważniejszych okoliczności pozwalających na udowodnienie świadomego udziału w oszustwie beneficjentom procederu. W przypadku prowadzenia czynności przez osobę nierozumiejącą, na czym polega karuzela podatkowa, istnieje ryzyko pominięcia tego typu dowodu lub potraktowanie go jako zwykłego, nieistotnego zapisku.

Defensywny sposób prowadzenia postępowania, zakładający oczekiwanie na zakończenie wszystkich wskazanych wyżej czynności przed ewentualnym przedstawieniem zarzutów sprawcom oszustw, zazwyczaj jest obarczony wieloma negatywnymi konsekwencjami, zarówno z punktu widzenia prowadzonego postępowania, jak i interesów Skarbu Państwa. W przypadku postępowań karnych, w których toku przedstawianie sprawcom zarzutów następuje po bardzo długim okresie od momentu wszczęcia postępowania (czasem po kilku latach), na ogół nie ma szansy na dokonanie zabezpieczenia majątkowego[7] w odniesieniu do środków pieniężnych zdeponowanych na rachunkach bankowych należących do firm słupów oraz odzyskanie przynajmniej części środków wyłudzonych przez beneficjentów oszustwa (m.in. przez nienależne uzyskiwanie zwrotów podatku naliczonego) i wykorzystywanych do popełniania kolejnych oszustw.

Najczęściej podjęcie jakiejkolwiek czynności procesowej wobec słupa (będącego znikającym podatnikiem bądź słupem kolejnych poziomów), który bierze jeszcze udział w przestępczej działalności, powoduje natychmiastowe zaprzestanie transakcji na rachunkach bankowych firmy słupa, po uprzednim dokonaniu transferu znajdujących się tam środków – nierzadko sięgających w momencie prowadzonych czynności kwot od kilkuset tysięcy do kilku milionów złotych. Jest to często równoznaczne z zaprzestaniem dalszej działalności przez ten podmiot. Także dane statystyczne przez wiele lat (przede wszystkim do momentu wydania w 2017 r. *Wytycznych*...) wskazywały na poważne trudności związane ze skutecznym dokonywaniem zabezpieczeń majątkowych. Jak wynikało z informacji Ministerstwa Sprawiedliwości i Prokuratury Krajowej, w latach 2011–2012 wartość zabezpieczeń majątkowych zastosowanych przez prokuratorów we wszystkich kategoriach spraw sięgnęła 732 mln zł,

karuzelowa jako forma oszustwa w podatku od wartości dodanej, „Annales Universitatis Mariae Curie-Skłodowska" 2016, nr 1, s. 621–629; K. Pashev, *Cross-border VAT fraud in an enlarged Europe*, w: *European crime-markets at cross-roads: Extended and extending criminal Europe*, P.C. van Duyne i in. (red.), Nijmegen 2008, s. 237–259; M. Keen, S. Smith, *VAT Fraud and Evasion: What Do We Know, and What Can be Done?*, Washington 2007, s. 12 i nast.; L. Wilk, *„Kryminalne" aspekty przestępczości podatkowej*, „Archiwum Kryminologii" 2009, t. 31, s. 209–221; P.C. van Duyne, *Organized crime and business crime-enterprises in the Netherlands*, „Crime, Law and Social Change" 1993, nr 2, s. 103–142; P.C. van Duyne, A.A. Block, *Organized cross-atlantic crime*, „Crime, Law and Social Change" 1995, nr 22, s. 127–147; J. Glumińska-Pawlic, K. Nowak, *Oszustwa w podatku VAT: geneza, istota, przeciwdziałanie*, „Doradztwo Podatkowe – Biuletyn Instytutu Studiów Podatkowych" 2017, nr 10, s. 6–15; K. Nowak, *Wybrane zagadnienia dotyczące działalności tzw. słupów w ramach zorganizowanych grup przestępczych dopuszczających się oszustw podatkowych w związku z obrotem wyrobami stalowymi*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 171–185.

[7] Na podstawie art. 291 kpk i nast.

w 2013 r. – 363,5 mln, w 2014 r. – 600,7 mln zł, a w 2015 r. – 303,5 mln zł[8]. Wskazane kwoty wynosiły więc jedynie od około 1 proc. do 2 proc. wartości luki podatkowej[9] w podatku VAT w powyższym okresie, a tego typu zabezpieczeń dokonywano przecież we wszystkich postępowaniach karnych, nie tylko w tych, które dotyczyły oszustw podatkowych. To jeszcze bardziej uwidaczniało niewielką skuteczność odzyskiwania „owoców przestępstwa" we wskazanym czasie.

W późniejszym okresie skuteczność organów państwowych w zwalczaniu procederu wzrosła, zarówno w odniesieniu do wysokości dokonywanych zabezpieczeń majątkowych, jak i zmniejszania wielkości luki podatkowej. Na przykład w 2018 r. wielkość luki podatkowej wyniosła ok. 25 mld zł, a więc prawie dwukrotnie mniej niż np. w 2015 r.[10], z kolei wysokość dokonanych zabezpieczeń majątkowych w postępowaniach zakończonych aktem oskarżenia, wnioskiem z art. 335 § 1 kpk, wnioskiem o warunkowe umorzenie oraz wnioskiem o rozpoznanie sprawy w postępowaniu przyspieszonym – ok. 1,050 mld zł[11].

Pozbawiony sensu był również taki sposób prowadzenia postępowania, w którym zabezpieczenia rzeczy mogących stanowić dowód w sprawie dokonywano jedynie na podstawie postanowień o żądaniu wydania rzeczy, które doręczano osobom mającym rzeczy podlegające wydaniu. Ta praktyka, choć czasem bywa uzasadniona np. z uwagi na wielkość podmiotu i konieczność przygotowania znacznej ilości dokumentacji rozproszonej w różnych jednostkach organizacyjnych podmiotu, w przypadku jej nadużywania może niweczyć efekt zaskoczenia i powodować, że zabezpieczona zostanie tylko ta dokumentacja, którą chce wydać jej posiadacz i co do której sprawcy mają pewność, że nie zawiera informacji mogących potwierdzać ich świadomy udział w oszustwie.

Prokuratorzy, którzy są zwolennikami defensywnego sposobu prowadzenia postępowania przygotowawczego, zazwyczaj nie zarządzali również zatrzymywania podejrzanych i poprzestawali na wysyłaniu im wezwań do stawiennictwa w celu przedstawienia zarzutów. Z punktu widzenia oszustów podatkowych, w tym słupów, „objęcie ich" postępowaniem prowadzonym we wskazany sposób – niezależnie od ewentualnego przedstawienia im zarzutów – w praktyce nie miało żadnego wpływu na działalność przestępczą, jaką prowadzili. Odpowiadanie z wolnej stopy oraz

---

[8] http://www.podatki.gazetaprawna.pl/artykuly/965872,wiceszef-ms-25-lat-za-wyludzenia-vat-pod-koniec-2016.html; www.https://www.pk.gov.pl/g2/oryginal/2015_04/c3752155bf43c48bf342459d3e96865c.pdf; http:// www.arch.pg.gov.pl/upload_doc/000003715.pdf; http://www.pk.gov.pl/sprawozdania-i-statystyki/sprawozdania-statystyczne-pg-p1k-pg-p1ca-i-pg-1n-za-2015-r.html#.WBeqJi3hCHs [dostęp: 6 III 2018].

[9] Luka podatkowa – różnica pomiędzy podatkiem VAT teoretycznie należnym (teoretyczne dochody budżetu) a VAT faktycznie pobranym (rzeczywiste wpływy).

[10] Szerzej zob. http://www.money.pl/gospodarka/uszczelnianie-podatkow-mf-luka-vat-spadla-do-125-proc-w-2018-roku-6372387258513025a.html [dostęp: 23 IV 2019].

[11] *PK-P1K. Sprawozdanie z działalności powszechnych jednostek organizacyjnych prokuratury w sprawach karnych za rok 2018*, Warszawa 2019, s. 6.

niedokonywanie zabezpieczeń majątkowych sprawiało, że czuli się bezkarni i kontynuowali popełnianie oszustw.

Ofensywny sposób prowadzenia postępowania przygotowawczego

Ofensywny (dynamiczny) sposób prowadzenia postępowania przygotowawczego jest oparty m.in. na przedstawianiu zarzutów popełnienia przestępstwa podejrzanym niezwłocznie, w miarę uzyskiwania informacji pozwalających na przeprowadzenie tej czynności zgodnie z art. 313 § 1 kpk[12]. Inaczej niż w modelu defensywnym, zazwyczaj jeszcze przed zakończeniem oględzin całości zabezpieczonego materiału na bieżąco są gromadzone informacje uzyskane od podejrzanych współpracujących z organami ścigania. Zbiera się dane istotne dla postępowania przygotowawczego, które pozwalają na znacznie szersze, szybsze i bardziej wnikliwe spojrzenie na zabezpieczone materiały i ujawnienie nieznanych wcześniej okoliczności.

W przypadku posiadania danych dostatecznie uzasadniających podejrzenie, że czyn popełniła określona osoba, w ramach tak prowadzonego postępowania zwykle jednocześnie dokonuje się przeszukania miejsca pobytu tej osoby w celu zabezpieczenia dokumentacji związanej z oszustwami podatkowymi oraz zatrzymania tej osoby. Taka sytuacja – zwłaszcza w przypadku, gdy dochodzi do zabezpieczenia materiałów obciążających, które wskazują na świadomy udział w procederze – zapobiega ewentualnej ucieczce i ukrywaniu się wyżej wymienionej osoby, skoro czynności zatrzymania dokonuje się w tym samym czasie co przeszukania. Natomiast w modelu defensywnym prawdopodobnym skutkiem czynności przeszukania, której nie towarzyszy zatrzymanie osoby, może być rozpoczęcie ukrywania się sprawcy przed organami ścigania, niekiedy nawet za granicą. Może to znacznie opóźnić lub nawet uniemożliwić pociągnięcie sprawcy do odpowiedzialności. Niweczy to również możliwość zablokowania rachunków bankowych – w przypadkach, gdy są one jeszcze aktywne – i dokonania zabezpieczenia majątkowego, zwłaszcza w odniesieniu do znikających podatników, których mocodawcy otrzymują sygnał o zainteresowaniu się określonym podmiotem przez organy ścigania.

Ofensywny model prowadzenia postępowania jest także wyraźnym sygnałem kierowanym przez prokuratora w stronę środowiska przestępczego, wskazującym na zdecydowanie w zwalczaniu procederu, w przeciwieństwie do modelu defensywnego. W wariancie ofensywnym – jak już wskazano – w przypadku zaistnienia okoliczności, o których mowa w art. 247 § 1 i 2 kpk[13], zamiast wzywania w celu przedstawienia

[12] Art. 313 § 1 kpk: „Jeżeli dane istniejące w chwili wszczęcia śledztwa lub zebrane w jego toku uzasadniają dostatecznie podejrzenie, że czyn popełniła określona osoba, sporządza się postanowienie o przedstawieniu zarzutów, ogłasza je niezwłocznie podejrzanemu i przesłuchuje się go, chyba że ogłoszenie postanowienia lub przesłuchanie podejrzanego nie jest możliwe z powodu jego ukrywania się lub nieobecności w kraju".

[13] Art. 247 § 1 kpk: „Prokurator może zarządzić zatrzymanie i przymusowe doprowadzenie osoby

zarzutów zarządza się zatrzymanie i przymusowe doprowadzenie osób podejrzanych[14] albo podejrzanych[15], a po dokonanych czynnościach – w zależności od ich wyniku – podejmuje się decyzje w sprawie zastosowania środków zapobiegawczych. Przy czym z góry (jak w modelu defensywnym) nie wyklucza się wystąpienia z wnioskiem do sądu o tymczasowe aresztowanie, które jest przecież często uzasadnione w przypadku działalności sprawców należących do zorganizowanych grup przestępczych zajmujących się oszustwami związanymi z podatkiem VAT. Natomiast w przypadku defensywnego sposobu postępowania prokuratorzy będący jego zwolennikami nie tylko najczęściej odstępowali od zatrzymywania sprawców, lecz także z góry – niezależnie od uzyskiwanych informacji i przebiegu postępowania – wykluczali występowanie do sądu z wnioskami o zastosowanie tymczasowego aresztowania wobec podejrzanych.

Wpływ sposobu prowadzenia postępowania przygotowawczego na postawę podejrzanych

Jak wskazuje praktyka organów ścigania, w przypadku postępowań prowadzonych w sposób ofensywny są znacznie większe szanse na uzyskanie mocnych dowodów dotyczących działalności osób stojących wyżej w przestępczej hierarchii niż osoby będące tzw. słupami, a czasem nawet – dowodów obciążających organizatorów i pomysłodawców tych przestępstw. Wynika to m.in. z tego, że w przeciwieństwie do defensywnego sposobu prowadzenia postępowania, w którego przypadku podejrzany ma pełną świadomość odpowiadania z wolnej stopy niezależnie od treści złożonych przez siebie wyjaśnień lub odmowy ich złożenia, w postępowaniu prowadzonym ofensywnie zdaje on sobie sprawę z możliwych konsekwencji swojego czynu i wagi zgromadzonych dowodów, a także uświadamia sobie możliwość wystąpienia przez prokuratora do sądu o zastosowanie wobec niego tymczasowego aresztowania. Najczęściej więc podejrzany dostrzega, że dzięki współpracy z organami ścigania można wobec niego zastosować np. nadzwyczajne złagodzenie kary, ponadto przeważnie odpowiada on z wolnej stopy. W przypadku osób fizycznych – słupów – zazwyczaj dopiero w trakcie

podejrzanej albo podejrzanego, jeżeli zachodzi uzasadniona obawa, że:
1) nie stawią się na wezwanie w celu przeprowadzenia z ich udziałem czynności, o których mowa w art. 313 § 1 lub art. 314, albo badań lub czynności, o których mowa w art. 74 § 2 lub 3;
2) mogą w inny bezprawny sposób utrudniać postępowanie.

§ 2. Zatrzymanie i przymusowe doprowadzenie, o którym mowa w § 1, może nastąpić także wtedy, gdy zachodzi potrzeba niezwłocznego zastosowania środka zapobiegawczego".

[14] Osoba podejrzana – w polskim postępowaniu karnym osoba, co do której istnieje uzasadnione podejrzenie, że popełniła przestępstwo, ale nie przedstawiono jej jeszcze zarzutów. Zob. K. Marszał, *Proces karny. Zagadnienia ogólne*, Katowice 2013, wyd. 2, s. 250 i nast.

[15] Podejrzany – w polskim postępowaniu karnym uczestnik postępowania definiowany w art. 71 § 1 kpk jako osoba, wobec której wydano postanowienie o przedstawieniu zarzutów albo której bez wydania takiego postanowienia postawiono zarzut w związku z rozpoczęciem przesłuchania w charakterze podejrzanego.

pierwszego przesłuchania te osoby uświadamiają sobie rozmiar oszustwa podatkowego, w którym uczestniczył podmiot gospodarczy założony z wykorzystaniem ich danych, i zaczynają rozważać możliwość ujawnienia tożsamości osób, które rzeczywiście zajmowały się prowadzeniem w ich imieniu rzekomej działalności gospodarczej.

Przedstawiciele środowiska przestępczego oraz ich obrońcy, dzięki doświadczeniom z lat wcześniejszych, najczęściej wiedzą, którzy prokuratorzy preferują określone sposoby prowadzenia postępowania. W przypadku sposobu defensywnego podejrzani nie dostrzegają żadnych korzyści płynących dla nich ze złożenia wyjaśnień zgodnych z prawdą i opisania mechanizmów oszustw podatkowych. Wręcz przeciwnie, mają świadomość, że złożenie takich wyjaśnień może spowodować ich wykluczenie z grupy dopuszczającej się tego typu przestępstw, a grupa w dalszym ciągu będzie mogła działać. Tym samym nie widzą możliwości swojej współpracy z organami ścigania.

Ze spostrzeżeń autora artykułu wynika, że w postępowaniach prowadzonych defensywnie podejrzani od chwili rozpoczęcia pierwszego przesłuchania w charakterze podejrzanego spodziewali się, mieli niemalże pewność, odpowiadania z wolnej stopy i konsekwentnie nie przyznawali się do popełnienia przestępstw. W czasie postępowań przygotowawczych prowadzonych w ten sposób właściwie nigdy nie udaje się rozbić zmowy milczenia wśród osób działających w ramach grupy przestępczej. Konsekwentnie nikt nie przyznaje się do winy. Proceder jest zatem bez większych przeszkód kontynuowany i nie ma powodu, dla którego podejrzani mieliby choćby zacząć zastanawiać się nad celowością składania wyjaśnień zgodnych z prawdą.

Jednocześnie w przypadku defensywnego sposobu prowadzenia postępowania przygotowawczego niekiedy przesłuchiwano w charakterze świadków osoby podejrzewane o popełnienie oszustwa z pouczeniem ich o treści art. 183 § 1 kpk[16], które to czynności były pozbawione większego sensu. Skutkiem ich przeprowadzenia może być (pośrednio) poinformowanie świadka – przez zadawane mu pytania – o zakresie przedmiotowym i podmiotowym śledztwa oraz o kierunkach zainteresowania śledczych. Skoro zatem np. śledczy zapyta przesłuchiwaną osobę A o działalność osoby fizycznej B, która z nią współpracuje w związku z funkcjonowaniem karuzeli podatkowej i która, według posiadanej wiedzy, jest np. opiekunem słupów, a formalnie w żaden sposób nie jest powiązana z żadnym podmiotem gospodarczym, to istnieje ryzyko, że osoba A poinformuje osobę B o tym, że organy ścigania się nią interesują. Osoba B zapewne podejmie czynności zmierzające do uniemożliwienia zabezpieczenia przez organy ścigania ewentualnych dowodów przestępczej działalności, które może jeszcze posiadać (może np. przechowywać w swoim miejscu zamieszkania lub pobytu dokumentację znikających podatników, dokonywać za pomocą swojego komputera przelewów na rachunkach bankowych czy przygotowywać dokumentację finansowo-

[16] Art. 183 § 1 kpk: „Świadek może uchylić się od odpowiedzi na pytanie, jeżeli udzielenie odpowiedzi mogłoby narazić jego lub osobę dla niego najbliższą na odpowiedzialność za przestępstwo lub przestępstwo skarbowe".

-księgową). Te materiały zapewne natychmiast po otrzymaniu ostrzeżenia zostaną usunięte z miejsca zamieszkania osoby B lub zniszczone.

Niestety, zdarzały się również sytuacje, w których prokuratorzy działający w sposób defensywny, pomimo uzyskania – jak się wydaje – mocnych dowodów potwierdzających świadomy udział określonej osoby w oszustwie podatkowym (np. zeznań kilku świadków lub wyjaśnień kilku podejrzanych) stali na stanowisku, że te informacje w dalszym ciągu były niewystarczające, aby przedstawić zarzuty ustalonym sprawcom oszustw, gdyż nie były dość szczegółowe, i wymagali uzyskania niemalże absurdalnie drobiazgowych danych (np. aby osoba składająca obciążające zeznania lub wyjaśnienia podawała wszystkie daty dzienne wystawionych faktur lub dokładne wartości zawarte we wszystkich wystawionych fikcyjnych fakturach, co w praktyce jest nierealne). Trudno zakładać, że osoba, która była zatrudniona np. jako pomoc biurowa, będzie pamiętała tak szczegółowe dane w sytuacji, gdy wystawiała kilkaset faktur w ciągu miesiąca.

Do opisanych przypadków – choć wydaje się to niezrozumiałe, a czasami nawet absurdalne – niestety dochodziło. Niweczyły one wysiłek funkcjonariuszy organów ścigania i niepowtarzalną okazję do pociągnięcia do odpowiedzialności karnej osób rzeczywiście organizujących oszustwa podatkowe, a nie tylko słupów, będących – jak to słusznie zauważył Jerzy Duży: (…) *pożywką dla organów ścigania*[17], oraz okazję do skutecznego zabezpieczenia konkretnych, mocnych dowodów, póki one istniały.

Modus operandi sprawców oszustw podatkowych, na co już wcześniej wskazywano, zakłada dopuszczenie do wiedzy na temat tych przestępstw jedynie ograniczonej grupy osób. Zdaniem autora w przypadku przyjęcia ofensywnego sposobu prowadzenia postępowania przygotowawczego, choć wymaga on zdecydowanie większego wysiłku zarówno od prokuratora, jak i od pozostałych organów ścigania i większego nakładu pracy, znacznie bardziej prawdopodobne jest uzyskanie wartościowych informacji pozwalających na ustalenie struktury grupy przestępczej (czasem nawet całej grupy lub znacznej jej części) oraz dokonanie zabezpieczeń majątkowych. Do uzyskania takich informacji, ustalenia osób znajdujących się wyżej w strukturze grupy przestępczej niż słupy oraz dokonania zabezpieczeń majątkowych w praktyce natomiast najczęściej nie dochodzi w przypadku postępowań prowadzonych defensywnie, gdy śledczy nie nadążają za działaniami sprawców oszustw podatkowych, a koncentrują się jedynie na działalności tzw. słupów i oględzinach wszystkich dokumentów.

Z obserwacji autora artykułu wynika również, że prokuratorzy preferujący defensywny sposób prowadzenia postępowania przygotowawczego najczęściej byli zwolennikami stosowania kwalifikacji w odniesieniu do oszustw podatkowych wyłącznie na podstawie kodeksu karnego skarbowego (zazwyczaj art. 56, art. 62 lub art. 76 kks) i wykluczali zarówno konstrukcję idealnego zbiegu czynów z art. 8 § 1 kks, jak i możliwość kwalifikacji jedynie na podstawie przepisów kodeksu karnego, co skutkowało

[17] J. Duży, *Zorganizowana przestępczość podatkowa w Polsce. Zwalczanie przestępnego nadużycia mechanizmów podatków VAT i akcyzowego*, Warszawa 2013, s. 40–42.

łagodniejszym karaniem sprawców tych przestępstw oraz krótszymi okresami przedawnienia[18]. Była to jednocześnie kolejna okoliczność, która powodowała, że podejrzani – wobec grożącej im niewielkiej (czasem symbolicznej) kary – odmawiali współpracy ze śledczymi.

Natomiast postępowanie prowadzone w sposób ofensywny najczęściej pozwala na skuteczne wstrzymywanie transakcji lub blokowanie rachunków na podstawie przepisów *Ustawy z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (DzU z 2018 r. poz. 723)[19], a także na dokonywanie zabezpieczeń majątkowych umożliwiających późniejsze odbieranie sprawcom oszustw przynajmniej części „owoców przestępstwa".

W analizowanym przez autora artykułu okresie ostatnich dziesięciu lat, a więc w głównej mierze jeszcze w czasie obowiązywania *Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (t.j.: DzU z 2017 r. poz. 1049), w postępowaniach prowadzonych w sposób ofensywny najczęściej była zauważalna owocna współpraca z Generalnym Inspektorem Informacji Finansowej (dalej: GIIF) w związku z planowanymi czynnościami polegającymi na zatrzymywaniu podejrzanych i na dokonywaniu przez GIIF, w koordynacji z prokuratorem, blokad rachunków bankowych powiązanych z podejrzanymi oraz z podmiotami gospodarczymi, które reprezentowali[20]. Brak koordynacji, chaos, przypadkowość działań i próba blokowania rachunków z opóźnieniem – często zauważalne w przypadku postępowań prowadzonych w sposób defensywny – zazwyczaj były zagrożone ryzykiem dokonania przez oszustów wyprzedzającego przelewu środków pieniężnych na rachunki bankowe innych podmiotów, co w przypadku przelewów na rachunki zagraniczne bezpowrotnie niweczyło możliwość dokonania zabezpieczenia majątkowego.

W ramach ofensywnego sposobu prowadzenia postępowania bardzo ważne jest również bieżące i kompleksowe ustalanie stanu majątkowego (m.in. rachunków bankowych, nieruchomości, pojazdów czy udziałów w spółkach) osób podejrzewanych o popełnienie oszustwa podatkowego jeszcze przed wykonaniem czynności z ich udziałem. Dzięki temu jest możliwe wydanie postanowienia o zabezpieczeniu majątkowym niemalże w tym samym czasie, w którym nastąpi przedstawienie zarzutów i uniemożliwienie podejrzanym zbycia składników majątkowych, które do nich należą. Te ustalenia są niekiedy określane mianem tzw. śledztwa finansowego, które

[18] Było to szczególnie widoczne do momentu wprowadzenia do kodeksu karnego *Ustawą z dnia 10 lutego 2017 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw* (DzU z 2017 r. poz. 244) przepisów art. 270a, 271a oraz art. 277a–277d.

[19] W okresie wcześniejszym na podstawie *Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (t.j.: DzU z 2017 r. poz.1049, ze zm.).

[20] Na podstawie nieobowiązującego już art. 19 ust. 1 ustawy z 16 listopada 2000 r.: „W przypadku otrzymania od Generalnego Inspektora zawiadomienia, o którym mowa w art. 18 ust. 1 zdanie drugie, prokurator może postanowieniem wstrzymać transakcję lub dokonać blokady rachunku na czas oznaczony, nie dłuższy jednak niż 3 miesiące od otrzymania tego zawiadomienia".

powinno być standardem w ramach każdego postępowania przygotowawczego, a niestety – jak wynika ze spostrzeżeń autora niniejszego artykułu – często nie jest.

Osoba dokonująca ustaleń majątkowych powinna zwrócić uwagę także na ewentualne zbycie majątku w związku ze spodziewaniem się ze strony sprawców oszustw przedstawienia im zarzutów. Ta okoliczność w praktyce jest możliwa do zweryfikowania przede wszystkim w odniesieniu do nieruchomości i środków pieniężnych zgromadzonych na rachunkach bankowych. Trudniej natomiast – przede wszystkim ze względów dowodowych – dokonać takich ustaleń np. w odniesieniu do gotówki czy przedmiotów wartościowych (nieewidencjonowanych).

Pożądane jest również przeprowadzenie – równolegle do toczącego się postępowania karnego – kontroli celno-skarbowej[21] w odniesieniu do podmiotów biorących udział w oszustwie podatkowym VAT, w tym firm słupów. Decyzje wydane w toku postępowania podatkowego przez naczelnika urzędu celno-skarbowego, choć rzecz jasna z uwagi na samodzielność jurysdykcyjną sądu karnego ich uzyskanie nie jest obowiązkiem organu procesowego, mogą stanowić ważny i pożądany dowód w ramach postępowania karnego.

Należy przypomnieć, że ustawodawca rozróżnia pojęcia właściwe prawu karnemu skarbowemu – uszczuplenie lub narażenie na uszczuplenie należności publicznoprawnej, i prawu podatkowemu – zobowiązanie podatkowe i wymiar zobowiązania podatkowego. Słusznie więc wskazywał – jeszcze przed reformą aparatu skarbowego w 2016 r. – Jerzy Duży[22], że o ile jedynie organy podatkowe w drodze decyzji mogą określić zobowiązanie podatkowe w sposób odmienny, niż dokonał tego podatnik w deklaracji podatkowej, o tyle powinnością autonomicznie działającego organu procesowego jest określenie wysokości należności publicznoprawnej uszczuplonej lub narażonej na uszczuplenie. Z drugiej strony warto pamiętać, że relacji wyroków administracyjnych do wyroków karnych ani decyzji administracyjnych do wyroków karnych nie określają żadne przepisy prawa. Ewentualna decyzja podatkowa powinna być zatem wykorzystana w postępowaniu karnym jako dowód istotny i podlegający swobodnej ocenie, który jednak nie ma waloru jakiejkolwiek decyzji procesowej w ramach postępowania karnego[23]. Zatem dopiero sąd orzekający w sprawie karnej dokona oceny zasadności decyzji organu administracji w zakresie potrzebnym do rozpoznania sprawy karnej. Natomiast pozbawione sensu jest – dokonywane przez niektórych prokuratorów opowiadających się za defensywnym sposobem prowadzenia postępowania przygotowawczego – zawieszanie postępowania karnego na podstawie art. 22 § 1 kpk[24] z uwagi na konieczność

[21] Art. 54 i nast. *Ustawy z dnia 16 listopada 2016 r. o Krajowej Administracji Skarbowej* (t.j.: DzU z 2020 r. poz. 505).

[22] J. Duży, *Zorganizowana przestępczość podatkowa*…, s. 163 i nast.

[23] Podobnie: wyrok SA w Warszawie z 11 VIII 2017 r., II AKa 210/17, LEX2347819.

[24] Art. 22 § 1 kpk: „Jeżeli zachodzi długotrwała przeszkoda uniemożliwiająca prowadzenie postępowania, a w szczególności jeżeli nie można ująć oskarżonego albo nie może on brać udziału

oczekiwania na zakończenie postępowania podatkowego, traktowanego w tym wypadku jako „długotrwała przeszkoda" w rozumieniu wskazanego wyżej przepisu. Pożądanym rozwiązaniem jest równoległy bieg obu postępowań i wzajemna koordynacja między organami prowadzącymi te postępowania, a także współpraca i wymiana informacji między nimi, co z pewnością będzie ograniczane w przypadku, gdy postępowanie karne zostanie zawieszone.

Bibliografia

Aronowitz A.A., Laagland D.C.G., Paulides G., *Value-Added Tax Fraud in the European Union*, New York–Amsterdam 1996, Kegler Publications.

Duyne P.C. van, *Organized crime and business crime-enterprises in the Netherlands*, „Crime, Law and Social Change" 1993, nr 2, s. 103–142.

Duyne P.C. van, Block A.A., *Organized cross-atlantic crime*, „Crime, Law and Social Change" 1995, s. 127–147.

Duży J., *Zorganizowana przestępczość podatkowa w Polsce. Zwalczanie przestępnego nadużycia mechanizmów podatków VAT i akcyzowego*, Warszawa 2013, Wolters Kluwer.

Glumińska-Pawlic J., Nowak K., *Oszustwa w podatku VAT: geneza, istota, przeciwdziałanie,* „Doradztwo Podatkowe – Biuletyn Instytutu Studiów Podatkowych" 2017, nr 10, s. 6–15.

Intra-Community VAT Fraud, Den Haag, Bonn, Brussel 2009, Algemene Rekenkamer, Bundesrechnungshof, Rekenhof.

Keen M., Smith S., *VAT Fraud and Evasion: What Do We Know, and What Can be Done?*, Washington 2007, International Monetary Fund.

Marszał K., *Proces karny. Zagadnienia ogólne*, Katowice 2013, wyd. II, Volumen.

Nowak K., *Wybrane zagadnienia dotyczące działalności tzw. słupów w ramach zorganizowanych grup przestępczych dopuszczających się oszustw podatkowych w związku z obrotem wyrobami stalowymi*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 171–185.

Pashev K., *Cross-border VAT fraud in an enlarged Europe*, w: *European crime-markets at cross-roads: Extended and extending criminal Europe*, P.C. van Duyne i in. (red.), Nijmegen 2008, Wolf Legal Publishers.

Pauch D., *Transakcja karuzelowa jako forma oszustwa w podatku od wartości dodanej*, „Annales Universitatis Mariae Curie-Skłodowska" 2016, nr 1, s. 621–629.

w postępowaniu z powodu choroby psychicznej lub innej ciężkiej choroby, postępowanie zawiesza się na czas trwania przeszkody".

PK-P1K, *Sprawozdanie z działalności powszechnych jednostek organizacyjnych prokuratury w sprawach karnych za rok 2018*, Warszawa 2019, Prokuratura Krajowa.

Wilk L., *„Kryminalne" aspekty przestępczości podatkowej*, „Archiwum Kryminologii" 2009, t. 31, s. 209–221.

Wyrok SA w Warszawie z 11 VIII 2017 r., II AKa 210/17, LEX2347819.

Strony internetowe

http:// www.arch.pg.gov.pl/upload_doc/000003715.pdf [dostęp: 6 III 2018].

http://www.money.pl/gospodarka/uszczelnianie-podatkow-mf-luka-vat-spadla-do-125-proc--w-2018-roku-6372387258513025a.html [dostęp: 23 IV 2019].

http://www.pk.gov.pl/sprawozdania-i-statystyki/sprawozdania-statystyczne-pg-p1k-pg-p1ca-i--pg-1n-za-2015-r.html#.WBeqJi3hCHs [dostęp: 6 III 2018].

http://www.podatki.gazetaprawna.pl/artykuly/965872,wiceszef-ms-25-lat-za-wyludzenia-vat--pod-koniec-2016.html [dostęp: 6 III 2018].

https://www.pk.gov.pl/g2/oryginal/2015_04/c3752155bf43c48bf342459d3e96865c.pdf [dostęp: 6 III 2018].

https://www.pk.gov.pl/wp-content/uploads/2018/01/c04ff96e25d267beeb4d5341305fcc16.pdf [dostęp: 7 IV 2019].

Abstrakt

Artykuł przedstawia dwa odmienne sposoby prowadzenia postępowania przygotowawczego w sprawach dotyczących oszustw w zakresie podatku VAT, ukształtowane w okresie ostatnich kilkunastu lat. Na podstawie ich metodyki można je określić jako sposób defensywny i sposób ofensywny. Skutkiem zastosowania sposobu defensywnego (zachowawczego) były najczęściej: brak możliwości skutecznego zwalczania oszustw VAT-owskich, brak dynamiki w działaniu śledczych, skupienie się niemal wyłącznie na zakończeniu oględzin wszystkich zabezpieczonych materiałów oraz niemożliwość ustalenia rzeczywistych organizatorów i beneficjentów procederu.

Model ofensywny (dynamiczny) natomiast jest oparty m.in. na: przedstawianiu podejrzanym zarzutów dotyczących popełnienia przestępstwa niezwłocznie po uzyskaniu informacji pozwalających na przeprowadzenie tej czynności, współpracy z GIIF i organami skarbowymi, zwróceniu szczególnej uwagi na dokonywanie zabezpieczeń majątkowych oraz występowaniu w uzasadnionych przypadkach z wnioskami

o tymczasowe aresztowanie, co jest wykluczone w przypadku postępowań prowadzonych przez prokuratorów będących zwolennikami sposobu defensywnego.

Słowa kluczowe: oszustwo, VAT, postępowanie karne, defensywny sposób prowadzenia postępowania, ofensywny sposób prowadzenia postępowania.

Abstract

This article presents two different ways of conducting the VAT investigations in the last several years, which can be described as defensive and offensive based on their methodology. The results of the adoption of the defensive model were most often the lack of the possibility of effective combating the VAT frauds, lack of dynamics of the investigators, focusing almost exclusively on completing survey reports and the inability to reveal the actual organizers and beneficients of the crime.

The offensive (dynamic) model is based eg. on prosecution immediately after obtaining information that allow carrying out this procedural step, cooperation with GIIF and tax authorities, and pay special attention to security on property and if necessary requests for provisional detention, which in practice was excluded by prosecutors who are supporters of the defensive model.

Keywords: fraud, VAT, investigation, defensive way of conducting the investigation, offensive way of conducting the investigation.

Paweł Gacek

Nawiązanie stosunku służbowego z funkcjonariuszami Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu. Charakter prawny mianowania – wybrane aspekty

Zgodnie z treścią art. 48 ust. 1 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[1] (dalej: uabwaw) stosunek służbowy[2] funkcjonariusza Agencji Bezpieczeństwa Wewnętrznego (ABW) albo Agencji Wywiadu (AW), zwanego dalej „funkcjonariuszem", powstaje w drodze mianowania[3] na podstawie dobrowolnego zgłoszenia się do służby. Pomimo użytego przez ustawodawcę określenia m i a n o w a n i e, nie wskazano precyzyjnie, co należy rozumieć pod tym pojęciem.

Analizując treść normy prawnej zawartej w przywołanym na początku przepisie, należałoby ustalić granice znaczeniowe pojęcia „mianowanie". Ustawodawca bowiem posługuje się nim w obrębie różnych gałęzi prawa, w celu określenia różnych rodzajowo (różnych typów) stosunków prawnych[4]. Zasadnicze różnice w znaczeniu tych pojęć mogą prowadzić do nieporozumień. Jest to o tyle istotne, że uregulowana w pragmatyce służbowej instytucja „mianowania", o której mowa w niniejszym artykule, wpływa w istotny sposób na kształt stosunku służbowego, a co za tym idzie –

---

1 Tekst jednolity: DzU z 2020 r. poz. 27.

2 Szerzej na temat pojęcia s t o s u n e k s ł u ż b o w y zob. T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy*, seria: *System prawa administracyjnego*, t. 11, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2011, s. 3 i nast.

3 Porównaj z § 4 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 2 lipca 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* (t.j.: DzU z 2013 r. poz. 862), a także z § 4 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 28 listopada 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Wywiadu* (DzU z 2003 r. nr 210 poz. 2039, ze zm.).

4 „Stosunku prawnego rozumianego jako jednego z rodzajów stosunków społecznych, tj. relacji pomiędzy co najmniej dwoma podmiotami prawa, w których zachowania (działania lub zaniechania) jednej strony wywołują reakcję (działania lub zaniechania) innej strony i podlegają kontroli norm społecznych (prawnych, moralnych, obyczajowych, wewnątrzorganizacyjnych)", za: T. Chauvin, T. Stawecki, P. Winczorek, *Wstęp do prawoznawstwa*, Warszawa 2009, s. 257. „Pojęciem stosunku prawnego określa się taki stosunek społeczny, który jest regulowany normą społeczną", za: Z. Rybicki, S. Piątek, *Zarys prawa administracyjnego i nauki administracji*, Warszawa 1984, s. 120 – i tam cytowany: R.O. Chałfina (zob. tenże, *Ogólna nauka o stosunku prawnym*, Warszawa 1979, s. 53). W tym samym duchu wypowiada się Z. Leoński (zob. tenże, *Zarys prawa administracyjnego*, Warszawa 2004, s. 32).

na prawa i obowiązki funkcjonariusza z niego wynikające. Stąd też niezbędne jest wyjaśnienie, że pomimo identycznej nazwy, „mianowanie" określone w pragmatyce służbowej nie jest pojęciem tożsamym z „mianowaniem" uregulowanym w innej gałęzi prawa, tj. w prawie pracy. Należy wyjaśnić zarówno główne różnice, jak i podobieństwa, jakie zachodzą między tymi pojęciami. Potrzebne jest również ustalenie ich granic znaczeniowych, a także wskazanie desygnatów, które stanowią o istocie tych – tak różnych od siebie – konstrukcji prawnych. Porównanie tych konstrukcji ujawni te odmienności i pozwoli na postawienie tezy *de lege ferenda* o konieczności zróżnicowania pojęcia „mianowanie", w zależności od gałęzi prawa, w ramach której zostało ono uregulowane. Omówienie tych zagadnień pozwoli na usytuowanie „mianowania" określonego w art. 48 ust. 1 uabwaw we właściwym środowisku. Tym samym będzie można precyzyjnie wskazać gałąź prawa, w której jest ono zakotwiczone.

Rodzaje mianowania

Jedną z form pracowniczego zatrudnienia, obok umowy o pracę, powołania, wyboru lub spółdzielczej umowy o pracę, jest mianowanie[5]. Zostało ono wskazane wprost w treści art. 76 *Kodeksu pracy*[6] (dalej: kp). Mianowanie wiąże się z jednej strony z powierzeniem indywidualnie wskazanej osobie kompetencji związanych z zajmowanym stanowiskiem, z drugiej – z nawiązaniem stosunku pracy[7]. Można zatem, dla zaakcentowania zainicjowania stosunku pracy (będącego rodzajem stosunku prawnego), użyć określenia „mianowanie pracownicze". Zainicjowanie stosunku pracy następuje w tym przypadku wyłącznie na podstawie aktu mianowania (nominacji) i dla swojej ważności nie wymaga potwierdzenia umową o pracę[8]. Charakter tego rodzaju aktu mianowania budzi jednak wątpliwości. Jedni uważają, że mianowanie jest aktem administracyjnym[9], inni natomiast uznają akt mianowania za swoistą czynność z zakresu

[5] „Kodeks pracy ustalił pięć podstaw stosunku pracy", za: W. Muszalski, *Prawo socjalne*, Warszawa 1996, s. 31. Wykaz tych podstaw ma charakter wyczerpujący. Zob. *Kodeks pracy. Komentarz*, Z. Salwa (red.), Warszawa 2000, s. 13. Szerzej na temat stosunków służbowych w administracji zob. W. Jaśkiewicz, *Stosunki służbowe w administracji*, Warszawa–Poznań 1969.

[6] *Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy* (t.j.: DzU z 2019 r. poz. 1040, ze zm.).

[7] „Stosunek pracy na podstawie mianowania jest stosunkiem administracyjno-prawnym w sferze prawa pracy. (…) Akt mianowania zawiera w sobie dwa elementy: wyposażenie w część władztwa państwowego określającego kompetencję danej osoby do działania w imieniu państwa oraz nawiązanie stosunku pracy (jak dawniej określano służby)", za: *Kodeks pracy. Komentarz*, W. Muszalski (red.), Warszawa 2017, Legalis (komentarz do art. 76 kp); w tym samym tonie zob. tenże, *Prawo socjalne*…, s. 32.

[8] A. Giedrewicz-Niewińska, komentarz do art. 76 kp. Zob. *Kodeks pracy. Komentarz*, K. Walczak (red.), Warszawa 2017, Legalis.

[9] „Stosunek pracy z mianowania (służbowy) powstać może wyłącznie w wyniku aktu mianowania, który jest decyzją administracyjną w rozumieniu art. 104 k.p.a.", za: postanowienie Naczelnego Sądu Administracyjnego (dalej: NSA) z 15 IV 1991 r., II SA 258/91, Legalis nr 143575);

prawa pracy[10]. Mimo omówionych wcześniej rozbieżności co do charakteru nominacji[11], poza sporem jest to, że zainicjowanie tego rodzaju więzi prawnej powoduje nawiązanie stosunku pracy.

Oprócz wyżej wskazanego mianowania istnieje odrębna kategoria stosunków prawnych mających tę samą nazwę. Stąd też konieczne jest zaakcentowanie, że pomimo jednej nazwy, mianowanie, o którym mowa w kp, nie jest tożsamą konstrukcją prawną z mianowaniem wskazanym w art. 48 ust. 1 uabwaw[12]. Stosunek służbowy w formacjach zmilitaryzowanych czy paramilitarnych, w tym nawiązywany z funkcjonariuszami ABW i AW, ma charakter wyłącznie administracyjny[13]. Oznacza to, że powstała więź prawna nie implikuje automatycznie nawiązania stosunku pracy[14]. Należy podzielić stanowisko Anety Korcz-Maciejko, według której: (…) *nie mamy zatem do czynienia ze zmodyfikowanym stosunkiem pracy uregulowanym w Kodeksie pracy, ale ze stosunkiem zatrudnienia, który czerpie swój byt z władczej, jednostronnej wypowiedzi organu administracji publicznej skierowanej do osoby zatrudnionej*

„Stosunek pracy na podstawie mianowania jest stosunkiem administracyjnoprawnym w sferze prawa pracy", za: wyrok NSA z 24 IX 1991 r., II SA 746/91, Legalis nr 36962) – orzeczenia dotyczą pracowników NBP. W tym samym duchu zob. *Kodeks pracy. Komentarz*, W. Muszalski (red.)…, (komentarz do art. 76 kp).

[10] „Akt mianowania na stanowisko nauczyciela nie jest decyzją administracyjną w rozumieniu przepisów Kodeksu postępowania administracyjnego", za: wyrok Sądu Najwyższego (dalej: SN), Izba Administracyjna, Pracy i Ubezpieczeń Społecznych z 10 IV 1997 r., I PKN 57/96, Legalis nr 30942; wyrok SN, Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z 23 XI 2004 r., I PK 35/04, Legalis nr 68713; wyrok SN, Izba Administracyjna, Pracy i Ubezpieczeń Społecznych z 18 VI 1998 r., I PKN 167/98, Legalis nr 43387. Krytycznie do tego odnoszono się w doktrynie. Zob. A. Giedrewicz-Niewińska, komentarz do art. 76 kp, w: *Kodeks pracy. Komentarz*, K. Walczak (red.)…, i tam przywołana literatura.

[11] W tym przypadku n o m i n a c j a jest rozumiana jako powierzenie obywatelowi w drodze aktu administracyjnego stanowiska związanego z wykonywaniem funkcji z zakresu działania administracji, tzw. inwestyturę, za: L. Florek, T. Zieliński, *Prawo pracy*, wyd. 5, Warszawa 2003, s. 75.

[12] P. Wojtunik, *Pojęcie, źródła i przedmiot stosunków służbowych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 202 i nast.

[13] Jak wynika z definicji zawartej w *Leksykonie policyjnym*, stosunek służbowy jest stosunkiem administracyjno-prawnym powstającym z mianowania na podstawie dobrowolnego zgłoszenia się do służby. Nie jest to stosunek pracy w rozumieniu kodeksu pracy. Zob. *Leksykon policyjny*, W. Pływaczewski i G. Kędzierska (red.), Szczytno 2001, s. 304. Chociaż ta definicja została sformułowana w odniesieniu do funkcjonariusza Policji, można ją odnieść *per analogiam* do funkcjonariuszy wszystkich służb mundurowych, których podstawą zatrudnienia jest mianowanie.

[14] M. Liwo, *Status służb mundurowych i funkcjonariuszy w nich zatrudnionych*, Warszawa 2013, s. 311; W. Maciejko, A. Korcz-Maciejko, *Postępowanie w sprawach osobowych w Policji*, Wrocław 2010, s. 20; J. Kacprzak, *Stosunki służbowe w formacjach zmilitaryzowanych – charakter prawny, ochrona sądowa*, „Przegląd Policyjny" 1994, nr 1, s. 97. Odmienne stanowisko zajmuje Tadeusz Hanausek, który wskazuje, w odniesieniu do mianowania funkcjonariuszy Policji, że stosunek służbowy wiąże się również z nawiązaniem stosunku pracy. Nie rozwija jednak argumentacji potwierdzającej tę tezę. Zob. tenże, *Ustawa o Policji. Komentarz*, Kraków 1996, s. 72.

w aparacie administracji publicznej[15]. Mianowanie jest więc formą niepracowniczego zatrudnienia[16]. Jak słusznie zauważa Naczelny Sąd Administracyjny: *Są dwa rodzaje mianowania (nominacji). Mianowanie (nominacja), które powoduje powstanie stosunku pracy (tzw. służbowego stosunku pracy), o jakim mowa w art. 76 Kodeksu pracy, oraz mianowanie (nominacja), której skutkiem jest powstanie stosunku służbowego o charakterze administracyjno-prawnym. Drugi rodzaj mianowania dotyczy służb mundurowych*[17].

Wspólną cechą obu stosunków prawnych jest to, że mianowanie zostało przewidziane wyłącznie dla określonych kategorii grup zawodowych. W przypadku mianowania z art. 76 kp są to np. nauczyciele czy pracownicy korpusu służby cywilnej[18], w przypadku zaś formacji zmilitaryzowanych – funkcjonariusze tych służb. Status pracowników i funkcjonariuszy został także uregulowany w odrębnych aktach prawnych, które są nazywane pragmatykami. Aby jednak rozgraniczyć te dwa typy stosunków prawnych, należałoby stosować nomenklaturę, która w sposób wyraźny pozwoli na ich rozróżnienie. Mianowanie, o którym mowa w art. 76 kp, należałoby określać jako: pracowniczy stosunek służbowy z mianowania, stosunek służbowy typu pracowniczego z mianowania albo mianowanie pracownicze, w przypadku mianowania funkcjonariuszy poszczególnych służb jest zasadne stosowanie pojęcia: stosunek służbowy z mianowania. Zatem w odniesieniu do aktów regulujących status osób zatrudnionych na podstawie mianowania (pierwsza z wymienionych grup zawodowych) należałoby mówić o pragmatykach pracowniczych[19], a w odniesieniu do aktów regulujących status funkcjonariuszy poszczególnych formacji – o pragmatykach służbowych.

Szczegółowe omówienie różnic między mianowaniem z art. 76 kp a mianowaniem, o którym mowa w art. 48 ust. 1 uabwaw, przekracza ramy tego opracowania.

---

[15] A. Korcz-Maciejko, *Prawny charakter rozkazu personalnego*, „Administracja. Teoria. Dydaktyka. Praktyka" 2013, nr 3, s. 138 i nast.

[16] *Wielka encyklopedia prawa*, B. Hołyst (red.), Warszawa 2005, s. 981. Mowa tam o pozapracowniczym charakterze stosunków służbowych. W tym samym duchu W. Muszalski, *Prawo socjalne*…, s. 31.

[17] Wyrok NSA z 3 X 2006 r., I OSK 210/06, Legalis nr 606379; „Stosunek służbowy policjanta powstaje w drodze mianowania, które nie jest mianowaniem w rozumieniu Kodeksu pracy z uwagi na występowanie w tym stosunku elementów o charakterze władczego kształtowania sytuacji funkcjonariusza. Stosunek służbowy policjanta ma charakter administracyjno-prawny, za: wyrok Wojewódzkiego Sądu Administracyjnego (dalej: WSA) w Białymstoku z 23 II 2006 r., II SA/Bk 943/05, Legalis nr 826774; wyrok WSA w Poznaniu z 5 II 2009 r., IV SA/Po 430/08, Legalis nr 170824; wyrok WSA w Warszawie z 10 XII 2007 r., II SA/Wa 1620/07, Legalis nr 121289 – dotyczące stosunku służbowego policjanta. Zob. także: wyrok NSA z 5 VI 1991 r., II SA 35/91, ONSA z 1991 r., nr 3, poz. 64.

[18] Szerzej na temat statusu pracownika administracji państwowej zob. J. Łętowski, *Polecenie służbowe w administracji*, Warszawa 1974, s. 9 i nast.

[19] Jan Piątkowski używa pojęcia pragmatyka urzędnicza. Zob. J. Piątkowski, M.K. Kolasiński, A. Kolasiński, *Stosunki pracy w administracji publicznej (na tle prawa wspólnotowego)*, Toruń 2008, s. 85.

Warto jedynie wskazać na podstawowe różnice między tymi stosunkami prawnymi. Jak wspomniano wyżej, mianowanie z art. 76 kp wiąże się jednocześnie z aktem nominacji, który jest decyzją administracyjną, i z nawiązaniem stosunku pracy. Natomiast stosunek służbowy skutkuje wyłącznie zainicjowaniem więzi prawnej mającej charakter administracyjno-prawny, co powoduje, że funkcjonariusze poszczególnych służb nie są pracownikami w rozumieniu art. 2 kp, a właściwi przełożeni, tj. szef ABW oraz szef AW, nie są pracodawcami w rozumieniu art. 3 kp. Wynika to z wykładni literalnej art. 2 kp[20] oraz art. 3 kp[21], zgodnie z którymi pracownikiem jest wyłącznie osoba fizyczna zatrudniona na jednej z podstaw wskazanych w tym przepisie, a pracodawcą jednostka organizacyjna, choćby nie posiadała osobowości prawnej, a także osoba fizyczna, jeżeli zatrudnia ona pracowników. Skoro szef ABW oraz szef AW nie zatrudniają pracowników, to nie mogą spełniać kryteriów pozwalających na uznanie ich za pracodawców[22] funkcjonariuszy, którzy są zatrudnieni w danej służbie. W odniesieniu do osób zatrudnionych na podstawie mianowania w formacjach zmilitaryzowanych czy paramilitarnych bardziej adekwatne byłoby stosowanie pojęcia funkcjonariusz, a do podmiotów, którym przysługują kompetencje do ich zatrudnienia – podmiot zatrudniający[23].

Inną cechą charakterystyczną pragmatyk pracowniczych i pragmatyk służbowych jest to, że regulują one status poszczególnych grup zawodowych w sposób kompleksowy. Różni je to, że w przypadku pragmatyk pracowniczych w sprawach nieuregulowanych należy stosować przepisy prawa pracy, na zasadzie art. 5 kp. Zatem subsydiarne (posiłkowe)[24] stosowanie regulacji kodeksu pracy następuje wyłącznie w obszarach

[20] W art. 2 kp zdefiniowano pojęcie pracownik. Jest to definicja legalna. Pracownikiem jest wyłącznie osoba pozostająca w stosunku pracy, bez względu na szczególny sposób jego powstawania, trwałość więzi prawnej oraz okoliczność, czy praca stanowi dla niej zajęcie główne czy uboczne, a także jaką rolę odgrywa dochód z pracy w jej statusie majątkowym. Zob. *Kodeks pracy. Komentarz*, A. Sobczyk (red.), Warszawa 2017, Legalis (komentarz do art. 2 kp); A.M. Świątkowski, *Kodeks pracy. Komentarz*, wyd. 2, Warszawa 2006, s. 9.

[21] „Elementem definicji pracodawcy jest zatrudnienie pracowników. Tym samym pracodawcą jest podmiot, który zatrudnia co najmniej jednego pracownika", za: *Kodeks pracy. Komentarz*, A. Sobczyk (red.)… (komentarz do art. 2 kp); „Drugą stroną stosunku pracy jest pracodawca, czyli każdy kto zatrudnia pracownika (…)", za: W. Muszalski, *Prawo socjalne*…, s. 30. W tym samym duchu: *Kodeks pracy. Komentarz*, Z. Salwa (red.)…, s. 14 i nast. (w przytaczanych przykładach chodzi o pracownika w rozumieniu art. 2 kp).

[22] Należy dodać, że mogą oni być pracodawcami w stosunku do osób cywilnych zatrudnionych w tej organizacji, jeśli to zatrudnienie następuje na jednej z podstaw wskazanych w art. 2 kp. Nie są natomiast pracodawcą w stosunku do funkcjonariuszy zatrudnionych w tych formacjach. Funkcjonariusze nie mogą bowiem łączyć różnych podstaw zatrudnienia w danej formacji. Nie jest możliwe zatrudnienie osoby na podstawie stosunku służbowego z mianowania w danej formacji i jednocześnie zatrudnienie jej w tej samej formacji na podstawie stosunku pracy (na jednej z podstaw wskazanych w art. 2 kp).

[23] Aneta Korcz-Maciejko używa pojęć: osoba zatrudniona oraz podmiot zatrudniający. Zob. taż, *Prawny charakter rozkazu personalnego*…, s. 139.

[24] W. Muszalski i in., *Kodeks pracy z komentarzem*, Gdańsk 1996, s. 20.

nieuregulowanych. Jeśli dana pragmatyka pracownicza zawiera określone rozwiązania, nawet mniej korzystne niż to wynika z przepisów powszechnego (ogólnego) prawa pracy, ma ona pierwszeństwo stosowania[25]. Nie jest przy tym konieczne, aby w danej pragmatyce pracowniczej została zawarta norma zezwalająca na posiłkowe stosowanie przepisów prawa pracy. Wystarczającą podstawą jest regulacja art. 5 kp, odsyłająca do przepisów prawa pracy w przypadku niekompletności uregulowań danej pragmatyki pracowniczej.

Pragmatyki służbowe, z uwagi na odrębność konstrukcji stosunku służbowego, w zakresie nieuregulowanym nie korzystają z wyżej wymienionego ogólnego odesłania do kodeksu pracy[26]. Jak zauważa Tadeusz Zieliński, pragmatyki służbowe normujące stosunki służbowe nie są aktami szczególnymi wobec kodeksu pracy (w rozumieniu art. 5 kp), czego konsekwencją jest wyłączenie możliwości subsydiarnego stosowania tego aktu w sprawach nieuregulowanych w tych pragmatykach[27]. Takie odesłanie (zarówno do kodeksu pracy, jak i do przepisów zawartych w odrębnych regulacjach prawnych) jest możliwe wyłącznie w przypadku przepisu szczególnego, zawartego w pragmatyce służbowej lub w aktach do niej wykonawczych. W takiej sytuacji przepis szczególny wskazuje na zakres możliwego, tj. dopuszczalnego, stosowania nie tylko przepisów prawa pracy, lecz także norm zawartych w regulacjach

[25] Jak zauważa Jan Piątkowski, pragmatyki urzędnicze są regulacjami wyprzedzającymi w stosunku do kodeksu pracy. Zob. J. Piątkowski, M.K. Kolasiński, A. Kolasiński, *Stosunki pracy w administracji publicznej*…, s. 85. „Kodeks pracy obowiązuje w stosunku do wszystkich pracowników, bez wyjątku, niemniej czyni to dwojako, a mianowicie albo obowiązuje w pełni bezpośrednio, co ma miejsce w większości przypadków, albo pośrednio w sposób pomocniczy w tych przypadkach, w których warunki pracy danej grupy pracowników są regulowane odrębną ustawą. Te ustawy stanowią regulację szczególną w stosunku do przepisów Kodeksu pracy. Wówczas obowiązują postanowienia takiej ustawy szczególnej, a Kodeks pracy znajduje zastosowanie jedynie w sprawach nieuregulowanych ustawą szczególną. (…) Dopiero w razie braku regulacji danej kwestii w ustawie szczególnej znajduje zastosowanie przepis Kodeksu pracy bezpośrednio, a nie w sposób odpowiedni. Ustawy szczególne są bowiem tak pomyślane, aby regulowały jedynie kwestie wymagające regulacji odmiennej, pozostawiając bezpośrednio w mocy Kodeksu pracy te, w których nie zachodzi potrzeba różnicowania", za: *Kodeks pracy. Komentarz*, W. Muszalski (red.)…, (komentarz do art. 5 kp).

[26] Postanowienie SN, Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z 19 II 2014 r., I PK 264/13, Legalis nr 1169341; wyrok SN, Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z 7 IV 2009 r., I PK 218/08, Legalis nr 158199; uchwała SN, Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z 18 III 2008 r., II PZP 3/08, Legalis nr 95381 (dotyczą funkcjonariusza Państwowej Straży Pożarnej); wyrok NSA z 30 VI 2010 r., I OSK 78/10, Legalis nr 293195, wyrok NSA z 18 XII 2008 r., I OSK 12/08, Legalis nr 186470, wyrok NSA z 28 X 2008 r., I OSK 1721/07, Legalis nr 207868 (dotyczą funkcjonariusza służby więziennej); wyrok NSA z 3 X 2006 r., I OSK 210/06 (dotyczy funkcjonariusza służby celnej). Odmienne stanowisko stanowiące wyjątek od reguły, ugruntowanej w doktrynie i judykaturze, przyjął Trybunał Konstytucyjny w odniesieniu do funkcjonariuszy ABW i AW w kontekście problematyki związanej z uprawnieniami do urlopu wychowawczego. Zob. wyrok TK z 29 VI 2006 r., P 30/05, OTK – A z 2006 r., nr 6, poz. 70, także: DzU z 2006 r. nr 122 poz. 852.

[27] T. Zieliński, *Stosunek prawa pracy do prawa administracyjnego*, Warszawa 1977, s. 180.

należących do innych gałęzi prawa. Brak stosownego przepisu regulującego daną sferę praw i obowiązków funkcjonariusza danej formacji, a także brak przepisu umożliwiającego skorzystanie w tym zakresie z regulacji pozostającej poza pragmatyką służbową powoduje, że takie uprawnienie czy obowiązek nie istnieją w odniesieniu do funkcjonariusza. Nie ma też instrumentów prawnych, które służą ochronie przed nieuprawnionym naruszeniem tej sfery.

Charakter prawny stosunku służbowego z mianowania

Jak już wspomniano, stosunek służbowy z mianowania jest rodzajem stosunku administracyjno-prawnego. Eugeniusz Ochendowski zauważa[28], że stosunki prawne pomiędzy państwem i działającymi w jego imieniu podmiotami administracji publicznej a obywatelami są oparte na normach wynikających z przepisów prawa administracyjnego. Stąd też te kategorie uregulowań prawnych są nazywane administracyjno-prawnymi.

Stosunek administracyjno-prawny powstaje, gdy organ administracji publicznej, na podstawie przepisu prawa, występuje do zindywidualizowanego adresata (będącego podmiotem zewnętrznym wobec niego), nakłada na niego określone obowiązki lub przyznaje mu określone uprawnienia, żąda od niego określonego świadczenia albo na coś mu zezwala[29]. Ma on zatem, w przeciwieństwie do stosunków cywilnoprawnych (obligacyjnych), charakter władczy, co wyróżnia ten typ stosunków prawnych spośród innych.

Zasadnicze znaczenie dla pojęcia s t o s u n e k a d m i n i s t r a c y j n o - p r a w n y ma istnienie przepisu prawa statuującego właściwy podmiot administracji publicznej oraz jego kompetencje do nawiązania określonego rodzaju stosunków. Organy administracyjne są zawsze zobowiązane do działania na podstawie przepisów prawa oraz w granicach wyznaczonych przez to prawo (przez normę wynikającą z konkretnych przepisów).

Szczególną cechą stosunku administracyjno-prawnego są elementy składające się na jego konstrukcję, tj.:

- podmiot (z jednej strony podmiot administracyjny lub inny podmiot pełniący funkcję administracyjną, z drugiej – podmiot zewnętrzny wobec tego pierwszego),
- przedmiot (sprawy z zakresu administracji publicznej objęte działalnością wskazanych wyżej podmiotów administracyjnych lub innych podmiotów pełniących funkcję administracyjną, prowadzoną w formach określonych prawem),
- treść (prawa i obowiązki podmiotów uczestniczących w tym stosunku)[30].

---

[28] E. Ochendowski, *Prawo administracyjne. Część ogólna*, wyd. 8, Toruń 2009, s. 45 i nast.

[29] *Zarys prawa*, J. Kuciński (red.), Warszawa 2010, s. 184.

[30] Z. Rybicki, S. Piątek, *Zarys prawa administracyjnego*…, s. 121. Z kolei Janusz Łętowski wskazuje na takie cechy stosunku administracyjno-prawnego, jak: indywidualny charakter (łączy

Tym, co odróżnia stosunki administracyjno-prawne od innego rodzaju stosunków jest zatem zarówno podmiot, przedmiot, jak i jego treść.

Podmiotami są, z jednej strony, wyłącznie organy administracji publicznej[31] (w tym przypadku szef ABW lub szef AW), z drugiej – podmiot zewnętrzny (w tym przypadku osoba fizyczna). Stosunek administracyjno-prawny *in genere* zakłada nierównorzędność podmiotów[32], co oznacza, że organ może jednostronnie i w sposób władczy określić jego treść[33]. Może on więc, co do zasady, w celu realizacji praw i obowiązków wynikających z zaistniałego stosunku prawnego, korzystać ze środków prawnych, które umożliwiają wyegzekwowanie przymusowego ich wykonania.

Stosunek służbowy jest szczególnego rodzaju stosunkiem administracyjno-prawnym, został on bowiem ograniczony wyłącznie do podmiotów wskazanych w uabwaw, czyli szefa ABW albo szefa AW (podmiot administracji publicznej) oraz funkcjonariusza tych służb (zindywidualizowany podmiot), wobec którego podmiot wskazany jako pierwszy działa władczo. Szef ABW lub szef AW pełni zatem funkcję organu administracyjnego. Jest to organ jednoosobowy. Istotne w tym przypadku jest to, że nie może on scedować swoich uprawnień do nawiązania stosunku służbowego (administracyjno-prawnego) na żaden inny podmiot. Treść normy wynikającej z art. 50 ust. 1 uabwaw nie pozostawia wątpliwości, że w zakresie swojego działania szef ABW i szef AW są właściwi do przyjmowania kandydatów do służby (nawiązania z nimi stosunku służbowego z mianowania, w wyniku czego stają się oni funkcjonariuszami) w podległych im formacjach. Zarówno tej kompetencji, jak i pozostałych, enumeratywnie wymienionych w tym przepisie, nie mogą przenieść na inny podmiot. W innych sprawach (mających przymiot sprawy osobowej) mogą oni scedować swoje uprawnienia na innych przełożonych, przez siebie upoważnionych (art. 50 ust. 2 uabwaw),

konkretnie oznaczony podmiot z konkretnie oznaczonym organem wykonującym zadania administracyjne, dotyczy jednostkowej, indywidualnie oznaczonej sprawy), ma charakter władczy (jedna z jego stron reprezentująca państwo może stosować środki przymusu w celu jego realizacji), powstaje na podstawie wyraźnie wskazanych przepisów prawa administracyjnego, a rozstrzyganie konfliktów pojawiających się na tle treści tego stosunku następuje w trybie procedury administracyjnej. Charakterystyczną cechą stosunku administracyjnego są podmioty tego stosunku (z jednej strony podmiot administracyjny lub podmiot upoważniony przez prawo do wykonywania funkcji administracyjnych, z drugiej – podmiot niezwiązany organizacyjnie lub służbowo z administracją). Zob. tenże, *Prawo administracyjne. Zagadnienia podstawowe*, Warszawa 1990, s. 52 i nast. Zbigniew Leoński, wskazując na cechy charakterystyczne stosunku administracyjno-prawnego, wymienia: przedmiot, podmioty w nim występujące oraz wzajemny układ między tymi podmiotami. Zob. tenże, *Zarys prawa administracyjnego*…, s. 32. Porównaj także z elementami stosunku administracyjnego wskazanymi przez Jerzego Starościaka. Zob. tenże, *Administracja. Zagadnienia teorii i praktyki*, Warszawa 1974, s. 216 i nast.

[31] Szerzej na temat pojęcia organ administracji w doktrynie prawa administracyjnego zob. G. Łaszczyca, Cz. Martysz, A. Matan, *Postępowanie administracyjne ogólne*, Warszawa 2003, s. 169 i nast. oraz tam cytowana literatura.

[32] W przeciwieństwie do stosunku pracy, w ramach którego obie strony tego stosunku, tj. pracownik i pracodawca, co do zasady są równorzędne. Zob. W. Muszalski, *Prawo socjalne*…, s. 30.

[33] Tę cechę akcentuje także Zbigniew Leoński. Zob. tenże, *Zarys prawa administracyjnego*…, s. 32.

z zastrzeżeniem, że te uprawnienia nie mogą obejmować spraw określonych w art. 50 ust. 1 uabwaw, w tym szczególnie prawa do zainicjowania, zmiany i rozwiązania więzi prawnej, wynikającej ze stosunku służbowego z mianowania. Warte podkreślenia jest to, że art. 50 ust. 1 uabwaw stanowi *numerus clausus* przełożonych właściwych do nawiązania, zmiany i rozwiązania stosunku służbowego. Norma wynikająca z przepisu art. 50 ust. 1 uabwaw ma charakter kompetencyjny. Na jej podstawie wyznaczono krąg podmiotów, którym zostały przekazane określone uprawnienia (kompetencje), a także wyznaczono ich zakres (granice). Nie jest zatem możliwe skuteczne nawiązanie tego stosunku, jeśli dany rozkaz personalny (decyzja administracyjna) zostanie wydany przez organ administracyjny inny niż szef ABW albo szef AW. Taka decyzja byłaby dotknięta wadą kwalifikowaną i jako taka musiałaby zostać usunięta z obrotu prawnego przez stwierdzenie jej nieważności, na zasadzie art. 156 § 1 pkt 1 *Kodeksu postępowania administracyjnego*[34] (dalej: kpa). Czynności wskazane w art. 50 ust. 1 uabwaw są bowiem zastrzeżone wyłącznie dla określonego przełożonego, jakim jest szef ABW albo szef AW. Oczywiste jest natomiast, że oba podmioty mogą wykonywać czynności związane z nawiązaniem, zmianą albo rozwiązaniem stosunku służbowego tylko w odniesieniu do osób zatrudnionych w podległych im formacjach.

Drugą stroną stosunku służbowego może być jedynie osoba fizyczna, która po spełnieniu wszystkich wymogów określonych w art. 44 uabwaw[35], stwierdzonych w wyniku pozytywnie przeprowadzonego wobec niej postępowania kwalifikacyjnego, nawiązała stosunek służbowy z mianowania. Przed jego nawiązaniem osobie fizycznej przysługuje status kandydata do odpowiedniej służby. Nawiązanie więzi prawnej przez przyjęcie rozkazu personalnego o mianowaniu powoduje zmianę dotychczasowego statusu tej osoby. Od tego momentu staje się ona funkcjonariuszem ABW albo AW. Ten przymiot przysługuje jej tak długo, jak długo istnieje stosunek służbowy, i kończy się z chwilą jego rozwiązania (art. 54 ust. 3 oraz art. 60 uabwaw), jego wygaśnięcia wskutek śmierci tej osoby albo nieobecności funkcjonariusza w służbie powyżej trzech miesięcy z powodu tymczasowego aresztowania – chyba że wcześniej nastąpiło zwolnienie funkcjonariusza ze służby (art. 61 uabwaw).

Stosunek służbowy funkcjonariusza ABW albo AW z pewnością leży w sferze publicznej, gdyż po nawiązaniu tej więzi prawnej osoba fizyczna jest wyposażana w swoistego rodzaju *imperium*[36], upoważniające ją do działania w imieniu państwa. Stosunek służbowy funkcjonariusza ABW albo AW, a także innych funkcjonariuszy formacji zmilitaryzowanych, jest zatem stosunkiem publicznoprawnym, ponieważ jest przeznaczony do realizacji celu publicznego. Konsekwencją tego jest

[34] *Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego* (t.j.: DzU z 2018 r. poz. 2096, ze zm.).

[35] P. Gacek, *Wymogi formalne niezbędne do pełnienia służby w Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 56 i nast.

[36] Określony prawem zakres władzy decyzyjnej organów państwowych (przyp. red.).

usytuowanie przez prawodawcę kwestii z nim związanych ściśle w sferze norm prawa administracyjnego[37]. Dlatego też wszelkie formalności dotyczące stosunku służbowego (związane z jego nawiązaniem, zmianą i rozwiązaniem) należy odnosić do szeroko rozumianych spraw z zakresu administracji publicznej.

Istotnym elementem stosunku administracyjno-prawnego oprócz wymienionych stron, czyli organu administracyjnego i podmiotu zewnętrznego, oraz przedmiotu są prawa i obowiązki wynikające z nawiązanego stosunku służbowego. Stanowią one jego treść.

Stosunek służbowy jest zorientowany na określenie praw i obowiązków zindywidualizowanego adresata, jakim jest funkcjonariusz odpowiedniej służby. W wyniku nawiązania tej więzi prawnej jednostka, tj. osoba fizyczna będąca podmiotem zewnętrznym wobec organu administracyjnego, zostaje włączona w strukturę organizacyjną odpowiedniej formacji i staje się tym samym (od tego momentu) jego częścią składową (elementem składowym). Nie oznacza to, że w wyniku nawiązania stosunku służbowego taka jednostka zostaje tym samym włączona w skład struktury samego organu. Organ reprezentują wyłącznie właściwi przełożeni, w tym przypadku szef ABW albo szef AW. Stosunek służbowy nie powoduje scalenia (zespolenia) organu z jednostką, która w wyniku przyjęcia nominacji stała się funkcjonariuszem, a jedynie włączenie jej w skład osobowy właściwej organizacji.

Jak każdy inny stosunek administracyjny, tak i ten zakłada nierównorzędność stron. Jego indywidualną cechą jest jednak to, że musi być poprzedzony dobrowolnym zgłoszeniem się osoby fizycznej do służby w ABW albo AW. Co do zasady organy administracyjne mogą działać z urzędu lub na wniosek zainteresowanego[38]. W tym przypadku jedyną możliwością zainicjowania stosunku służbowego jest złożenie wniosku przez osobę fizyczną, tj. kandydata do służby. Dobrowolność bowiem stoi u podstaw służby. Należy dodać, że dobrowolność nie ogranicza się wyłącznie do wstąpienia do ABW, AW bądź do innych formacji zmilitaryzowanych. Stanowi ona warunek *sine qua non* istnienia (kontynuacji) tego stosunku. Jej brak skutkuje zaś koniecznością rozwiązania stosunku służbowego. Jedynie dobrowolność daje upoważnienie właściwemu przełożonemu do egzekwowania obowiązków wynikających z treści tego stosunku. Stąd też jest ważne, aby ta dobrowolność była wyraźna. Niedopuszczalne jest jej domniemywanie. Nie oznacza to, że organ (przełożony) jest zobowiązany do badania jej istnienia na każdym etapie trwania stosunku służbowego. Kandydat do służby, składając dokumenty w postępowaniu kwalifikacyjnym, wypełnia kwestionariusz osobowy, co skutkuje wszczęciem wobec niego postępowania kwalifikacyjnego.

---

[37] Zagadnienia dotyczące prawa administracyjnego jako prawa publicznego omawia Jan Boć. Zob. *Prawo administracyjne*, J. Boć (red.), Wrocław 2001, s. 37 i nast.

[38] Stosunki administracyjno-prawne mogą powstać z mocy ustawy, w drodze aktu administracyjnego, przez zgłoszenie się strony z roszczeniem o określone zachowanie organu administracyjnego bądź przez działania faktyczne. Zob. *Zarys prawa*…, s. 187 i nast., a także Z. Rybicki, S. Piątek, *Zarys prawa administracyjnego*…, s. 121. Stosunek służbowy może powstać wyłącznie w drodze wydanego rozkazu personalnego (aktu administracyjnego), jakim jest akt mianowania.

Uczestnicząc w poszczególnych etapach tego postępowania[39], potwierdza swoją gotowość do nawiązania stosunku służbowego. Przyjęcie rozkazu personalnego, w związku ze wstąpieniem do służby, jest również traktowane jako deklaracja gotowości do dobrowolnego pełnienia służby i zgoda na dobrowolne poddanie się reżimowi wynikającemu z istoty tego stosunku. Przystępując do wykonywania rozkazów i poleceń służbowych, a także realizując swoje obowiązki służbowe, funkcjonariusz konkludentnie (w sposób dorozumiany) potwierdza dobrowolne pełnienie służby, dając tym samym uprawnienie przełożonemu do egzekwowania władztwa wynikającego z tej więzi prawnej. Warto w tym miejscu przytoczyć stanowisko ugruntowane w doktrynie, zgodnie z którym: (…) *ponieważ jednak akt ten* (nawiązania stosunku służbowego – przyp. aut.) *poprzedzony musi być dobrowolnym zgłoszeniem się kandydata do służby, a następnie poparty przystąpieniem do wykonywania czynności służbowych* [,] *uważa się, że wola kandydata stanowi – równorzędną z wolą organu mianującego – przesłankę powstania stosunku służbowego*[40]. Mimo że to zdanie zostało wypowiedziane w kontekście mianowania funkcjonariusza Policji, tezę w nim zawartą można *per analogiam* odnieść do nawiązania stosunku służbowego funkcjonariuszy wszystkich służb, w tym do funkcjonariuszy ABW oraz AW, których podstawą zatrudnienia jest mianowanie.

Jest jednak niezbędne poczynienie jednego zastrzeżenia. Oświadczenie kandydata jest wiążące wyłącznie dla organu, w zakresie, w jakim kandydat dobrowolnie zgłasza gotowość do podjęcia i pełnienia służby. Jest to warunek konieczny, umożliwiający organowi nawiązanie z taką osobą stosunku służbowego. Nie może ona jednak dokonywać zastrzeżeń w złożonym oświadczeniu, zwłaszcza odnoszących się sposobu czy terminu zawarcia z nią stosunku służbowego, a także warunków pełnienia służby. Oświadczenie złożone przez kandydata musi być bezwarunkowe. Wszelkie dodatkowe

[39] Szczególnie w rozmowie kwalifikacyjnej mającej na celu ustalenie przydatności kandydata do służby w ABW albo AW, motywacji do jej podjęcia oraz poznania jego cech osobowych, na podstawie § 5 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 29 listopada 2002 r. w sprawie wzoru kwestionariusza osobowego oraz szczegółowych zasad i trybu przeprowadzania postępowania kwalifikacyjnego wobec kandydatów do służby w Agencji Bezpieczeństwa Wewnętrznego* (t.j.: DzU z 2014 r. poz. 61), a także na podstawie § 5 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 24 kwietnia 2003 r. w sprawie wzoru kwestionariusza osobowego oraz szczegółowych zasad i trybu przeprowadzania postępowania kwalifikacyjnego wobec kandydatów do służby w Agencji Wywiadu* (t.j.: DzU z 2014 r. poz. 445). W trakcie takiej rozmowy kandydat do służby w ABW albo AW powinien złożyć wyraźne oświadczenie o gotowości do podjęcia tej służby. Jest to niezbędny element mający na celu ustalenie jego przydatności do jej pełnienia. Byłoby jednak zasadne, aby kandydat składał odrębne oświadczenie, w którym zgłaszałby dobrowolnie gotowość do podjęcia służby w ABW albo AW. Wzorem mogłoby być rozwiązanie, jakie zostało przyjęte w odniesieniu do kandydatów do służby w Policji. W treści kwestionariusza osobowego, w części B, zawarto „Oświadczenie kandydata do służby", w tym punkt 10 o treści: „(…) jestem świadomy (-ma), że Policja to formacja uzbrojona, o szczególnym reżimie dyscypliny służbowej i że jako funkcjonariusz Policji mogę być w każdym czasie oddelegowany (-na) do pełnienia służby w innej jednostce organizacyjnej Policji". Zob. *Rozporządzenie Ministra Spraw Wewnętrznych z dnia 18 kwietnia 2012 r., w sprawie postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie do służby w Policji* (DzU z 2012 r. poz. 432, ze zm.).

[40] T. Hanausek i in., *Prawo policyjne. Komentarz*, t. 1, Katowice 1992, s. 69.

zastrzeżenia kandydata nie są wiążące dla organu. Wydaje się zasadne, aby kandydat do służby otrzymał informacje (np. w trakcie trwania rozmowy kwalifikacyjnej) o tym, że dobrowolne zgłoszenie się do służby musi mieć charakter bezwarunkowy. W innym przypadku treść tego oświadczenia może budzić wątpliwości, które powinny być usunięte jeszcze przed nawiązaniem stosunku służbowego. Tylko organ może jednostronnie kształtować jego treść, określać parametry, a także zakres praw i obowiązków przyszłego funkcjonariusza. Dokonuje tego na podstawie przepisów pragmatyki służbowej, tj. ustawy o ABW oraz AW, i aktów do niej wykonawczych. Kandydat może na te warunki przystać w całości, przyjmując rozkaz personalny o mianowaniu w związku z przyjęciem do służby w ABW lub AW, albo je odrzucić. Nie ma znaczenia, czy kandydat odmówił przyjęcia rozkazu personalnego o mianowaniu, gdyż nie chciał nawiązać stosunku służbowego, czy też zgłosił zastrzeżenia co do kształtu tej więzi prawnej albo do poszczególnych warunków, na jakich ta więź ma funkcjonować. W obu rozważanych przypadkach zainicjowanie stosunku służbowego jest niemożliwe, z uwagi na wystąpienie przesłanki negatywnej, jaką jest brak bezwarunkowego i dobrowolnego zgłoszenia się kandydata do służby.

Zmiana stanowiska kandydata do służby co do dobrowolnej gotowości jej podjęcia powoduje wyłącznie ten skutek, że organ nie może nawiązać z nim tej więzi prawnej. Nie oznacza to jednak konieczności wydania rozkazu personalnego o odmowie nawiązania stosunku służbowego z kandydatem, o nienawiązaniu tego stosunku, a także o odstąpieniu od jego nawiązania, mimo spełnienia przez niego ustawowych wymogów do pełnienia służby, potwierdzonych w toku postępowania kwalifikacyjnego. Takie działanie organu byłoby równoznaczne z wydaniem decyzji niemającej podstawy prawnej. Rozkaz personalny (decyzja administracyjna), w powyższym zakresie, podlegałby stwierdzeniu o nieważności na podstawie art. 156 § 1 pkt 2 kpa.

Nawiązanie stosunku służbowego jest uprawnieniem organu (przełożonego, określonego w art. 51 ust. 1 uabwaw), nie zaś jego obowiązkiem[41]. Organ podejmuje jednak działanie wyłącznie w przypadku nawiązania stosunku służbowego. Odstąpienie nie wymaga takiej aktywności. Kandydat do służby nie ma także żadnych instrumentów prawnych, które pozwalałyby mu na wyegzekwowanie od organu dokonania czynności nawiązania z nim stosunku służbowego. Skoro przepisy prawa przewidują wyłącznie uprawnienie organu w zakresie możliwości nawiązania stosunku służbowego, to nie

[41] Zob. § 8 ust. 1 rozporządzenia PRM w sprawie wzoru kwestionariusza osobowego oraz szczegółowych zasad i trybu przeprowadzania postępowania kwalifikacyjnego wobec kandydatów do służby w Agencji Bezpieczeństwa Wewnętrznego, w brzmieniu: „Kandydata, wobec którego przeprowadzone postępowanie kwalifikacyjne zakończyło się pozytywną oceną predyspozycji do służby w Agencji Bezpieczeństwa Wewnętrznego, zawiadamia się o możliwości przyjęcia do służby w Agencji Bezpieczeństwa Wewnętrznego", a także § 10 pkt 1 rozporządzenia PRM w sprawie wzoru kwestionariusza osobowego oraz szczegółowych zasad i trybu przeprowadzania postępowania kwalifikacyjnego wobec kandydatów do służby w Agencji Wywiadu, w brzmieniu: „Kandydata, wobec którego przeprowadzone postępowanie kwalifikacyjne zakończyło się: 1) pozytywną oceną predyspozycji do służby w AW i którego zamierza się przyjąć do służby w AW – zawiadamia się o możliwości przyjęcia do służby w AW".

istnieje korelujące z tym uprawnieniem prawo jednostki do żądania od organu jego nawiązania. Kandydat do służby nie może mieć takiego roszczenia. Wobec tego nie istnieje też prawna ochrona tej sfery, brakuje bowiem uprawnienia po stronie kandydata do służby, na którą można rozciągnąć tę sferę.

Jak już wspomniano, nawiązanie stosunku służbowego z funkcjonariuszem ABW albo AW wymaga podjęcia dwóch czynności[42]:

- dobrowolnego zgłoszenia się do służby przez kandydata,
- przyjęcia aktu mianowania (rozkazu personalnego o mianowaniu).

Istotne jest to, że te czynności muszą wystąpić we wskazanej wyżej sekwencji. Najpierw kandydat musi wyrazić gotowość dobrowolnego podjęcia służby i dopiero w następstwie tego oświadczenia organ administracyjny (po spełnieniu przez kandydata wszystkich ustawowych wymogów, potwierdzonych prowadzonym wobec niego postępowaniem kwalifikacyjnym, zakończonym pozytywnym wynikiem) może sporządzić rozkaz personalny o mianowaniu.

Organ administracyjny nie może zmuszać żadnej osoby do pełnienia służby nie tylko w ABW czy AW, lecz także w każdej innej formacji zmilitaryzowanej. Byłoby niedopuszczalne narzucanie obowiązku przyjęcia aktu mianowania przez osobę, która nie zgłaszała zainteresowania daną służbą. Nie oznacza to jednak, że formacja nie może podejmować czynności związanych z poszukiwaniem odpowiednich kandydatów do tych służb (z odpowiednimi kwalifikacjami czy predyspozycjami). Działania w tym zakresie nie stanowią zaprzeczenia zasady dobrowolności służby. Ustalenie, że dana osoba ma wszystkie predyspozycje i kwalifikacje pożądane w służbie w ABW czy AW, nadal wymaga jej zgody. Nie można werbować osoby wbrew jej woli, a następnie przymusowo wcielać do służby. Formalne bądź nieformalne działania, mające na celu pozyskanie danej osoby jako kandydata do służby, mogą być prowadzone wyłącznie do chwili złożenia przez nią wyraźnego oświadczenia o zainteresowaniu bądź braku zainteresowania służbą w ABW czy AW. Wyrażenie zgody umożliwia zainicjowanie procesu rekrutacji do służby i weryfikację przymiotów kandydata w chwili spełnienia przez niego ustawowych przesłanek. Zarówno brak takiej zgody, jak i zmiana uprzednio złożonej deklaracji o gotowości wstąpienia do służby powodują konieczność zaniechania dalszych czynności zmierzających do nawiązania stosunku służbowego.

Skoro wykazano wcześniej, że stosunek służbowy z mianowania ma charakter *stricte* administracyjno-prawny, to należy ustalić, czym w istocie jest mianowanie. M i a n o w a n i e to szczególny rodzaj stosunku wiążący się ze wzmożoną dyspozycyjnością funkcjonariusza w służbie co do czasu, miejsca i rodzaju wykonywanych czynności, zwiększonym stopniem podporządkowania przełożonemu (i to zarówno bezpośredniemu przełożonemu, jak i pozostałym przełożonym) oraz charakteryzującego się trwałością powstałego stosunku, a także zaostrzoną odpowiedzialnością dyscyplinarną

[42] B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017 (komentarz do art. 48 uabwaw).

i porządkową[43]. Dyspozycyjność jest jednym z najbardziej charakterystycznych cech tego stosunku[44]. Jak każdy stosunek służbowy ustanowiony dla funkcjonariuszy formacji zmilitaryzowanych oraz paramilitarnych ma on być zdatnym (skutecznym) instrumentem do osiągnięcia określonego celu. Oznacza to, że ma stwarzać jak najlepsze warunki do realizacji ustawowych zadań przewidzianych dla danej organizacji. Te z kolei są wskazane w art. 1 i 2 uabwaw jako cele wytyczone dla obu formacji. Szczegółowe zadania są wyliczone w treści art. 5 i 6 uabwaw. Jeżeli stosunek nie może być wykorzystany do realizacji tych celów, konieczne jest podjęcie czynności służących jego rozwiązaniu. Oczywiście musi to nastąpić z uwzględnieniem jednej z podstaw umożliwiających zwolnienie funkcjonariusza ze służby, wskazanych w art. 54 ust. 3 lub art. 60 ust. 1–3 uabwaw. Analiza poszczególnych podstaw zwolnienia potwierdza jednak powyższą tezę. Każda z nich bowiem wskazuje na okoliczności, które albo utrudniają, albo uniemożliwiają realizację misji przewidzianej dla tych formacji.

Najbardziej dobitnym tego przykładem jest przesłanka zawarta w art. 60 ust. 2 pkt 5 uabwaw umożliwiająca zwolnienie ze służby ze względu na „ważny interes służby". Ustawodawca wskazał wprost na dobro, któremu dał prymat. W przypadku kolizji między interesem jednostki, zorientowanej na zatrudnienie i realizację zawodową, a „ważnym interesem służby", którego priorytetem jest sprawne i prawidłowe funkcjonowanie tej formacji, możliwe jest zwolnienie jednostki. Odmienne stanowisko nie wytrzymuje krytyki, sprowadziłoby bowiem instytucję zatrudnienia w ABW albo AW, a także w innych formacjach zmilitaryzowanych, do konstrukcji mającej charakter socjalny. Musiałaby ona zostać zorientowana na zatrudnienie członków tej organizacji po to, aby ci mogli ewentualnie realizować przydzielone im zadania, a tym samym zadania wytyczone danej formacji. W rzeczywistości odpowiedzialną za realizację zadań jest konkretna służba, a ta działa za pośrednictwem swoich członków będących elementami jej struktury organizacyjnej. Jak już wspomniano, instrumentem umożliwiającym zapewnienie odpowiedniego zasobu kadrowego dla konkretnej służby jest stosunek służbowy. Jego konstrukcja gwarantuje z jednej strony trwałość powstałej więzi prawnej (zwolnienie jest możliwe wyłącznie na podstawie przesłanek

[43] P. Gacek, *Nawiązanie stosunku służbowego z funkcjonariuszem Policji*, „Administracja. Teoria. Dydaktyka. Praktyka" 2011, nr 2, s. 75. Porównaj także z elementami charakterystycznymi dla stosunków służbowych wskazanych przez Przemysława Szustakiewicza: „Z treści przepisów pragmatycznych wynika, że stosunek służbowy osób pełniących służbę w omawianych formacjach zmilitaryzowanych posiada 4 elementy odróżniające go od innych stosunków prawnych: 1) obowiązek poświęcenia; 2) dyspozycyjność i obowiązek podporządkowania; 3) szczególne uprawnienia związane z wykonywaniem służby; 4) administracyjnoprawne uregulowanie stosunku prawnego funkcjonariusza lub żołnierza". Zob. *Stosunek służbowy w formacjach mundurowych*, W. Maciejko, P. Szustakiewicz (red.), 2016, Legalis/el; także A. Korcz-Maciejko, *Prawny charakter rozkazu personalnego*…, s. 144 i nast.

[44] „Istotą służby w ABW jest dyspozycyjność funkcjonariuszy, co oznacza, że zmianę miejsca, a czasem też i warunków służby funkcjonariuszy, należy oceniać według kryteriów zobiektywizowanych, uwzględniających skuteczność działania jednostki, a nie według osobistych odczuć funkcjonariusza", za: wyrok WSA w Warszawie z 17 IV 2012 r., II SA/Wa 311/12, Legalis nr 498569.

enumeratywnie wskazanych w art. 54 ust. 3 oraz art. 60 ust. 1–3 uabwaw), z drugiej zaś zobowiązuje do ciągłej dyspozycyjności co do czasu, miejsca i rodzaju wykonywanych czynności. Każdy funkcjonariusz realizuje swoje zadania na podstawie przydzielonego zakresu obowiązków właściwych dla zajmowanego stanowiska służbowego. Nie oznacza to, że nie ma on obowiązku podejmowania innych zadań, które są podyktowane potrzebami służby, wynikłymi *ad hoc* ze specyfiki funkcjonowania danej komórki czy jednostki organizacyjnej, a także ze zmieniających się okoliczności (w tym szczególnie z pojawiających się lub eskalujących zjawisk godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny bądź zewnętrznych, godzących w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium Rzeczpospolitej Polskiej). Jak wynika wprost z art. 51 ust. 1 uabwaw[45], czas służby funkcjonariusza jest określany wymiarem jego obowiązków[46]. Nie jest to więc czas wykonywania przez pracownika pracy czy pozostawania w dyspozycji pracodawcy, tak jak to ma miejsce na gruncie prawa pracy[47]. Wyeksponowanie tego elementu nie jest przypadkowe. Świadczy ono o celowym działaniu ustawodawcy wskazującego na te elementy stosunku służbowego, które są najbardziej dla niego charakterystyczne. Służba nie jest zwykłą pracą najemną. Funkcjonariusz nie jest pracownikiem, nie świadczy pracy, ale pełni służbę, nie obowiązują go także (co do zasady) regulacje prawa pracy. Dobro służby wymaga sprawnego wykonywania zadań służbowych, a co za tym idzie – prawidłowej realizacji ustawowych zadań przewidzianych dla tej formacji. Te wartości muszą mieć odzwierciedlenie w konstrukcji stosunku służbowego, który ma być instrumentem przyczyniającym się do wypełniania misji tych organizacji. Stąd też konieczność stworzenia właściwego środowiska, w którym usytuowany jest funkcjonariusz. Jest nim właśnie stosunek służbowy.

Jak zauważono w doktrynie[48], mianowanie wywołuje dwa skutki: w sferze wewnętrznej (służbowej) oraz w sferze zewnętrznej. Pierwszym jest nabycie przez osobę fizyczną przymiotu funkcjonariusza jako podmiotu usytuowanego w strukturze organizacyjnej tej formacji, mającej charakter zmilitaryzowany i zhierarchizowany. Funkcjonariusz nabywa tym samym określone uprawnienia i obowiązki przysługujące jedynie funkcjonariuszowi. Skutkuje to koniecznością podporządkowania się określonej

[45] Szczegółowe kwestie związane z czasem służby w ABW i AW określają: *Rozporządzenie Prezesa Rady Ministrów z dnia 3 października 2003 r. w sprawie rozkładu czasu służby funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* (t.j.: DzU z 2013 poz. 935) oraz *Rozporządzenie Prezesa Rady Ministrów z dnia 24 kwietnia 2003 r. w sprawie rozkładu czasu służby funkcjonariuszy Agencji Wywiadu* (DzU z 2003 r. nr 86 poz. 793, ze zm.).

[46] „Niedopuszczalna jest zatem sytuacja, w której funkcjonariusz przestaje wykonywać obowiązki, ponieważ uznaje, że wyczerpał się czas jego służby", za: B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego*... (komentarz do art. 51 uabwaw).

[47] Na temat różnicy między czasem pracy a czasem służby zob. P. Gacek, *Czas służby a czas pracy – wybrane aspekty. Przyczynek do dyskusji*, „Policja. Kwartalnik Kadry Kierowniczej Policji" 2014, nr 2, s. 41 i nast.

[48] B. Opaliński, M. Rogalski, P. Szustakiewicz, *Ustawa o Agencji Bezpieczeństwa Wewnętrznego*… (komentarz do art. 48 uabwaw).

dyscyplinie służbowej. Powoduje także powstanie więzi służbowej, będącej sformalizowanym typem relacji, jaka zostaje zainicjowana pomiędzy poszczególnymi podmiotami tej organizacji. Funkcjonariusze stają się podwładnymi swoich przełożonych. Oczywiście, stopień podporządkowania i dyspozycyjności jest różny w zależności od stanowiska służbowego zajmowanego przez poszczególnych funkcjonariuszy. Podwładni są zobowiązani do większego podporządkowania się swoim przełożonym oraz do wykonywania wydawanych im poleceń i rozkazów. Przełożeni z kolei są zobowiązani do większej dyspozycyjności, w porównaniu z podwładnymi, którymi kierują. Wynika to z konieczności permanentnego nadzorowania i koordynowania działań zespołów funkcjonariuszy wykonujących wytyczone im zadania służbowe. Ponadto kontakt pomiędzy podwładnymi i poszczególnymi przełożonymi odbywa się za pośrednictwem kanału komunikacyjnego, jakim jest droga służbowa, specjalnie stworzonego na te potrzeby.

Osoba fizyczna, która staje się funkcjonariuszem, uzyskuje określone uprawnienia funkcjonariusza publicznego. Wiążą się one z możliwością podejmowania czynności wobec osób pozostających poza strukturą organizacyjną tej formacji. Funkcjonariusz otrzymuje tym samym uprawnienia do ingerowania w sferę praw i wolności szerokiego grona osób, w tym obywateli Rzeczpospolitej Polskiej. Państwo wyposaża go także w swoistego rodzaju *imperium*, pozwalające na występowanie w imieniu tego państwa, w relacjach z innymi osobami (w tym z obywatelami tego państwa), reprezentowania tego państwa i jego interesów, a także do stosowania (jeżeli wymagają tego okoliczności, w przypadkach przewidzianych przez przepisy prawa) środków represji, które mają na celu przymusowe wykonanie określonych czynności przez tę osobę albo uzyskanie pożądanego stanu rzeczy, zgodnego z wolą tego organu. Uprawnienia funkcjonariusza korelują z kolei z obowiązkami osób znajdujących się poza tymi służbami, które muszą podporządkować się poleceniom wydawanym przez funkcjonariuszy, a także muszą tolerować ewentualną ingerencję w ich prawa i wolności zagwarantowane konstytucyjnie.

Zakończenie

Nie sposób odnieść się do wszystkich zagadnień związanych z tym tematem, z uwagi na obszerność przedmiotowej problematyki. Celem tego opracowania było wyłącznie ukazanie konstrukcji prawnej „mianowania" jako stosunku administracyjno-prawnego oraz wskazanie jego najbardziej charakterystycznych cech. Kontekstem rozważań zaś była czynność nawiązania stosunku służbowego z funkcjonariuszami ABW albo AW.

Ustawodawca, mimo że posługuje się jednym pojęciem („mianowanie"), odnosi je do różnych konstrukcji prawnych, zamieszczonych w regulacjach usytuowanych w odrębnych gałęziach prawa. Niezbędne zatem było omówienie mianowania, o którym mowa w art. 76 kp, oraz mianowania, o którym mowa w art. 48 uabwaw. Wskazano podobieństwa, a także zasadnicze różnice, jakie zachodzą między tymi odmiennymi

konstrukcjami prawnymi. Najbardziej znamienne jest to, że mianowanie wynikające z pragmatyki służbowej, dotyczącej statusu funkcjonariuszy ABW oraz AW (ale także innych funkcjonariuszy służb mundurowych), powoduje powstanie więzi prawnej mającej charakter *stricte* administracyjny, w przeciwieństwie do mianowania wynikającego z art. 76 kp, które wywołuje skutek zarówno w sferze prawa administracyjnego, jak i prawa pracy (nawiązanie stosunku pracy). Zainicjowany stosunek pracy w wyniku aktu mianowania (nominacji) stanowi linię demarkacyjną oddzielającą te dwie tożsame z nazwy, lecz w istocie różne, instytucje prawne. Konsekwencją tego jest to, że reżim prawa pracy nie ma, co do zasady, zastosowania do stosunków prawnych regulujących status członków organizacji militarnych lub paramilitarnych, w tym ABW oraz AW, chyba że przepisy szczególne pragmatyki zezwalają na subsydiarne stosowanie norm prawa należących do innych gałęzi prawa, w tym prawa pracy.

Postulowano również *de lege ferenda* zmianę i ujednolicenie obowiązującej siatki pojęciowej, stosowanej zarówno przez prawodawcę w tekstach aktów prawnych, jak i w nauce prawa. Jest konieczne wyraźne wskazanie, że ze względu na specyfikę stosunku służbowego, będącego niepracowniczym stosunkiem zatrudnienia, pojęcia właściwe prawu pracy nie mogą mieć zastosowania do definiowania pojęć stanowiących elementy składowe tego rodzaju konstrukcji prawnej. Należy rozdzielić mianowanie, o którym mowa w prawie pracy, od mianowania funkcjonariuszy formacji zmilitaryzowanych i paramilitarnych. To pierwsze nosiłoby nazwę „mianowanie pracownicze", drugie natomiast byłoby „mianowaniem służbowym" lub po prostu „mianowaniem". W dalszej kolejności należałoby doprecyzować pojęcia odnoszące się do obu typów stosunków prawnych przez wskazanie ich istotnych cech. Mianowanie, o którym mowa w art. 76 kp, byłoby określane jako „pracowniczy stosunek służbowy z mianowania" albo „stosunek służbowy typu pracowniczego z mianowania", a w przypadku mianowania funkcjonariuszy poszczególnych służb byłoby zasadne stosowanie pojęcia „stosunek służbowy z mianowania". Istotne jest także wyodrębnienie pojęć immanentnie związanych z poszczególnymi stosunkami prawnymi i wyraźne przeciwstawienie im następujących pojęć: „pracodawca", „pracownik", „stosunek pracy", „wynagrodzenie" z takimi pojęciami, jak: „podmiot zatrudniający", „funkcjonariusz" lub „osoba zatrudniona w formacji zmilitaryzowanej", „służba" oraz „uposażenie". Te pojęcia nie są bowiem tożsame. Zamienne stosowanie ich do przeciwstawnych konstrukcji prawnych zaciera wyraźną różnicę między oboma typami stosunków prawnych. Konsekwentnie należałoby również oddzielić (na gruncie pojęciowym) akty regulujące status pracowników zatrudnionych na podstawie mianowania od aktów dotyczących funkcjonariuszy zatrudnionych na podstawie mianowania. Pierwsze nosiłyby nazwę „pragmatyka pracownicza", drugie – „pragmatyka służbowa".

Bibliografia

Chałfina R.O., *Ogólna nauka o stosunku prawnym*, Warszawa 1979, PWN.

Chauvin T., Stawecki T., Winczorek P., *Wstęp do prawoznawstwa*, Warszawa 2009, C.H. Beck.

Florek L., Zieliński T., *Prawo pracy*, wyd. 5, Warszawa 2003, C.H. Beck.

Gacek P., *Czas służby a czas pracy – wybrane aspekty. Przyczynek do dyskusji*, „Policja. Kwartalnik Kadry Kierowniczej Policji" 2014, nr 2, s. 41–53.

Gacek P., *Nawiązanie stosunku służbowego z funkcjonariuszem Policji*, „Administracja. Teoria. Dydaktyka. Praktyka" 2011, nr 2, s. 68–93.

Gacek P., *Wymogi formalne niezbędne do pełnienia służby w Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu – wybrane aspekty*, „Przegląd Bezpieczeństwa Wewnętrznego" 2017, nr 17, s. 56–86.

Giedrewicz-Niewińska A., komentarz do art. 76 kp, w: *Kodeks pracy. Komentarz*, K. Walczak (red.), Warszawa 2017, Legalis.

Hanausek T., *Ustawa o Policji. Komentarz*, Kraków 1996, Zakamycze.

Hanausek T. i in., *Prawo Policyjne. Komentarz*, t. 1, Katowice 1992, Polbod.

Jaśkiewicz W., *Stosunki służbowe w administracji*, Warszawa–Poznań 1969, PWN.

Kacprzak J., *Stosunki służbowe w formacjach zmilitaryzowanych – charakter prawny, ochrona sądowa*, „Przegląd Policyjny" 1994, nr 1, s. 97–111.

Kodeks pracy. Komentarz, W. Muszalski (red.), Warszawa 2017, Legalis.

Kodeks pracy. Komentarz, A. Sobczyk (red.), Warszawa 2017, Legalis.

Kodeks pracy. Komentarz, Z. Salwa (red.), Warszawa 2000, Wydawnictwo Prawnicze.

Korcz-Maciejko A., *Prawny charakter rozkazu personalnego*, „Administracja. Teoria. Dydaktyka. Praktyka" 2013, nr 3, s. 134–155.

Kuczyński T., Mazurczak-Jasińska E., Stelina J., *Stosunek służbowy*, seria: *System prawa administracyjnego*, t. 11, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2011, C.H. Beck, Instytut Nauk Prawnych.

Leksykon policyjny, W. Pływaczewski, G. Kędzierska (red.), Szczytno 2001, WSPol.

Leoński Z., *Zarys prawa administracyjnego*, Warszawa 2004, LexisNexis.

Liwo M., *Status służb mundurowych i funkcjonariuszy w nich zatrudnionych*, wyd. 1, Warszawa 2013, LexisNexis.

Łaszczyca G., Martsz C., Matan A., *Postępowanie administracyjne ogólne*, Warszawa 2003, C.H. Beck.

Łętowski J., *Polecenie służbowe w administracji*, Warszawa 1974, Wydawnictwo Prawnicze.

Łętowski J., *Prawo administracyjne, Zagadnienia podstawowe*, Warszawa 1990, PWN.

Maciejko W., Korcz-Maciejko A., *Postępowanie w sprawach osobowych w Policji*, Wrocław 2010, Gaskor.

Muszalski W., *Prawo socjalne*, Warszawa 1996, Wydawnictwo Naukowe PWN.

Muszalski W. i in., *Kodeks pracy z komentarzem*, Gdańsk 1996, ODDK.

Ochendowski E., *Prawo administracyjne. Część ogólna*, wyd. 8, Toruń 2009, TNOiK „Dom Organizatora".

Opaliński B., Rogalski M., Szustakiewicz P., *Ustawa o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Komentarz*, Warszawa 2017, Legalis.

Piątkowski J., Kolasiński M.K., Kolasiński A., *Stosunki pracy w administracji publicznej (na tle prawa wspólnotowego)*, Toruń 2008, TNOiK „Dom Organizatora".

Prawo administracyjne, J. Boć (red.), Wrocław 2001, Kolonia Limited.

Rybicki Z., Piątek S., *Zarys prawa administracyjnego i nauki administracji*, Warszawa 1984, PWN.

Starościak J., *Administracja. Zagadnienia teorii i praktyki*, Warszawa 1974, Wydawnictwo Prawnicze.

Stosunek służbowy w formacjach mundurowych, W. Maciejko, P. Szustakiewicz (red.), 2016, Legalis/el.

Świątkowski A.M., *Kodeks pracy. Komentarz*, wyd. 2, Warszawa 2006, C.H. Beck.

Wielka encyklopedia prawa, B. Hołyst (red.), Warszawa 2005, Prawo i Praktyka Gospodarcza.

Wojtunik P., *Pojęcie, źródła i przedmiot stosunków służbowych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8, s. 202–217.

Zarys prawa, J. Kuciński (red.), Warszawa 2010, LexisNexis.

Zieliński T., *Stosunek prawa pracy do prawa administracyjnego*, Warszawa 1977, PWN.

Akty prawne

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j.: DzU z 2020 r. poz. 27).

Ustawa z dnia 26 czerwca 1974 r. – Kodeks pracy (t.j.: DzU z 2019 r. poz. 1040, ze zm.).

Ustawa z dnia 14 czerwca 1960 r. – Kodeks postępowania administracyjnego (t.j.: DzU z 2018 r. poz. 2096, ze zm.).

Rozporządzenie Ministra Spraw Wewnętrznych z dnia 18 kwietnia 2012 r., w sprawie postępowania kwalifikacyjnego w stosunku do kandydatów ubiegających się o przyjęcie do służby w Policji (DzU z 2012 r. poz. 432, ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 28 listopada 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Wywiadu (DzU z 2003 r. nr 210 poz. 2039, ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 3 października 2003 r. w sprawie rozkładu czasu służby funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego (t.j.: DzU z 2013 r. poz. 935).

Rozporządzenie Prezesa Rady Ministrów z dnia 2 lipca 2003 r. w sprawie przebiegu służby funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego (t.j.: DzU z 2013 r. poz. 862).

Rozporządzenie Prezesa Rady Ministrów z dnia 24 kwietnia 2003 r., w sprawie rozkładu czasu służby funkcjonariuszy Agencji Wywiadu (DzU z 2003 r. nr 86 poz. 793, ze zm.).

Rozporządzenie Prezesa Rady Ministrów z dnia 24 kwietnia 2003 r. w sprawie wzoru kwestionariusza osobowego oraz szczegółowych zasad i trybu przeprowadzania postępowania kwalifikacyjnego wobec kandydatów do służby w Agencji Wywiadu (t.j.: DzU z 2014 r. poz. 445).

Rozporządzenie Prezesa Rady Ministrów z dnia 29 listopada 2002 r. w sprawie wzoru kwestionariusza osobowego oraz szczegółowych zasad i trybu przeprowadzania postępowania kwalifikacyjnego wobec kandydatów do służby w Agencji Bezpieczeństwa Wewnętrznego (t.j.: DzU z 2014 r. poz. 61).

Uchwała Sądu Najwyższego, Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z 18 III 2008 r., II PZP 3/08, Legalis nr 95381.

Orzecznictwo

Wyrok Trybunału Konstytucyjnego z 29 VI 2006 r., P 30/05, OTK – A z 2006 r., nr 6, poz. 70, DzU z 2006 r. nr 122 poz. 852.

Wyrok Sądu Najwyższego, Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych, z 7 IV 2009 r., I PK 218/08, Legalis nr 158199.

Wyrok Sądu Najwyższego – Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z 23 XI 2004 r., I PK 35/04, Legalis nr 68713.

Wyrok Sądu Najwyższego – Izba Administracyjna, Pracy i Ubezpieczeń Społecznych z 18 VI 1998 r., I PKN 167/98, Legalis nr 43387.

Wyrok Sądu Najwyższego – Izba Administracyjna, Pracy i Ubezpieczeń Społecznych z 10 IV 1997 r., I PKN 57/96, Legalis nr 30942.

Postanowienie Sądu Najwyższego, Izba Pracy, Ubezpieczeń Społecznych i Spraw Publicznych z 19 II 2014 r., I PK 264/13, Legalis nr 1169341.

Wyrok Naczelnego Sądu Administracyjnego z 30 VI 2010 r., I OSK 78/10, Legalis nr 293195.

Wyrok Naczelnego Sądu Administracyjnego z 18 XII 2008 r., I OSK 12/08, Legalis nr 186470.

Wyrok Naczelnego Sądu Administracyjnego z 28 X 2008 r., I OSK 1721/07, Legalis nr 207868.

Wyrok Naczelnego Sądu Administracyjnego z 3 X 2006 r., I OSK 210/06, Legalis nr 606379.

Wyrok Naczelnego Sądu Administracyjnego z 24 IX 1991 r., II SA 746/91, Legalis nr 36962.

Wyrok Naczelnego Sądu Administracyjnego z 5 VI 1991 r., II SA 35/91, ONSA z 1991 r., nr 3, poz. 64.

Postanowienie Naczelnego Sądu Administracyjnego z 15 IV 1991 r., II SA 258/91, Legalis nr 143575.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 17 IV 2012 r., II SA/Wa 311/12, Legalis nr 498569.

Wyrok Wojewódzkiego Sądu Administracyjnego w Poznaniu z 5 II 2009 r., IV SA/Po 430/08, Legalis nr 170824.

Wyrok Wojewódzkiego Sądu Administracyjnego w Warszawie z 10 XII 2007 r., II SA/Wa 1620/07, Legalis nr 121289.

Wyrok Wojewódzkiego Sądu Administracyjnego w Białymstoku z 23 II 2006 r., II SA/Bk 943/05, Legalis nr 826774.

Abstrakt

Głównym celem artykułu było wprowadzenie do zagadnienia dotyczącego prawnego charakteru mianowania, o którym mowa w art. 48 *Ustawy dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, w kontekście nawiązania tego stosunku. Artykuł poświęcono analizie prawno-porównawczej stosunku służbowego z mianowania oraz stosunku pracy z mianowania, co pozwoliło na wyraźne rozgraniczenie dwóch rodzajów stosunków prawnych. Elementem odróżniającym stosunek pracy z mianowania od stosunku służbowego z mianowania jest to, że w pierwszym przypadku oprócz stosunku administracyjnego musi współistnieć

stosunek pracy. W drugim – stosunek pracy nie istnieje. W przypadku stosunku pracy z mianowania jej stronami są odpowiednio pracodawca i pracownik, podczas gdy tych konstrukcji nie da się zastosować *per analogiam* do stosunku służbowego. Stronami tego rodzaju stosunku zatrudnienia mogą być jedynie: funkcjonariusze Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu lub innych formacji zmilitaryzowanych oraz podmiot zatrudniający. Wskazanie tych elementów pozwoliło pokazać różnice między tymi dwiema konstrukcjami prawnymi. Postulowano, aby te dwie wyżej wymienione instytucje prawne zostały ponownie zdefiniowane przez prawodawcę. Nomenklatura stosowana dotychczas w doktrynie nie jest bowiem jednolita.

Słowa kluczowe: służba w ABW lub AW, zatrudnienie w ABW lub AW, mianowanie (nominacja), stosunek służbowy, stosunek administracyjny (stosunek administracyjno-prawny), funkcjonariusz, pragmatyka służbowa.

Abstract

The main research aim of this article was to introduce problems concerning legal character of nomination, based on the Article 48 Act of 24 May 2002 The Internal Security Agency and Foreign Intelligence Agency, in the context of establishing this service relationship. This article was devoted to a comparative analysis of legal service relationship have been proved with the nomination of the official employment relationship to the nomination which allowed a clear demarcation of the boundary existing between the two types of legal relations. An important element that distinguishes employment business relationship with the nomination and the service relationship with the nomination is that in the first case next to the administrative relationship employment relationship must coexist. In the latter case the employment relationship does not exist. On the other hand, in the case of business relationship with the nomination its sides are respectively the employer and the employee, while these structures cannot be applied *per analogiam* to the service relationship with the nomination. Only officer of the Internal Security Agency and the Foreign Intelligence Agency or other militarized formations and employing entity can be a party to the employment service relationship. Highlighting these elements inter alia allowed to show the differences between this two structures of law. It was postulated that the two above-mentioned legal institutions should be redefined by the legislator. The nomenclature used so far in the doctrine is not uniform in this respect.

Keywords: service in the Internal Security Agency and in the Foreign Intelligence Agency, employment in the Internal Security Agency and in the Foreign Intelligence Agency, nomination, service relationship, administrative relationship (administrative – legal relation), officer, service pragmatics.

Maciej A. Kędzierski

Współpraca Agencji Bezpieczeństwa Wewnętrznego z Generalnym Inspektorem Informacji Finansowej na podstawie przepisów nowej ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu

Nowa *Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[1] (dalej: nuop) weszła w życie 13 lipca 2018 r. Utrzymano w niej dotychczasowy model przeciwdziałania tym zjawiskom, który był oparty na działalności Generalnego Inspektora Informacji Finansowej (dalej: GIIF) oraz współdziałających z nim instytucji obowiązanych, jednostek współpracujących oraz zagranicznych jednostek analityki finansowej (dalej: ZJAF). Dokonano w nim jednak pewnych zmian w odniesieniu do modelu, który funkcjonował w ramach *Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*[2] (dalej: pppft).

Jedną z jednostek współpracujących z GIIF jest Agencja Bezpieczeństwa Wewnętrznego (dalej: ABW). To rozwiązanie logicznie wynika z zadań przypisanych zarówno GIIF, jak i ABW. Zadania polegające na przeciwdziałaniu praniu pieniędzy i finansowaniu terroryzmu oraz zwalczaniu tych negatywnych zjawisk (określane jako AML/CTF[3]) są realizowane na różnych szczeblach i przy wykorzystaniu wielu instrumentów prawnych. Zaliczamy do nich: czynności analityczne, informacyjne, kontrolne, operacyjno-rozpoznawcze i dochodzeniowo-śledcze. Nowa ustawa nie wyposażyła polskiej jednostki analityki finansowej (dalej: PJAF) w instrumenty o charakterze operacyjno-rozpoznawczym i dochodzeniowo-śledczym. Konsekwencją takiego stanu oraz uplasowania GIIF w strukturze organów państwowych (głównie tych, które działają w sferze bezpieczeństwa narodowego) jest potrzeba bezpośredniej współpracy pomiędzy Generalnym Inspektorem a podmiotami, które mają takie kompetencje. Należy również zauważyć, że w 2016 r. weszła do obrotu prawnego *Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[4], której zapisy, w tym także te zawarte w aktach wykonawczych, mają swoje przełożenie na funkcjonowanie GIIF i podejmowane

---

1 Tekst jednolity: DzU z 2019 r. poz. 1115, ze zm.

2 DzU z 2017 r. poz. 1049, ze zm.

3 Skróty od: *Anti-Money Laundering* oraz *Counter Terrorist Financing* (przyp. red.).

4 Tekst jednolity: DzU z 2019 r. poz. 796.

przez niego decyzje. Z tego powodu relacje między GIIF a ABW należy rozpatrywać znacznie szerzej niż tylko przez pryzmat nuop i ustawy kompetencyjnej ABW[5].

W nuop ABW jest wymieniona wielokrotnie oraz wskazana jako jednostka współpracująca (jako organ administracji rządowej, tj. szef ABW)[6]. Artykuł 10 nuop wymienia organy informacji finansowej, którymi są minister finansów oraz Generalny Inspektor w randze sekretarza stanu lub podsekretarza stanu w Ministerstwie Finansów. Zgodnie natomiast z treścią ust. 2 tego artykułu: *Generalnego Inspektora powołuje i odwołuje Prezes Rady Ministrów na wniosek ministra właściwego do spraw finansów publicznych po zasięgnięciu opinii ministra – członka Rady Ministrów właściwego do spraw koordynowania działalności służb specjalnych, jeżeli został wyznaczony przez Prezesa Rady Ministrów*. Tym samym jest możliwe, że koordynator ds. służb specjalnych wystąpi do szefa ABW z zapytaniem, czy nie ma przeciwwskazań do powołania wskazanego kandydata na stanowisko Generalnego Inspektora[7]. Zgodnie z art. 11 pkt 5 nuop może nim być osoba, która spełnia m.in. wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do tych o klauzuli „ściśle tajne". Jednym z zadań ABW, realizowanych w granicach właściwości Agencji, jest ochrona takich informacji, jak również pełnienie funkcji krajowej władzy bezpieczeństwa w sferze ochrony informacji niejawnych w stosunkach międzynarodowych (art. 5 ust. 1 pkt 3 ustawy o ABW oraz AW). W tym przypadku działania ABW będą polegały przede wszystkim na sprawdzeniu, czy kandydat na GIIF daje rękojmię zachowania tajemnicy. Jest to (…) *zdolność osoby do spełnienia ustawowych wymogów dla zapewnienia ochrony informacji niejawnych przed ich nieuprawnionym ujawnieniem, stwierdzona w wyniku przeprowadzenia postępowania sprawdzającego*[8]. Tego rodzaju postępowania nie przeprowadza się wobec członka Rady Ministrów (art. 34 ust. 10 pkt 5 uoin). Wśród organów informacji finansowej taki status ma tylko jeden z nich, tj. minister finansów jako organ naczelny informacji finansowej. Natomiast GIIF, który zgodnie z art. 10 ust. 3 nuop jest sekretarzem albo podsekretarzem stanu w urzędzie obsługującym ministra właściwego do spraw finansów publicznych, podlega – zgodnie z uoin – postępowaniu sprawdzającemu. Wynika to ze wspomnianej potrzeby posiadania przez niego uprawnienia dostępu do dokumentów opatrzonych klauzulą

[5] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (DzU z 2020 r. poz. 27).

[6] Jednostki współpracujące – pod tym pojęciem rozumie się organy administracji rządowej, organy jednostek samorządu terytorialnego oraz inne państwowe jednostki organizacyjne, a także Narodowy Bank Polski, Komisję Nadzoru Finansowego i Najwyższą Izbę Kontroli (art. 2 ust. 2 pkt 8 nuop).

[7] *Rozporządzenie Prezesa Rady Ministrów z dnia 13 grudnia 2017 r. w sprawie szczegółowego zakresu działania Ministra – Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych* (DzU z 2017 r. poz. 2332).

[8] Zgodnie z *Ustawą z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (t.j.: DzU z 2019 r. poz. 742), dalej: uoin.

„ściśle tajne". W przypadku wyłączenia GIIF z wykonywania zadań – jego zadania realizuje minister właściwy do spraw finansów publicznych (art. 15 ust. 3 pkt 1 nuop).

Kandydatem na stanowisko Generalnego Inspektora może być osoba pełniąca już wcześniej funkcję państwową, która jednocześnie spełnia wymogi bycia podmiotem z katalogu osób zajmujących ważne stanowiska polityczne (ang. *politically exposed persons*, PEP)[9]. Jest konieczne, aby instytucje obowiązane stosowały wobec takich osób wzmożone środki bezpieczeństwa finansowego (art. 43 ust. 1 w zw. z art. 46 nuop). Odbiorcą informacji, szczególnie o występowaniu PEP w konfiguracji negatywnej, tj. powiązania takiej osoby czy też członków jej rodziny bądź bliskich współpracowników z okolicznościami mogącymi wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, jest GIIF (art. 74 ust. 1 nuop). Skutkuje to specyficzną sytuacją, w której Generalny Inspektor ma wiedzę m.in. o zdarzeniach mogących wpłynąć na ocenę rękojmi zachowania tajemnicy przez kandydata na to stanowisko i może ją przekazać innym organom decyzyjnym (np. szefowi ABW) – zwłaszcza gdy zachodzi podejrzenie udziału PEP w procederze prania pieniędzy i finansowania terroryzmu. Jakkolwiek jednym z głównych celów stosowania środków bezpieczeństwa finansowego (w tym wzmożonych) jest ustalenie symptomów czy śladów zaangażowania klienta instytucji obowiązanej w tego rodzaju przestępczy proceder, to wnioski płynące z oceny zachowań takiej osoby mogą wskazywać również na inne niż wymienione rodzaje aktywności niezgodnych z prawem (np. podejrzenie udziału w dokonaniu przestępstw podatkowych, skarbowych – jako przestępstw pierwotnych wobec wskazanych). „Automatyczne" mianowanie kandydata na Generalnego Inspektora, tj. bez uzyskania wiedzy z zasobów GIIF oraz ustalenia, czy dostępne dane o zdarzeniach nie uniemożliwiają udzielenia rękojmi w zakresie dostępu do informacji ściśle tajnych, nie wydaje się zatem właściwe.

Postępowania sprawdzające mające na celu umożliwienie dostępu do informacji niejawnych są przeprowadzane także w stosunku do kierownictwa Departamentu Informacji Finansowej Ministerstwa Finansów (dalej: DIF MF) jako komórki organizacyjnej, o której mowa w art. 12 ust. 2 nuop, oraz pracowników tego departamentu. Należy mieć na uwadze, że niektóre działania w stosunku do tych podmiotów są podejmowane i realizowane z upoważnienia wydanego przez Generalnego Inspektora oraz ministra finansów. Może to dotyczyć także spraw związanych z obiegiem dokumentów niejawnych i zaznajamianiem się z nimi, jak również uczestnictwa kierownika komórki organizacyjnej, o której mowa w art. 12 ust. 2 nuop, w Komitecie Bezpieczeństwa Finansowego (dalej: KBF) w randze jego wiceprzewodniczącego (art. 20 ust. 1 pkt 2 nuop).

Generalny Inspektor przedstawia Prezesowi Rady Ministrów, za pośrednictwem ministra właściwego do spraw finansów publicznych, sprawozdanie roczne ze swojej działalności w terminie trzech miesięcy od zakończenia roku, za który jest ono składane (art. 14 nuop). Przy jego sporządzaniu GIIF współpracuje z ABW w zakresie

[9] Katalog takich osób został określony w art. 2 ust. 2 pkt 11 nuop.

sporządzenia lub weryfikacji dokumentów dotyczących relacji pomiędzy GIIF i ABW oraz działalności samej ABW w obszarze AML/CTF. Weryfikacja obejmuje między innymi potwierdzenie liczby informacji przekazanych przez ABW w trybie przewidzianym w nuop czy też danych statystycznych odnoszących się do tych informacji. Dane, o których mowa w art. 14 ust. 2 pkt 11 nuop, szef ABW przekazuje Generalnemu Inspektorowi w ciągu miesiąca od zakończenia roku, za który powinny zostać dostarczone. Obejmują one informacje, na podstawie których prokurator czy inny organ lub jednostka administracji publicznej podjęły dalsze czynności, w tym przekazanie innemu organowi lub jednostce administracji publicznej, a w przypadku czynności podjętych przez prokuratora – wszczęcie postępowania przygotowawczego, postawienie zarzutu popełnienia przestępstwa, dokonanie blokady rachunku albo wstrzymanie transakcji, jak również wydanie postanowienia o zabezpieczeniu majątkowym. Ze względu na jawny charakter sprawozdania sporządzonego przez GIIF dane, o których mowa, powinny nie tylko odzwierciedlać rzeczywisty stan rzeczy w danym roku, lecz także zostać ocenione pod kątem możliwości ich ujawnienia[10].

Szef ABW oraz minister właściwy do spraw finansów publicznych mogą delegować – na wniosek Generalnego Inspektora – pracowników lub funkcjonariuszy jednostek i organów im podległych lub przez nich nadzorowanych do pracy lub służby w DIF MF. Dzięki takiemu rozwiązaniu DIF MF może zyskać merytoryczne wsparcie w sprawach pozostających w jego kompetencji. Powinno ono dotyczyć przede wszystkim zapewnienia bezpieczeństwa informacji, w tym także w relacjach międzynarodowych (art. 114 ust. 1 pkt 2–4 nuop), bezpieczeństwa fizycznego systemu teleinformatycznego, którego administratorem jest GIIF (art. 12 ust. 4 nuop), a także realizowania czynności analitycznych związanych z podejrzeniami o finansowanie działalności terrorystycznej. Warunki i tryb delegowania pracowników lub funkcjonariuszy regulują odrębne przepisy, określające sposób działania macierzystych jednostek i organów. W przypadku ABW będzie to *Rozporządzenie Prezesa Rady Ministrów z dnia 16 lutego 2004 r. w sprawie warunków i trybu oddelegowania funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego do wykonywania zadań poza Agencją*[11].

Istotnym elementem systemu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu jest ustanowienie przy Generalnym Inspektorze KBF, który jest organem opiniodawczym i doradczym. W skład KBF wchodzi między innymi przedstawiciel wskazany przez szefa ABW (art. 20 ust. 1 pkt 3 ppkt o nuop). Jako członek KBF powinien on mieć wiedzę na temat przeciwdziałania praniu pieniędzy i finansowaniu terroryzmu oraz spełniać wymagania dotyczące dostępu do informacji niejawnych o klauzuli „tajne" lub „ściśle tajne". Członkowie Komitetu uczestniczą w posiedzeniach osobiście. Komitet wydaje opinie oraz rekomendacje odnoszące się do kwestii

[10] Generalny Inspektor udostępnia sprawozdanie w Biuletynie Informacji Publicznej na stronie podmiotowej urzędu obsługującego ministra właściwego do spraw finansów publicznych (art. 14 ust. 7 nuop).

[11] DzU z 2004 r. nr 34 poz. 296.

merytorycznych, w tym również rozwiązań ustawodawczych we wskazanych obszarach oraz kierunków przeciwdziałania zjawiskom, które generują lub utrzymują zagrożenie związane z praniem pieniędzy i finansowaniem terroryzmu, i sposobów ich zwalczania. Do jego zadań należy między innymi: opiniowanie krajowej oceny ryzyka prania pieniędzy oraz finansowania terroryzmu, opiniowanie strategii przeciwdziałania, wydawanie rekomendacji na temat zastosowania wobec danej osoby lub podmiotu szczególnych środków ograniczających, dokonywanie analiz i ocen rozwiązań prawnych z zakresu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu i przedstawianie opinii o potrzebie wprowadzenia zmian w przepisach. Zadania KBF oraz udział przedstawiciela ABW w ich realizacji to ważne elementy systemu monitorowania zagrożeń w państwie. Warto zauważyć, że ABW nie tylko przyznano status wiodącej służby realizującej działania antyterrorystyczne (przede wszystkim w sferze operacyjnej), lecz także ma ona potencjał do przygotowywania globalnych analiz na temat zagrożeń w państwie. Zgodnie z art. 5 ust. 4 ustawy o ABW oraz AW do zadań ABW należy uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji, które mogą mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Uprawnienia funkcjonariuszy ABW i AW wynikające z tych zadań zostały określone w art. 21 ust. 1 pkt 2 wspomnianej ustawy. Instrumentarium wykonawcze, którym dysponuje ABW, w pełni pozwala na współdziałanie analityczne z Generalnym Inspektorem w zakresie zadań realizowanych przez KBF. Należy wskazać, że analiza i uzyskane wyniki mogą obejmować także dane, którymi ABW dysponuje dzięki prowadzonym czynnościom operacyjno-rozpoznawczym oraz dochodzeniowo-śledczym w sprawach z art. 299 i 165a *Kodeksu karnego* (dalej: kk)[12].

Komitet oraz poszczególne jednostki współpracujące, w tym ABW, wspierają merytorycznie również opracowywanie dokumentu określanego jako krajowa ocena ryzyka (rozdział 4 nuop). Stanowi on podstawę do wypracowania na przyszłość strategii walki z praniem pieniędzy oraz finansowaniem terroryzmu. Generalny Inspektor weryfikuje aktualność tej oceny i w razie potrzeby, nie rzadziej jednak niż co dwa lata, ją uaktualnia. Krajowa ocena ryzyka jest swoistym *novum* w odniesieniu do działań zarówno Generalnego Inspektora, jak i poszczególnych podmiotów będących uczestnikami systemu przeciwdziałania. Co ważne, ma ona przełożenie także na działania instytucji obowiązanych, a więc kilku tysięcy podmiotów uplasowanych w różnych obszarach obrotu prawnego, finansowego oraz gospodarczego. Prowadzony przez nie stały monitoring i wykonywane analizy pozwalają w odpowiedni sposób stosować środki bezpieczeństwa finansowego, identyfikować i śledzić okoliczności, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania

[12] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny* (t.j.: DzU z 2019 r. poz. 1950, ze zm.). Artykuł 299 kk penalizuje zachowanie określane jako pranie pieniędzy, natomiast art. 165a kk – zachowanie sprawcy uprawiającego proceder finansowania terroryzmu.

terroryzmu[13]. Agencja Bezpieczeństwa Wewnętrznego z własnej inicjatywy przekazuje Generalnemu Inspektorowi informacje lub dokumenty, które mogą wpłynąć na krajową ocenę ryzyka. Mogą one kształtować zarówno pierwotną wersję tej oceny, jak i prowadzić do jej zmiany lub uzupełnienia w ramach procedury weryfikacji. Generalny Inspektor może też wystąpić do ABW z żądaniem ich dostarczenia, wskazując jednocześnie formę oraz termin przekazania. Szef ABW ma prawo odmówić GIIF, jeżeli miałoby to mu uniemożliwić wykonanie jego ustawowych zadań.

Wydaje się, że pomimo dwuletniego okresu przewidzianego na aktualizację krajowej oceny ryzyka byłoby wskazane przeprowadzanie jej znacznie częściej. Argumentami przemawiającymi za tym postulatem są: nieustanna fluktuacja zjawiska prania pieniędzy i finansowania terroryzmu, stale zmieniająca się taktyka działania sprawców oraz identyfikowanie coraz to nowszych źródeł środków, które są generowane w ramach tzw. przestępstw pierwotnych. Dotyczy to zarówno nielegalnych środków, które zostają później zalegalizowane (wyprane), jak i środków pochodzących z działalności przestępczej i przeznaczanych na finansowanie działań terrorystycznych. Nie ma przeszkód, oprócz zastrzeżeń określonych w art. 26 ust. 3 nuop, aby ABW w ramach współpracy przekazywała GIIF informacje o takich zagrożeniach na bieżąco, a nie tylko na potrzeby opracowania i nowelizacji krajowej oceny ryzyka czy też realizowania przez Generalnego Inspektora zadań własnych. Jednocześnie wydaje się słuszne, aby strategia przygotowana na podstawie tej oceny zawierała mechanizmy służące monitorowaniu realizacji zadań, które z niej wypływają. Jednostki współpracujące, a więc również ABW, przekazują do GIIF informacje o podjętych działaniach wynikających z zaleceń zawartych w strategii – w przypadku organów administracji rządowej – co najmniej raz na sześć miesięcy od dnia jej ogłoszenia w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" (art. 32 ust. 3 nuop).

Jednym z obowiązków jednostek współpracujących jest, o czym już wspomniano, przekazywanie informacji i dokumentów na wniosek Generalnego Inspektora. Dotyczy to również ABW, która na podstawie art. 82 nuop je przekazuje lub udostępnia w granicach swoich ustawowych kompetencji. We wniosku GIIF może wskazać termin oraz formę przekazania lub udostępnienia potrzebnych danych, a także zawrzeć w tym celu odpowiednie porozumienie. Jak sprecyzowano w uzasadnieniu do nuop:

> Art. 82 ust. 1 ustanawia podstawę prawną dla Generalnego Inspektora do pozyskiwania od jednostek współpracujących informacji koniecznych do realizacji jego zadań. W art. 82 ust. 2 przewidziano możliwość zawarcia przez Generalnego Inspektora porozumienia z daną jednostką współpracującą, porozumienia

[13] Artykuł 27 ust. 1 i 2 nuop: „Instytucje obowiązane identyfikują i oceniają ryzyko związane z praniem pieniędzy i finansowaniem terroryzmu odnoszące się do ich działalności, z uwzględnieniem czynników ryzyka dotyczących klientów, państw lub obszarów geograficznych, produktów, usług, transakcji lub kanałów ich dostaw. Te działania są proporcjonalne do charakteru i wielkości instytucji obowiązanej. Przy ocenianiu ryzyka instytucje obowiązane mogą uwzględniać obowiązującą krajową ocenę ryzyka (…)".

> określającego warunki techniczne przekazania lub udostępnienia informacji lub dokumentów. Celem regulacji z[a]wartej w ust. 2 jest zwiększenie efektywności wymiany informacji między Generalnym Inspektorem a konkretnymi jednostkami współpracującymi[14].

Wskazane rozwiązanie prawne umożliwia zawarcie przez Generalnego Inspektora i kierownika jednostki organizacyjnej, w tym szefa ABW, szczegółowego porozumienia w celu zapewnienia właściwej i merytorycznej współpracy. W omawianym przypadku zawężono je do warunków technicznych przekazania lub udostępnienia informacji i dokumentów. Stwarza to jednak – jak się wydaje – możliwości niejawnego komunikowania się w ramach podejmowanych działań o charakterze antyterrorystycznym czy też bieżącego wnioskowania przez GIIF o informacje i dokumenty. Dopuszczalne zdaje się również podpisanie szerszego porozumienia pomiędzy Generalnym Inspektorem a szefem ABW (jako porozumienia administracyjnego pomiędzy organami rządowymi), uwzględniającego wymianę informacji w kwestiach merytorycznych. Jej zakres oraz odpowiednie kompetencje Agencji zostały określone w nuop.

W tym miejscu należy zadać pytanie, czy szef ABW ma uprawnienia do zawarcia takiego porozumienia. W treści ustawy o ABW oraz AW nie ma ogólnego odniesienia, że może on podpisywać porozumienia w granicach uprawnień, jakimi dysponuje Agencja. Niemniej prawne formy jego działania to przede wszystkim: zarządzenie, decyzja, wytyczne, obwieszczenie i porozumienie[15]. Niejednokrotnie w takich porozumieniach nie przywołuje się podstawy prawnej lub też przytacza się ogólne przepisy kompetencyjne i prawa administracyjnego. Jest istotne, aby porozumienie administracyjne występowało między organami, które nie są sobie podporządkowane, a więc między którymi nie ma stosunku podległości służbowej (ten warunek spełnia relacja GIIF–szef ABW). Dopuszczalność zawierania takich porozumień wynika z tego, że współdziałanie stanowi podstawowy obowiązek wszystkich organów administracji państwowej. Porozumienie może być zawarte tylko w sprawach objętych kompetencjami stron i jest regulowane prawem administracyjnym. Aby było zgodne z obowiązującymi przepisami, wymaga istnienia podstawy prawnej, gdyż organy administracji publicznej nie mogą zmieniać zakresu swoich kompetencji bez wyraźnego upoważnienia ustawowego. Podstawą prawną do zawarcia takiego porozumienia będą uprawnienia ABW wskazane w ustawie kompetencyjnej oraz kompetencje Generalnego Inspektora określone w nuop. W omawianym rodzaju porozumienia może się znaleźć: wskazanie stron porozumienia, ustanowienie innych osób (z imienia i nazwiska lub z każdorazowo pełnionej funkcji) uprawnionych do działania w imieniu głównych

[14] Druk nr 2233 Sejmu RP VIII kadencji, *Rządowy projekt ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu*, s. 40, http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2233 [dostęp: 23 I 2020].

[15] *Zarządzenie nr 11 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 5 lutego 2019 r. w sprawie procedury legislacyjnej w Agencji Bezpieczeństwa Wewnętrznego*, § 2 pkt 3 (Dz. Urz. ABW z 2019 r. poz. 1).

stron (organów) porozumienia, zakres przedmiotowy i merytoryczny, określenie trybu przekazywania informacji lub dokumentów, ustalenia dotyczące przestrzegania przepisów o ochronie informacji niejawnych oraz informacji finansowych, sposobu wykorzystania informacji i dokumentów – także w relacjach z podmiotami trzecimi, w tym zagranicznymi. Dodatkowo może ono zawierać odnośniki dotyczące finansowania wspólnych przedsięwzięć oraz rozstrzygania sporów kompetencyjnych, a także możliwości i sposobu aneksowania porozumienia i jego wypowiadania. Należy zauważyć, że porozumienie podpisane przez Generalnego Inspektora wyłącznie na podstawie art. 82 ust. 2 nuop, mimo jego zawężenia do określenia warunków technicznych przekazania lub udostępnienia informacji czy dokumentów przez jednostkę współpracującą, może stanowić część szerszego porozumienia pomiędzy GIIF a kierownikiem takiej jednostki (w takim przypadku wraz z przywołaną podstawą prawną powinno znajdować się odniesienie do art. 82 ust. 2 nuop).

Niezależnie od podpisywanych porozumień ABW – na podstawie art. 83 nuop – powinna opracować instrukcję postępowania (procedura wewnętrzna) w przypadku podejrzenia popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu. Do obowiązków jednostki współpracującej należy między innymi niezwłoczne powiadomienie Generalnego Inspektora o zaistnieniu takiego podejrzenia.

> Art. 83 nakłada na jednostki współpracujące obowiązek przekazywania Generalnemu Inspektorowi powiadomień, w przypadku powzięcia podejrzeń popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, oraz obowiązek opracowania procedury postępowania obowiązującej w jednostce współpracującej w tego rodzaju przypadkach. Przepis stanowi odpowiednik art. 15a ustawy o p.p.p.f.t. Przykładowe wyliczenie informacji, które powinny zostać zwarte w powiadomieniu, określono w art. 83 ust. 2. W ust. 3 nałożono na Generalnego Inspektora obowiązek przekazania informacji zwrotnej dotyczącej związku informacji przekazanych w powiadomieniu z informacjami o podejrzeniach popełnienia przestępstwa prania pieniędzy, finansowania terroryzmu albo innych przestępstw lub przestępstw skarbowych uzyskanymi z innych źródeł[16].

Powiadomienie o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu powinno zawierać w szczególności: dane osób fizycznych, tj. imię i nazwisko, obywatelstwo, numer PESEL lub datę urodzenia (w przypadku gdy nie nadano numeru PESEL), państwo urodzenia, serię i numer dokumentu stwierdzającego tożsamość osoby, adres zamieszkania (jeśli instytucja obowiązana dysponuje tą informacją); nazwę (firmy), numer identyfikacji podatkowej (NIP) oraz adres głównego miejsca wykonywania działalności gospodarczej (w przypadku osoby fizycznej prowadzącej działalność gospodarczą); dane osób prawnych lub jednostek organizacyjnych nieposiadających osobowości prawnej, które pozostają w związku z okolicznościami mogącymi wskazywać na podejrzenie popełnienia przestępstwa

[16] Druk nr 2233…, s. 41.

prania pieniędzy lub finansowania terroryzmu; opis okoliczności mogących wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu oraz uzasadnienie przekazania powiadomienia. Generalny Inspektor informuje ABW, nie później niż w ciągu 30 dni, o okolicznościach świadczących o związku pomiędzy informacjami zawartymi w powiadomieniu a zawiadomieniami przekazanymi na podstawie art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1 oraz art. 90. Wskazane zawiadomienia to:

- zawiadomienie instytucji obowiązanych o okolicznościach, które mogą wskazywać na podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu (art. 74 ust. 1 nuop);
- niezwłoczne zawiadomienie Generalnego Inspektora przez instytucję obowiązaną o przypadku powzięcia uzasadnionego podejrzenia, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu (art. 86 ust. 1 nuop);
- niezwłoczne zawiadomienie przez instytucję obowiązaną, z wyłączeniem banków krajowych, oddziałów banków zagranicznych, oddziałów instytucji kredytowych i spółdzielczych kas oszczędnościowo-kredytowych, właściwego prokuratora o przypadku powzięcia uzasadnionego podejrzenia, że wartości majątkowe będące przedmiotem transakcji lub zgromadzone na rachunku pochodzą z przestępstwa innego niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwa skarbowego albo mają związek z przestępstwem innym niż przestępstwo prania pieniędzy lub finansowania terroryzmu lub z przestępstwem skarbowym (art. 89 ust. 1 nuop);
- niezwłoczne zawiadomienie Generalnego Inspektora przez instytucję obowiązaną o przeprowadzeniu transakcji, o której mowa w art. 86 ust. 1, w przypadku gdy przekazanie zawiadomienia było niemożliwe przed jej zrealizowaniem. W zawiadomieniu instytucja obowiązana uzasadnia przyczyny wcześniejszego nieprzekazania zawiadomienia oraz przekazuje posiadane informacje potwierdzające powzięcie podejrzenia, o którym mowa w art. 86 ust. 1 (art. 90 ust. 1 nuop).

Należy zauważyć, że ABW (a także Centralne Biuro Antykorupcyjne, Policja, Żandarmeria Wojskowa i Straż Graniczna) jako jedna z nielicznych jednostek współpracujących, które mają jednocześnie status służby specjalnej działającej w obszarze szeroko rozumianego bezpieczeństwa państwa, ma także uprawnienie do uzyskania od GIIF zwrotnego potwierdzenia, łączącego przekazywane informacje z danymi, które pozostają w dyspozycji Generalnego Inspektowa na podstawie nuop. Przedstawiona sytuacja jest swoistym „odpytaniem" GIIF na temat wiedzy zdobytej w wyniku działań określonych w art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1 i art. 90 nuop, a więc dotyczącej specyficznych zdarzeń. Pozyskanie tej wiedzy stwarza możliwość poszerzenia działań kompetencyjnych w sprawach prowadzonych przez ABW. Ponadto analiza i porównanie danych zawartych w powiadomieniu o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, skierowanym

do Generalnego Inspektora, z danymi uzyskanymi przez GIIF od instytucji obowiązanych stanowi istotny element szybkiej reakcji na działania podejmowane przez ABW. Stąd też bardzo ważna wydaje się „niezwłoczność", o której mowa w art. 83 ust. 1 nuop, zwłaszcza gdy dotyczy to czynności realizowanych przez Agencję na poziomie operacyjno-rozpoznawczym. Celem zapisów zawartych w art. 83 ust. 1 i 3 nuop jest jak najefektywniejsze skonfrontowanie przede wszystkim informacji operacyjnych (ale także procesowych – w przypadku realizowania czynności na zlecenie prokuratora) o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu z informacjami znajdującymi się w dyspozycji GIIF. Jest to zatem istotny składnik ustawowego wzorca współpracy, w którym uwzględniono brak uprawnień GIIF do wykonywania czynności operacyjno-rozpoznawczych oraz dysponowanie przez niego informacjami mającymi duże znaczenie dla taktyki działań operacyjnych realizowanych przez ABW.

Sformułowanie „niezwłoczne powiadomienie", które ma podkreślać konieczność szybkiego przekazania informacji i – w dalszej kolejności – pilnej ich weryfikacji, jest w pewnym stopniu przeciwstawne do zapisów art. 83 ust. 3. Wynika z nich bowiem, że GIIF udziela informacji zwrotnej „nie później niż w terminie 30 dni". To rozwiązanie ma dobre i złe strony. Czas na odpowiedź wskazany w ust. 3 nie uniemożliwia znacznie szybszego przekazania ABW informacji zwrotnej, zwłaszcza w sytuacji bezpośredniego zagrożenia zamachem terrorystycznym czy operacyjnego monitorowania środków, które należałoby zabezpieczyć na koncie przez dokonanie blokady lub wstrzymanie transakcji. W takim przypadku obydwa organy powinny ze sobą ściśle współdziałać i wskazać argumenty przemawiające za koniecznością szybkiego przekazania zwrotnego potrzebnych informacji. Należałoby także ustalić, czy i w jakim zakresie Generalny Inspektor mógłby podjąć działania na podstawie art. 76 nuop, tak aby nie naruszyć bezpieczeństwa osób zaangażowanych i informacji pozyskanych w ramach działań operacyjnych. Pomimo że w schemacie postępowania przyjętym ustawowo takiego sposobu współpracy GIIF i ABW nie uwzględniono, może on zostać ustalony na podstawie uzgodnień pomiędzy przedstawicielami obydwu organów. Możliwe jest również zaistnienie sytuacji, w której otrzymane zawiadomienie będzie wymagać od Generalnego Inspektora szerszej analizy lub pozyskania, na podstawie art. 76 nuop, dodatkowych informacji bądź podjęcia działań wydłużonych w czasie. Termin „do 30 dni" wskazany w ustawie ma więc swoje uzasadnienie. Ponadto należy wziąć pod uwagę, że po upływie tego terminu może pojawić się potrzeba przekazania informacji uzupełniającej, gdy GIIF pozyska nowe dane, powiązane z tymi zawartymi w „niezwłocznym powiadomieniu". Powiadomienia ABW w trybie określonym w art. 83 nuop są dostarczane w postaci papierowej lub za pomocą środków komunikacji elektronicznej. W nuop wskazano także na delegację ustawową dla ministra finansów, który określa w rozporządzeniu sposób sporządzania i przekazywania informacji, o których mowa w art. 83 ust. 1, oraz tryb ich przekazywania, mając na uwadze zapewnienie szybkiego, wiarygodnego i bezpiecznego ich przepływu. Do chwili obecnej nie ukazał się jednak odpowiedni akt wykonawczy. Jego wprowadzenie zdecydowanie

uporządkowałoby zagadnienia dotyczące struktury tego rodzaju dokumentów, zakresu informacji, jakie powinny zawierać (podstawowe lub uzupełniające), formy uzasadnienia, jak również warunków technicznych ich sporządzania i przesyłania. Ze względu na założenia prezentowane przez GIIF, zgodnie z którymi komunikacja z podmiotami zewnętrznymi ma być w całości oparta na systemach teleinformatycznych, opracowanie takiego rozporządzenia przyczyniłoby się do szybszej reakcji GIIF na informacje dostarczane przez ABW w „niezwłocznym powiadomieniu".

Kolejnym przykładem uregulowań prawnych w zakresie relacji pomiędzy GIIF a ABW jest zapis zawarty w art. 88 nuop. Stanowi on, że *Generalny Inspektor informuje niezwłocznie, za pomocą środków komunikacji elektronicznej, Szefa Agencji Bezpieczeństwa Wewnętrznego o przekazaniu żądania, o którym mowa w art. 86* (…) *ust. 5 oraz art. 87* (…) *ust. 1*. Jest to o tyle ważne, że prawo do „niezwłocznego poinformowania" ma wyłącznie Agencja. Nie dysponuje nim żadna inna służba specjalna ani policyjna. Jak wskazano w uzasadnieniu do nuop:

> Art. 88 projektu stanowi novum w stosunku do aktualnie obowiązujących przepisów. Zgodnie z regulacją tego artykułu informacja o przekazaniu przez Generalnego Inspektora żądania wstrzymania transakcji lub blokady rachunku w związku z uznaniem, że określona transakcja lub określone wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu powinna być przekazana Szefowi Agencji Bezpieczeństwa Wewnętrznego. Nałożenie tego rodzaju obowiązku na Generalnego Inspektora jest podyktowane złożonością, dynamiką oraz charakterem powiązań finansowych między podmiotami zaangażowanymi w pranie pieniędzy lub działalność finansowania terroryzmu oraz zakresem zadań realizowanych przez Agencję Bezpieczeństwa Wewnętrznego[17].

Zalecenie korzystania ze „środków komunikacji elektronicznej" ma na celu jak najszybsze przekazanie informacji na potrzeby ewentualnego podjęcia przez Agencję dalszych działań oraz wykorzystanie najbardziej bezpiecznego kanału przesyłu informacji. Przedmiotowy obowiązek Generalnego Inspektora dotyczy przede wszystkim przekazania instytucji obowiązanej żądania wstrzymania transakcji lub blokady rachunku na okres nie dłuższy niż 96 godzin, licząc od daty i godziny wskazanych w potwierdzeniu. Instytucja, która otrzymuje takie żądanie, niezwłocznie wdraża odpowiednie procedury. W żądaniu Generalny Inspektor określa wartości majątkowe nim objęte (art. 86 ust. 5 nuop). Artykuł 86 nuop odnosi się do sytuacji, w której żądanie GIIF dotyczące blokady rachunku i wstrzymania transakcji jest skutkiem informacji przekazanych przez instytucję obowiązaną (tryb z art. 86 ust. 1 nuop). Z takim żądaniem Generalny Inspektor może wystąpić (za pomocą środków komunikacji elektronicznej) do instytucji obowiązanej również z własnej inicjatywy, gdy uzna, że określona transakcja lub wartości majątkowe mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu. Również w tym przypadku w żądaniu dotyczącym

[17] Tamże, s. 42.

blokady rachunku Generalny Inspektor określa wartości majątkowe, które mają zostać zablokowane (art. 87 ust. 1 nuop). W obu przypadkach GIIF powinien niezwłocznie poinformować ABW. Warto wskazać różnice pomiędzy przedstawionymi rozwiązaniami. W sytuacji, gdy działania GIIF niejako zatwierdzają merytorycznie inicjatywę instytucji obowiązanej, mamy do czynienia wyłącznie z działaniami analitycznymi i sprawdzającymi ze strony Generalnego Inspektora. Zachodzi wtedy potrzeba ustalenia przez GIIF, czy podmiotami, które uczestniczą w określonej transakcji lub są powiązane z określonymi wartościami majątkowymi i które mogą mieć związek z praniem pieniędzy lub finansowaniem terroryzmu, interesują się inne jednostki współpracujące, w tym głównie służby specjalne i policyjne. Gdy tak nie jest, sytuacja jest prostsza. Postępowanie prowadzone przez Generalnego Inspektora kończy się skierowaniem do prokuratury zawiadomienia o podejrzeniu popełnienia przestępstwa. Natomiast w przypadku, gdy określone podmioty są w kręgu zainteresowania wskazanych służb, konieczne staje się opracowanie odpowiedniej taktyki działania. Powinna ona uwzględniać zabezpieczenie środków jako będących w przestępczym obrocie. W konsekwencji GIIF również złoży do prokuratora zawiadomienie o podejrzeniu popełnienia przestępstwa, ale z informacją, która służba rozpoznaje podejrzewane podmioty. Ustalenie odpowiedniej taktyki działania jest bardziej skomplikowane w sytuacji, gdy zabezpieczenie środków może być przedwczesne i negatywnie wpłynąć na czynności operacyjno-rozpoznawcze prowadzone przez służby. Dlatego też podjęcie inicjatywy uruchomienia trybu z art. 86 ust. 1 nuop pozostaje w gestii samej instytucji obowiązanej. To powoduje, że Generalny Inspektor może mieć trudności ze zrealizowaniem do końca tego trybu postępowania. Sytuację prowadzącą do konfliktu interesów między GIIF a służbą specjalną można uznać za wyjątkową, ale należy ją wziąć pod uwagę. Brak wątpliwości oznacza bowiem, że Generalny Inspektor nie może nie złożyć do prokuratury zawiadomienia o podejrzeniu popełnienia przestępstwa (działania na podstawie art. 86 ust. 5 nuop, tj. uznanie, że transakcja może mieć związek z praniem pieniędzy lub finansowaniem terroryzmu). Warto również zauważyć, że obowiązek GIIF wynikający z art. 88 nuop w sytuacji określonej w art. 86 ust. 5 oraz art. 87 ust. 1 nuop jest obowiązkiem *ex post* (po przekazaniu żądania). Wskazuje on na niezależność decyzyjną GIIF, jednak w ważnych przypadkach, takich jak podejrzenie finansowania terroryzmu, GIIF może wcześniej skonsultować się z ABW. Ze względu na odrębność działań operacyjnych prowadzonych przez ABW wydaje się to nawet wskazane. Aby zminimalizować negatywne skutki takich sytuacji, a nawet je wyeliminować, instytucje obowiązane powinny mieć na uwadze możliwość wcześniejszego skorzystania z art. 74 nuop. Okoliczności uwzględnione w zawiadomieniu pozwolą na przeprowadzenie szerszego rozpoznania *ex ante* przez jednostkę analityki finansowej (dalej: JAF) zarówno samodzielnie, jak i we współpracy z podmiotami zewnętrznymi. Na dalszym etapie jest możliwe uruchomienie działań z art. 76 nuop (w ramach własnej sprawy analitycznej GIIF), w tym zastosowanie środka bezpieczeństwa finansowego przez instytucję obowiązaną, o którym mowa w art. 34 ust. 1 pkt 4 (bieżące monitorowanie stosunków gospodarczych klienta). Przypomnijmy, że obowiązek Generalnego

Inspektora dotyczący przekazania informacji do szefa ABW następuje niezwłocznie, ale po przekazaniu żądania. Jest więc realizowany *post factum*, gdy do instytucji obowiązanej został już wysłany jednoznaczny komunikat w celu wstrzymania transakcji lub blokady rachunku. Sytuacja jest prostsza, gdy dzieje się to z inicjatywy Generalnego Inspektora. Wcześniej ma on bowiem możliwość dokonania ustaleń z jednostkami współpracującymi (na podstawie art. 82 nuop) oraz pozyskania dodatkowych informacji i dokumentów od instytucji obowiązanej (na podstawie art. 76 nuop) w celu ustalenia, czy tego rodzaju działanie powinno zostać uzgodnione z zainteresowanymi służbami. W tej sytuacji przekazanie informacji o żądaniu GIIF na podstawie art. 87 ust. 1 nuop jest jedynie elementem pewnej procedury powiadamiania. W sytuacji, w której instytucja obowiązana nie miała możliwości przekazania zawiadomienia do GIIF przed realizacją transakcji (art. 86 ust. 1 nuop), po dopełnieniu przez nią tego obowiązku (na podstawie art. 90 ust. 1 nuop) Generalny Inspektor powinien dokonać odpowiednich sprawdzeń i na podstawie art. 83 ust. 3 nuop przekazać zwrotnie informację do ABW.

Jeżeli z informacji posiadanych przez GIIF bądź też z ich przetworzenia lub analizy wynika uzasadnione podejrzenie popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu, Generalny Inspektor przekazuje właściwemu prokuratorowi zawiadomienie o podejrzeniu popełnienia przestępstwa wraz z informacjami lub dokumentami uzasadniającymi to podejrzenie (art. 103 ust. 1 nuop). Dotyczy to czynności analitycznych GIIF, które są prowadzone przez jednostki PJAF. Generalny Inspektor w ramach podjętych przez siebie czynności analitycznych nie tylko współdziała (wymienia informacje i zapytania) z jednostkami współpracującymi czy zagranicznymi odpowiednikami, lecz także podejmuje analizę przekazanych i pozyskanych informacji. W jej wyniku może, jak już wspomniano powyżej, wystąpić do instytucji obowiązanej z żądaniem dokonania blokady rachunku lub wstrzymania transakcji, a także zawiadomić o podejrzeniu popełnienia przestępstwa z art. 299 lub 165a kk.

W ramach prowadzonych czynności analitycznych GIIF pozyskuje informacje w różny sposób, tzn. otrzymuje je w sposób automatyczny (np. na podstawie art. 72 nuop) lub w wyniku inicjatywy instytucji obowiązanej czy jednostki współpracującej, dzięki wymianie międzynarodowej czy podpisanym porozumieniom. Jeżeli GIIF złożył wskazane zawiadomienie o podejrzeniu popełnienia przestępstwa na podstawie współpracy z jednostką współpracującą, w tym ABW, nie później niż w terminie 30 dni od dnia przekazania takiego zawiadomienia informuje o tym instytucję obowiązaną lub jednostkę współpracującą, która przekazała informacje będące podstawą tego zawiadomienia (art. 103 ust. 2 nuop). Nie dotyczy to jednak wszystkich informacji, a jedynie tych, które zostały przekazane przez ABW na podstawie art. 83 ust. 1 nuop. Konsekwencją takiego powiadomienia jest obowiązek Generalnego Inspektora dotyczący zwrotnego poinformowania Agencji, gdy przekazane informacje łączą się z działaniami GIIF podejmowanymi na podstawie art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 1, art. 90 oraz art. 103 ust. 1 nuop.

W celu realizacji zadań określonych w nuop Generalny Inspektor na bieżąco współpracuje z sądami i prokuratorami na potrzeby postępowania karnego. Rola GIIF nie kończy się bowiem z chwilą przekazania do prokuratury zawiadomienia o podejrzeniu popełniania przestępstwa. Prokurator może zażądać od Generalnego Inspektora udostępnienia informacji lub dokumentów, w tym informacji lub dokumentów objętych tajemnicami prawnie chronionymi (art. 104 ust. 2 nuop), w celu weryfikacji danych zawartych w tym zawiadomieniu. W przypadku gdy Generalny Inspektor nie dysponuje żądanymi informacjami, występuje do jednostek współpracujących, w tym do ABW. Jak wskazano w uzasadnieniu do nuop:

> (…) w celu zapewnienia efektywnego wsparcia prokuratorów prowadzących postępowania w sprawie prania pieniędzy lub finansowania terroryzmu wszczęte na podstawie zawiadomień o podejrzeniu popełnienia przestępstwa przekazanych przez Generalnego Inspektora, Generalny Inspektor przekazuje na ich wniosek również informacje lub dokumenty, które nie znajdują się w jego dyspozycji i dopiero muszą być pozyskane. Wprawdzie takie informacje lub dokumenty mogą być pozyskane bezpośrednio przez prokuratora, bez pośrednictwa Generalnego Inspektora, jednakże proponowane rozwiązania mają na celu maksymalne odciążenie prokuratora prowadzącego takie postępowanie i stanowią swojego rodzaju wyraz „wzięcia przez Generalnego Inspektora odpowiedzialności" za zasadność przekazanego zawiadomienia o podejrzeniu popełnienia przestępstwa prania pieniędzy lub finansowania terroryzmu[18].

W opisanej sytuacji „pośredniczenia" jest wskazana duża ostrożność, zwłaszcza gdy podstawą skierowania przez GIIF zawiadomienia o podejrzeniu popełnienia przestępstwa z art. 299 lub 165a kk były informacje zdobyte przez ABW podczas czynności operacyjno-rozpoznawczych. W takim przypadku prokurator powinien zwrócić się bezpośrednio do Agencji jako pierwotnego posiadacza tych informacji. Ze względu na specyfikę niektórych czynności operacyjno-rozpoznawczych, szczególnie tych, które mają walor dowodowy, relacje o zakresie i sposobie wykorzystania tych informacji powinny być rozstrzygane na poziomie prokurator–ABW. Jednocześnie dane, które ma GIIF i które są podstawą do złożenia zawiadomienia, mogą być tylko częścią materiału zgromadzonego przez ABW w zdecydowanie szerszym kontekście, niż to wynika z uprawnień Generalnego Inspektora. W związku z tym właściwe wydaje się (nie negując przy tym potrzeby zawarcia w nuop przedmiotowej podstawy do realizacji czynności przez GIIF) korzystanie z tego uprawnienia tylko wtedy, gdy Agencja po przeanalizowaniu materiałów „świadomie upoważni" GIIF do przekazania ich prokuratorowi. Należy przypomnieć, że Generalny Inspektor dysponuje informacjami od ABW na potrzeby wywiadu finansowego w trybie administracyjnym. Nie jest on podmiotem tak upoważnionym jak ABW do czynności prowadzonych w ramach

[18] Tamże, s. 52–53.

postępowania karnego, regulowanych kodeksem postępowania karnego[19] (należy pamiętać, że z chwilą wydania postanowienia przez prokuratora tryb administracyjny zmienia się w tryb postępowania na podstawie przepisów kpk). Jednocześnie konieczne jest dopilnowanie, aby w ramach przekazywania materiałów do GIIF Agencja nie ujawniła taktyki swoich działań operacyjnych, która podlega ochronie przez obwarowanie tych działań klauzulami niejawności. Te materiały będą bowiem, gdy prokurator uzna je za dowód w sprawie, przedmiotem zapoznania się przez strony postępowania karnego. Uprawnień do posiadania tego rodzaju wiedzy nie mają również pracownicy DIF MF. Przedstawiciel ABW (szef lub inna upoważniona osoba), który kieruje korespondencję do GIIF, powinien więc przestrzegać właściwego trybu. Zwłaszcza gdy dotyczy to trybu określonego w art. 83 ust. 1 nuop, którego konsekwencją może być skierowanie przez GIIF zawiadomienia o popełnieniu przestępstwa z powołaniem się na informacje przekazane przez ABW, czy też trybu z art. 105 ust. 1 nuop. W tym drugim przypadku relacja zostaje ściśle określona na wniosek szefa ABW w uzasadnieniu zawartym w zawiadomieniu. Jednocześnie wydaje się, że mimo treści art. 104 ust. 2 i 3 nuop udostępnienie informacji i dokumentów, które stanowiły podstawę do złożenia zawiadomienia przez GIIF, powinno zostać uzgodnione także w relacji prokurator–GIIF–ABW.

Jak już wspomniano, jednym z zadań Generalnego Inspektora jest podejmowanie czynności w celu przeciwdziałania praniu pieniędzy oraz finansowaniu terroryzmu, zwłaszcza przez wymianę informacji z jednostkami współpracującymi, w tym z ABW. Mają temu służyć rozwiązania wskazane w art. 105 nuop. Generalny Inspektor udostępnia posiadane informacje na pisemny i uzasadniony wniosek szefa ABW lub osób przez niego upoważnionych w zakresie ich ustawowych zadań (art. 105 ust. 1 pkt 5 nuop). Treść niniejszej jednostki redakcyjnej wskazuje przede wszystkim na wprowadzenie trybu wnioskowego dla relacji pomiędzy szefem ABW a GIIF. Ten tryb został obwarowany dwoma warunkami techniczno-merytorycznymi. Po pierwsze, wniosek musi mieć charakter pisemny, a więc inna droga nie jest dopuszczalna. Po drugie, jest konieczne załączenie uzasadnienia do niego. Z wnioskiem może wystąpić wyłącznie szef ABW albo osoba przez niego upoważniona. To rozwiązanie ma na celu nie tyle ograniczenie relacji z GIIF, ile ich zawężenie wyłącznie do osób sprawujących określoną funkcję w Agencji. Na poziomie szefa zakres współpracy z GIIF jest pełny i odnosi się do wszystkich kompetencji, jakie ma ABW. Natomiast w przypadku innych osób upoważnienie powinno wynikać z zakresu kompetencyjnego, jaki jest przyznany danej osobie w ramach Agencji lub w ramach upoważnienia wewnętrznego wydanego przez szefa ABW. Uprawnienie dostępu do informacji wymienianych z szefem ABW (lub osobami przez niego upoważnionymi) ma wyłącznie Generalny Inspektor. Tym samym osoby trzecie, np. zatrudnione w innych departamentach (komórkach

[19] Artykuł 21 ust. 3 ustawy o ABW i AW stanowi, że „(...) funkcjonariusze ABW wykonują czynności tylko w zakresie właściwości tej Agencji i w tym zakresie przysługują im uprawnienia procesowe Policji, wynikające z przepisów kodeksu postępowania karnego".

organizacyjnych MF), nie powinny mieć możliwości zapoznania się z nimi. Stąd postulat, aby cała korespondencja odbywała się za pośrednictwem kancelarii tajnej wyodrębnionej dla DIF MF, nie zaś ogólnej kancelarii tajnej MF. Ze względu na wyłączność adresata informacji finansowej, Generalny Inspektor nie powinien także dekretować pism z kancelarii tajnej na inne komórki organizacyjne MF, a wyłącznie na DIF MF. Odnosi się to również do ministra finansów w przypadku, gdy wykonuje on czynności GIIF.

Należy zauważyć, że nie został ustalony formalny kształt wniosku uprawnionego podmiotu występującego o informacje posiadane przez GIIF. Minister właściwy do spraw finansów publicznych może określić, w odpowiednim rozporządzeniu, sposób sporządzania i przyjmowania przez Generalnego Inspektora wniosków, o których mowa w art. 105 ust. 1, 3 i 4, oraz tryb ich przyjmowania (art. 109 nuop). Jest to rozwiązanie fakultatywne i do chwili obecnej nie wydano odpowiedniego aktu wykonawczego do nuop. Taki wniosek powinien jednak spełniać podstawowe wymagania określone przepisami prawa administracyjnego, a ponadto – co ważne – zawierać uzasadnienie i zostać podpisany przez uprawnioną osobę. Uzasadnienie jest o tyle ważne, że wniosek ogólnie dotyczy informacji posiadanych przez GIIF. Tym samym powinno się sprecyzować, jaka informacja zwrotna ma zostać przekazana wnioskodawcy. Warto mieć na względzie to, że w zasobach GIIF znajdują się miliony informacji, głównie pozyskanych po 2004 r. Jest zatem ważne, czy wniosek uprawnionej jednostki współpracującej dotyczy spraw bieżących, czy przeszłych (np. na potrzeby uzyskania wiedzy o składnikach majątkowych w związku z instytucją konfiskaty rozszerzonej).

Jednocześnie Generalny Inspektor udostępnia szefowi ABW informacje, o których mowa w art. 72 nuop, na warunkach określonych w art. 34 ust. 2a ustawy o ABW oraz AW[20]. W uzasadnieniu do projektu nuop wskazano, że:

> (…) w art. 104 ust. 1 (aktualnie art. 105 ust. 1 nuop – przyp. aut.), stanowiącym odpowiednik art. 33 ustawy o p.p.p.f.t., wskazano organy, które w zakresie wyznaczonym ich ustawowymi zadaniami są uprawnione do uzyskania informacji od Generalnego Inspektora. Art. 104 ust. 2 tworzy podstawę prawną do pozyskiwania przez Centralne Biuro Antykorupcyjne oraz Szefa Agencji Bezpieczeństwa Wewnętrznego informacji o „transakcjach ponadprogowych" w trybie i na zasadach lub na warunkach określonych w przepisach regulujących funkcjonowanie tych służb[21].

Odwołanie do art. 34 ust. 2a ustawy o ABW oraz AW jest nowym rozwiązaniem prawnym w zakresie dzielenia się z innymi podmiotami informacjami pozyskiwanymi przez GIIF od instytucji obowiązanych. Zawężono je do dwóch służb specjalnych – CBA i ABW. Zgodnie z tym artykułem administrator zbioru danych, o którym mowa

[20] Zob. pełny zakres zmian: DzU z 2018 r. poz. 2387, 2245, 2399; DzU z 2019 r. poz. 53, 125.

[21] Druk nr 2233…, s. 53.

w ust. 2[22] (administrator danych, w tym danych osobowych), udostępnia szefowi ABW w drodze teletransmisji informacje zgromadzone w zbiorach danych bez konieczności każdorazowego przedstawiania imiennego upoważnienia wydanego przez szefa ABW, okazywanego przez funkcjonariusza ABW wraz z legitymacją służbową, o których mowa w ust. 2. Udostępnianie informacji następuje, jeżeli jednostka organizacyjna ABW będąca odbiorcą informacji spełnia łącznie następujące warunki: 1) ma urządzenia umożliwiające odnotowanie w systemie, kto, kiedy, w jakim celu oraz jakie dane uzyskał; 2) ma zabezpieczenia techniczne i organizacyjne uniemożliwiające wykorzystanie danych niezgodnie z celem ich uzyskania; 3) specyfika lub zakres wykonywanych zadań uzasadnia takie udostępnienie. Dotyczy to m.in. tzw. informacji o transakcjach ponadprogowych, któremu to zagadnieniu poświęcono znacznie więcej uwagi. Polski ustawodawca wiele lat temu wprowadził do systemu AML/CFT możliwość uzyskania przez GIIF informacji o transakcjach ponadprogowych (o równowartości 15 tys. euro i powyżej). To pozwoliło na anonimowe pozyskiwanie informacji o wielu transakcjach, niezależnie od tego, czy wiążą się one z praniem pieniędzy, czy z finansowaniem działalności terrorystycznej. Mimo wielokrotnej krytyki tego rozwiązania, stało się ono wzorcem dla systemu STIR[23] (dotyczy tylko podmiotów gospodarczych – relacji pomiędzy nimi oraz ich relacji z osobami fizycznymi), opracowanego na potrzeby przeciwdziałania przestępczości podatkowej (związanej przede wszystkim z podatkiem VAT). W tym miejscu warto zwrócić uwagę na dwa aspekty. Pierwszy dotyczy technicznego sposobu przekazania informacji i w tym kontekście rozwiązania zaproponowane w nuop nie budzą wątpliwości. Drugi odnosi się do odpowiedzialności GIIF jako administratora systemu wobec podmiotu trzeciego, jakim będzie ABW, za sposób wykorzystania informacji. Przyjęte rozwiązanie wydaje się sprzeczne z zasadami ochrony danych osobowych i odpowiedzialnością administratora systemu za dystrybucję danych (art. 12 ust. 4 nuop), a szczególnie z zachowaniem zasady rozliczalności zgodnie z rozporządzeniem

[22] „Administrator zbioru danych jest obowiązany udostępnić dane osobowe, o których mowa w ust. 1, na podstawie imiennego upoważnienia wydanego odpowiednio przez Szefa ABW albo Szefa AW okazanego przez funkcjonariusza wraz z legitymacją służbową".

[23] STIR (system teleinformatycznej izby rozliczeniowej) – „(...) służy do przetwarzania danych przekazywanych przez banki i SKOK-i w celu ustalenia wskaźnika ryzyka wykorzystania sektora bankowego do dokonania wyłudzeń skarbowych. Ustawa STIR ma w zamiarze stopniowe uruchomienie systemu analizy i przekazywania informacji w celu zapobiegania wyłudzeniom skarbowym. Na podstawie przepisów wprowadzonych tą ustawą Szef Krajowej Administracji Skarbowej będzie otrzymywał informacje o rachunkach podmiotów kwalifikowanych w rozumieniu ustawy STIR (tj. innych niż rachunki osób fizycznych służące do celów prywatnych), a także o wszystkich transakcjach tych podmiotów dokonywanych za pośrednictwem objętych tym systemem rachunków bankowych lub rachunków spółdzielczej kasy oszczędnościowo-kredytowej (SKOK). W oparciu o te informacje system informatyczny Szefa KAS będzie dokonywał analizy ryzyka wystąpienia wyłudzenia skarbowego. Wszystkie informacje są przesyłane automatycznie i elektronicznie za pośrednictwem izby rozliczeniowej", https://poradnikprzedsiebiorcy.pl/-stir-system-teleinformatycznej-izby-rozliczeniowej [dostęp: 23 I 2020]. Zob. też: *Ustawa z dnia 24 listopada 2017 r. o zmianie niektórych ustaw w celu przeciwdziałania wykorzystania sektora finansowego do wyłudzeń skarbowych* (DzU z 2017 r. poz. 2491).

Parlamentu Europejskiego i Rady 2016/679[24]. Tym samym GIIF będzie mógł zastosować to rozwiązanie w przypadku, gdy upoważnienie szefa ABW nie będzie przedstawiane każdorazowo, ponieważ powinno ono mieć charakter stały i obejmować potrzeby różnych komórek organizacyjnych ABW. Nie ma natomiast przeszkód, aby podmiot wewnętrzny w strukturze ABW, który został jednorazowo upoważniony w ten sposób, kierował „zapytanie" do systemu teleinformatycznego GIIF z powołaniem się na numer rejestru sprawy. Jeżeli jest to związane z wewnętrzną polityką bezpieczeństwa w Agencji, to powinien być to przynajmniej przedstawiciel Centrum Antyterrorystycznego (CAT) czy Departamentu Zagrożeń Strategicznych (Departament VII)[25]. Materiały muszą trafiać – w przeciwieństwie do GIIF, u którego wpływają do wewnętrznego zbioru danych administrowanego przez Generalnego Inspektora na podstawie art. 12 ust. 4 nuop – do akt konkretnej sprawy prowadzonej w ABW. Generalny Inspektor jest jedynym podmiotem, który może być uprawniony zbiorczo do pozyskiwania tych danych, niemniej ich przetworzenie, analiza i wykorzystanie powinny wiązać się z konkretną sprawą realizowaną w DIF MF, zarejestrowaną wewnętrznie w systemie. W taki sposób zostanie zachowana, także w ramach struktury GIIF, zasada rozliczalności. Ta kwestia powinna zostać ujęta również w instrukcji, o której mowa w art. 12 ust. 3 nuop[26].

Należy również zauważyć, że w kontekście skuteczności działań mających na celu ustalenie podmiotu uczestniczącego w procederze prania pieniędzy lub finansowania terroryzmu wspomniana już wysokość progu (15 tys. euro) jest problematyczna. W rzeczywistości „pierze się", a więc legalizuje się, środki zdecydowanie poniżej lub znacznie powyżej tej kwoty. Natomiast kwoty przeznaczane na przygotowania do zamachu terrorystycznego są zdecydowanie niższe niż wskazane przez polskiego ustawodawcę, a także są rozłożone w czasie. Tym samym system jest mało efektywny i warto by było się zastanowić, w jakim celu pozyskuje się dane obwarowane taką wysokością. Należałoby zatem zrewidować oceny i poglądy dotyczące trybu i sposobu funkcjonowania systemu przeciwdziałania (głównie odnośnie do śledzenia zagrożeń związanych z finansowaniem terroryzmu), który powinien być zdecydowanie bardziej skuteczny niż aktualne rozwiązania systemowe. Odwołując się do wykładni celowościowej, należałoby zauważyć, że art. 105 ust. 2 wprowadzony do nuop powinien służyć przede wszystkim

[24] *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)*. Artykuł 5 ust. 2: „Administrator jest odpowiedzialny za przestrzeganie przepisów ust. 1 i musi być w stanie wykazać ich przestrzeganie („rozliczalność")" (Dz. Urz. UE L 119 z 4 V 2016 r., s. 1).

[25] *Zarządzenie nr 163 Prezesa Rady Ministrów z dnia 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (M.P. z 2018 r. poz. 927).

[26] W celu skutecznego i efektywnego wykonywania zadań Generalny Inspektor może wydać, z zachowaniem wymogów ochrony informacji niejawnych, instrukcję dotyczącą sposobu realizacji zadań przez komórkę organizacyjną, o której mowa w ust. 2 (DIF MF), w zakresie gromadzenia, przetwarzania i analizy informacji w trybie ustawy.

zwalczaniu przestępstw prania pieniędzy oraz finansowania terroryzmu. Poszerzenie liczby podmiotów, które mogłyby korzystać z pierwotnych danych określonych w art. 72 nuop, powinno stworzyć kolejne „sieci perkolacyjne”[27], które umożliwiłyby ujawnianie – za pomocą innych instrumentów niż będące w dyspozycji instytucji obowiązanej i jednostki analityki finansowej – zdarzeń związanych z podejrzeniem popełnienia wskazanych przestępstw. Ponadto warto mieć na uwadze, że zgodnie z art. 105 ust. 6 nuop w szczególnie uzasadnionych przypadkach Generalny Inspektor może odmówić udostępnienia informacji podmiotom, o których mowa w ust. 1–4 (a więc także szefowi ABW), jeżeli ich udostępnienie mogłoby: 1) negatywnie wpłynąć na proces analizowania przez Generalnego Inspektora informacji dotyczących wartości majątkowych, co do których powzięto podejrzenie, że mogą mieć związek z przestępstwem prania pieniędzy lub finansowania terroryzmu; 2) narazić na niewspółmierną szkodę osobę fizyczną lub osobę prawną. Odpowiedzialność za to spoczywa bezpośrednio na Generalnym Inspektorze. Automatyczne przekazywanie takich informacji nie zapewnia prawidłowego wypełniania tego obowiązku przez GIIF.

Należy zauważyć, że rola i zadania GIIF nie ograniczają się do przeciwdziałania zjawiskom opisanym w art. 299 i 165a kk. Zgodnie z treścią art. 106 nuop – w przypadku powzięcia podejrzenia popełnienia przestępstwa skarbowego lub innego przestępstwa niż przestępstwo prania pieniędzy lub finansowania terroryzmu Generalny Inspektor przekazuje informacje uzasadniające to podejrzenie właściwym organom wskazanym w art. 105 ust. 1 nuop (również szefowi ABW) w celu podjęcia czynności wynikających z ich ustawowych zadań. Po otrzymaniu informacji, o których mowa w art. 106, jednostka współpracująca przekazuje informację zwrotną o sposobie ich wykorzystania w terminie nie dłuższym niż 90 dni, licząc od dnia ich otrzymania. Informacja zwrotna zawiera sygnaturę akt jednostki współpracującej, znak i datę pisma, w którym Generalny Inspektor przekazał te informacje, oraz wskazanie sposobu ich wykorzystania (art. 108 ust. 1 i 2 nuop).

Generalny Inspektor w ramach swoich ustawowych uprawnień może pozyskiwać informacje w celu udostępnienia ich ZJAF. W nuop wiele uwagi poświęcono rozwiązaniom dotyczącym międzynarodowej wymiany informacji. Korzystanie z nich wymaga szczególnej ostrożności, gdyż JAF mogą być wykorzystywane na potrzeby realizacji zadań strategicznych, niekoniecznie związanych z przeciwdziałaniem praniu pieniędzy oraz finansowaniu terroryzmu. Służby specjalne powinny mieć to na uwadze, gdy przekazują GIIF określone informacje. Do informacji udostępnianych ZJAF nie stosuje się art. 99 ust. 7 nuop, w przeciwieństwie do przepisów uoin. Tak więc sposobem kontroli dostępu może być nałożenie na dokument klauzuli niejawności. Jest to jeden z najprostszych, a jednocześnie najwłaściwszy sposób zabezpieczenia

[27] Perkolacja (łac. *percolare* – przeciekać przez coś, filtrować) – termin używany m.in. w teorii układów złożonych o architekturze sieciowej. W tym ujęciu „perkolacja” jest rozumiana jako proces, dzięki któremu zbiór początkowo niezależnych obiektów formuje – na zasadzie „przeciekania” z jednego elementu do drugiego – większą, połączoną strukturę. Znajomość mechanizmów rządzących tym procesem służy do prognozowania rozrostu sieci (przyp. red.).

własnych aktywów w relacjach międzynarodowych w razie potrzeby udzielenia odpowiedzi na poziomie innego państwa. Jednocześnie warto zauważyć, że przekazanie informacji na podstawie „wiadomości" przesłanej ze ZJAF stanowi informacje dla służb specjalnych w kraju odbiorcy (np. ABW). Innym sposobem ochrony informacji jest wprowadzenie do dokumentu operującego w relacji z GIIF zastrzeżenia, że informacje mogą być wykorzystane wyłącznie na cele merytorycznych działań GIIF, a ich udostępnienie poza DIF MF (czyli także ZJAF) jest możliwe wyłącznie po uprzednim powiadomieniu ABW i wyrażeniu przez Agencję formalnej zgody na ich udostępnienie. W przypadku gdy informacje przekazane Generalnemu Inspektorowi w zawiadomieniu lub informacje, o których mowa w art. 74 ust. 1, art. 86 ust. 1, art. 89 ust. 8 lub art. 90, dotyczą innego państwa członkowskiego Unii Europejskiej, Generalny Inspektor niezwłocznie przekazuje z urzędu te informacje do JAF właściwego państwa członkowskiego Unii Europejskiej (art. 112 ust. 3 nuop). Generalny Inspektor odmawia udostępnienia informacji ZJAF, jeżeli: informacje podlegają ochronie zgodnie z przepisami o ochronie informacji niejawnych; udostępnienie informacji mogłoby utrudnić wykonywanie zadań organom wymiaru sprawiedliwości oraz służbom lub instytucjom odpowiedzialnym za ochronę porządku publicznego, bezpieczeństwa obywateli lub ściganie sprawców przestępstw lub przestępstw skarbowych; udostępnienie informacji mogłoby zagrozić bezpieczeństwu państwa lub porządkowi publicznemu; państwo trzecie nie gwarantuje odpowiedniego poziomu ochrony danych osobowych (art. 114 ust. 1 nuop). Odmowa udostępnienia informacji ZJAF wymaga uzasadnienia (art. 114 ust. 2 nuop).

Analiza *Ustawy z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[28] (dalej: uoda) oraz nuop prowadzi do wniosku, że niezależnie od przepisów zawartych w uoda charakter relacji między ABW i GIIF został określony w nuop. Wspomniana ustawa antyterrorystyczna nie ma zapisów odnoszących się wprost do Generalnego Inspektora. W trakcie jej projektowania prawdopodobnie uwzględniono to, że zadania GIIF będzie realizował szef Krajowej Administracji Skarbowej (dalej: KAS) i dlatego nie ujęto odrębnie zadań dla Generalnego Inspektora. Innym wytłumaczeniem jest to, że te relacje są utrzymywane przede wszystkim z podmiotami uprawnionymi do wykonywania czynności operacyjno-rozpoznawczych, a GIIF – jak wskazano – takich uprawnień nie ma. Kolejną możliwością jest to, że ustawodawca nie zdecydował się na uregulowanie współdziałania z GIIF w ramach uoda, ponieważ zostało to dostatecznie uregulowane w pppft i następnie w nuop. Po 13 lipca 2018 r. ani nie zmieniono tych przepisów, ani nie dodano, że w przypadku zaistnienia terrorystycznej sytuacji kryzysowej szef KAS przejmuje zadania GIIF.

Przedmiotem stałego rozpoznania operacyjnego powinny być objęte incydenty o charakterze terrorystycznym określone na podstawie przepisów wykonawczych do ustawy o działaniach antyterrorystycznych[29]. Katalog stanowi załącznik

[28] DzU z 2019 r. poz. 796.

[29] Zob. *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r.*

do rozporządzenia MSWiA wydanego na podstawie art. 5 ust. 2 uoda. Niektóre incydenty opisane w tym rozporządzeniu odnoszą się do zdarzeń związanych z finansowaniem terroryzmu. Punkt 11. załącznika do rozporządzenia otwiera katalog incydentów określonych jako incydenty związane z wprowadzaniem do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł. Aktualnie zapis art. 5 ust. 3 uoda wskazuje, że podmioty i służby specjalne (określone w powyższym katalogu) przekazują szefowi ABW, niezwłocznie po uzyskaniu, informacje służące realizacji działań antyterrorystycznych. Są one klasyfikowane zgodnie z katalogiem incydentów o charakterze terrorystycznym. W tym katalogu brakuje informacji o GIIF, mimo że niektóre incydenty bezpośrednio dotyczą jego działalności. Głównemu Inspektorowi pozostaje jedynie informowanie szefa ABW na podstawie nuop. Wydaje się jednak, że relacje opisane w tej ustawie odnoszą się raczej do czynności *post factum*, z wyjątkiem możliwości, jakie daje art. 105 ust. 1 nuop (w związku z art. 6 ust. 2 i 3 uoda) – tj. działania na wniosek szefa ABW, oraz art. 105 ust. 2 nuop. Pierwszy przypadek dotyczy skuteczności, a przede wszystkim szybkości, z jaką szef ABW wystąpi z wnioskiem. W drugim przypadku chodzi o przekazywanie informacji o transakcjach ponadprogowych. Przy dzisiejszym stanie prawnym (próg 15 tys. euro) nie wydaje się to jednak skutecznym rozwiązaniem, nie tylko pod względem reagowania na zdarzenie o charakterze terrorystycznym, lecz także stałego nadzoru analitycznego nad zjawiskiem finansowania terroryzmu. W relacji ABW–GIIF jest ważne ponadto rozróżnienie, jakiego rodzaju informacje mogą zostać wykorzystane w sposób bardziej ogólny, np. na potrzeby krajowej oceny ryzyka, a które są przekazywane w celu zarejestrowania i prowadzenia konkretnej sprawy analitycznej przez JAF. W relacjach pomiędzy ABW i GIIF związanych z działaniami antyterrorystycznymi powinny zostać uwzględnione między innymi te incydenty o charakterze terrorystycznym, co do których istnieje uzasadnione podejrzenie, że są finansowane z wykorzystaniem instytucji obowiązanych. W tym kontekście działania GIIF wydają się niezbędne dla poszerzenia wiedzy ABW o zagrożeniu. Jednocześnie jest możliwe wykorzystanie w tych relacjach zapisu art. 6 ust. 2 pkt 2 uoda. Stanowi on, że szef ABW stosownie do potrzeb przekazuje informacje, o których mowa w art. 5 ust. 3, oraz informacje zawarte w wykazie, o którym mowa w art. 6 ust. 1, także w postaci bieżących analiz stanu zagrożenia zdarzeniem o charakterze terrorystycznym innym organom administracji publicznej – w zakresie ich właściwości. W tym przypadku adresatem takich informacji może być również GIIF.

w sprawie katalogu incydentów o charakterze terrorystycznym (DzU z 2016 r. poz. 1092); *Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 5 lutego 2019 r. zmieniające rozporządzenie w sprawie katalogu incydentów o charakterze terrorystycznym* (DzU z 2019 r. poz. 317).

Bibliografia

Akty prawne

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (t.j.: DzU z 2019 r. poz. 1115, ze zm.).

Ustawa z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych (t.j.: DzU z 2019 r. poz. 796).

Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (t.j.: DzU z 2020 r. poz. 27).

Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (t.j.: DzU z 2019 r. poz. 742).

Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (DzU z 2017 r. poz. 1049, ze zm.).

Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny (t.j.: DzU z 2019 r. poz. 1950, ze zm.).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 5 lutego 2019 r. zmieniające rozporządzenie w sprawie katalogu incydentów o charakterze terrorystycznym (DzU z 2019 r. poz. 317).

Rozporządzenie Prezesa Rady Ministrów z dnia 13 grudnia 2017 r. w sprawie szczegółowego zakresu działania Ministra – Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych (DzU z 2017 r. poz. 2332).

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 lipca 2016 r. w sprawie katalogu incydentów o charakterze terrorystycznym (DzU z 2016 r. poz. 1092).

Zarządzenie nr 11 Szefa Agencji Bezpieczeństwa Wewnętrznego z dnia 5 lutego 2019 r. w sprawie procedury legislacyjnej w Agencji Bezpieczeństwa Wewnętrznego (Dz. Urz. ABW z 2019 r. poz. 1).

Zarządzenie nr 163 Prezesa Rady Ministrów z dnia 26 września 2018 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego (M.P. z 2018 r. poz. 927).

Źródła internetowe

https://poradnikprzedsiebiorcy.pl/-stir-system-teleinformatycznej-izby-rozliczeniowej

https://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=2233

Abstrakt

Ustawa z dnia 1 marca 2018 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu utrzymała wcześniejszy model współpracy pomiędzy Generalnym Inspektorem Informacji Finansowej a Agencją Bezpieczeństwa Wewnętrznego, ale trochę go zmodyfikowała. Nie ulega wątpliwości, że GIIF i szef ABW muszą ze sobą współpracować przy przeciwdziałaniu zarówno legalizowaniu przestępczych dochodów, jak i wykorzystywaniu środków na cele związane z działalnością terrorystyczną. Celem twórców modelu zawartego we wspomnianej ustawie było udoskonalenie dotychczasowych rozwiązań obowiązujących w relacji GIIF–ABW, jak również zwiększenie jego skuteczności. Jednym z mankamentów tego modelu jest brak uprawnień GIIF do realizowania czynności operacyjno-rozpoznawczych, co jednak nie ogranicza sprawnego funkcjonowania polskich jednostek analityki finansowej przy współpracy z ABW. Relacje pomiędzy GIIF a ABW powinny uwzględniać ochronę informacji niejawnych i informacji finansowych przed podmiotami trzecimi. Utrzymanie głównych założeń wcześniejszego modelu współpracy wskazuje, że jest on zgodny z celami realizowanymi przez obydwa podmioty i nie został oceniony jako nieskuteczny pod kątem ścigania przestępstw określonych w art. 299 i 165a kk. Niemniej jednak należałoby dokonać zmian w ustawie o działaniach antyterrorystycznych i przepisach wykonawczych przez umieszczenie GIIF wśród podmiotów współpracujących z ABW w przypadku incydentów o charakterze terrorystycznym.

Słowa kluczowe: Agencja Bezpieczeństwa Wewnętrznego, jednostka współpracująca, Generalny Inspektor Informacji Finansowej, przeciwdziałanie praniu pieniędzy, przeciwdziałanie finansowaniu terroryzmu, antyterroryzm, incydenty o charakterze terrorystycznym.

Abstract

The Act of March 1, 2018 on Counteracting Money Laundering and Terrorism Financing left a prior model of cooperation between the General Inspector and the Internal Security Agency, slightly modifying it. There is no doubt that both organs, ie the GIIF (the General Inspector for Financial Information) and the Head of the Internal Security Agency must cooperate with each other both in the area of counteracting the legalization of criminal income and the use of funds for purposes related to terrorist activities. The presented model, in the assumptions of the authors of the Act, was to improve the existing solutions in the GIIF–ABW relationship and increase its effectiveness. One of the shortcomings is the lack of the GIIF's powers to perform operational and reconnaissance activities, but this issue does not limit the smooth functioning of PJAF (Polish Financial Intelligence Uniting) cooperation with the Internal Security Agency. Nevertheless, mutual relations should take into

account both the protection of classified information and financial information from third parties. Leaving the current model of cooperation in its structural assumptions indicates that it remains in compliance with the objectives pursued by both entities and has not been assessed as ineffective from the point of view of prosecution of offenses set forth in art. 299 and 165a k.k. (the Penal Code). Nevertheless, it would be necessary to amend the Act on Counter-Terrorism and Implementing Provisions by including in the catalog of entities cooperating with the Internal Security Agency regarding terrorist incidents – GIIF.

Keywords: Internal Security Agency, cooperating unit, the General Inspector for Financial Information, counteracting money laundering, counteracting financing of terrorism, anti-terrorism, terrorist incidents.

Krzysztof Horosiewicz
Paweł Łabuz
Tomasz Safjański

Działania kontrwykrywcze grup przestępczych ukierunkowane na przeciwdziałanie infiltracji prowadzonej przez Policję z wykorzystaniem osób udzielających jej pomocy

Działania kontrwykrywcze prowadzone przez grupy przestępcze są elementem taktyki i techniki kryminalistycznej. Znaczna ich część nie jest czynami stypizowanymi w prawie karnym, m.in. stosowanie kontrobserwacji czy ochrona korespondencji przestępczej. Jednak niektóre z nich – z prawnokarnego punktu widzenia – są przestępstwami, np. korupcja, fałszowanie dokumentów czy zabójstwa, np. świadków, do których dochodzi w skrajnych przypadkach.

Działania kontrwykrywcze, ukierunkowane na przeciwdziałanie infiltracji grup przestępczych prowadzonej z wykorzystaniem osób udzielających pomocy policji, to wszelkie sposoby utrudniające lub uniemożliwiające organom ścigania działalność agenturalną. W praktyce są to takie poczynania przestępców, których celem jest zapobieżenie przeniknięciu do grupy osób inspirowanych przez policję lub ujawnienie i zidentyfikowanie osób powiązanych z grupą, przekazujących policji informacje o tej grupie przestępczej.

W ostatnich latach u liderów zorganizowanych grup przestępczych zaobserwowano zmianę sposobu myślenia o potrzebie przeciwdziałania infiltracji prowadzonej z udziałem osób udzielających pomocy policji, co sprawiło, że te grupy odnoszą sukcesy. Liderzy poważnie podchodzą do zagadnień ochrony kontrwykrywczej i ci, którzy chcą ich pokonać, muszą to zrozumieć[1].

Już pod koniec VI w. p.n.e. Sun Tzu w traktacie wojskowym *Sztuka wojny* napisał: *Mądrzy władcy i przebiegli dowódcy pokonują przeciwników i dokonują wybitnych czynów, ponieważ z wyprzedzeniem zdobywają wiedzę*[2]. Wskazane tam sugestie są wykorzystywane do dzisiaj w doktrynie wielu armii, przez światowy biznes, policję oraz – co nie powinno budzić zdziwienia – grupy przestępcze. Ujawnione w porę zainteresowanie organów ścigania umożliwia tym grupom przerwanie działalności,

[1] V. Foertsch, *The Role of Counterintelligence in Countering Transnational Organized Crime*, „Trends in Organized Crime" 1999, nr 2, s. 123 i nast.

[2] Sun Tzu, Sun Pin, *Sztuka wojny*, tłum. D. Bakałarz, Gliwice 2004, s. 36, 134.

czasowe zaprzestanie aktywności lub jej przeorientowanie, a także zniszczenie źródeł dowodowych, dzięki czemu zmniejsza się ryzyko rozbicia grupy, poniesienia odpowiedzialności karnej oraz przepadku „owoców przestępstwa". Z perspektywy grupy przestępczej utrzymanie w tajemnicy zarówno popełniania przez nią przestępstw, jak i samego jej istnienia, to czynniki warunkujące jej bezpieczeństwo, co pozwala jednocześnie na uzyskanie i utrzymanie przewagi nad organami ścigania. Opisanie działań kontrwykrywczych grup przestępczych, które przyczyniają się do ograniczenia obserwacji prowadzonej przez policję w ramach działań operacyjnych[3], kontroli operacyjnej oraz procesowej kontroli i utrwalania rozmów[4], pomaga uzmysłowić sobie, że grupy przestępcze podejmują również działania ukierunkowane na przeciwdziałanie infiltracji prowadzonej z wykorzystaniem osobowych źródeł informacji (dalej: OZI).

Użyty w artykule termin kontrwywiad odnosi się do działań podejmowanych przez grupy przestępcze, których celem jest monitorowanie oraz zapobieganie infiltracji[5] ze strony organów ścigania oraz minimalizowanie potencjalnych i realnych zagrożeń dla tych grup.

Problematyka działań kontrwykrywczych podejmowanych przez zorganizowane grupy przestępcze bardzo rzadko jest przedmiotem rozważań naukowych. Trzeba jednak pamiętać, że wszystkie grupy przestępcze (w tym zorganizowane) nie przyglądają się biernie działaniom służb policyjnych i specjalnych[6].

Zgodnie z definicją zawartą w *Słowniku terminów i definicji NATO*, „kontrwywiad" to: *Przedsięwzięcia związane z identyfikacją i przeciwdziałaniem zagrożeniu bezpieczeństwa ze strony wrogich agencji i organizacji wywiadowczych lub osób zaangażowanych w szpiegostwo, sabotaż, dywersje lub terroryzm*[7]. Michael A. Turner stwierdza, że kontrwywiad to przedsięwzięcia analityczne i operacyjne polegające na identyfikowaniu i neutralizowaniu działań obcego wywiadu skierowanych przeciwko własnemu państwu. Do głównych zadań kontrwywiadowczych należą: zapewnianie bezpieczeństwa fizycznego informacji, identyfikowanie i zatrzymywanie własnych obywateli działających na rzecz obcego wywiadu, a także identyfikowanie agentów innych państw prowadzących wrogie działania, jak również próby ich zamiany

[3] Zob. P. Łabuz, T. Safjański, *Działania kontrwykrywcze grup przestępczych ukierunkowane na ograniczenie skuteczności obserwacji prowadzonej w ramach działań operacyjnych*, „Problemy Kryminalistyki" 2017, nr 298, s. 20–27.

[4] Tamże, s. 28–35.

[5] Infiltracja – przenikanie obcych ludzi, wpływów lub ideologii do jakiegoś środowiska, za: *Słownik języka polskiego*, https://sjp.pl/infiltracja [dostęp: 14 II 2019].

[6] Opis licznych powiązań pomiędzy członkami zorganizowanych grup przestępczych, istniejących już w latach 80. XX w., a funkcjonariuszami resortu spraw wewnętrznych przedstawił szczegółowo (m.in. na podstawie materiałów zawartych w zbiorach Instytutu Pamięci Narodowej) S. Latkowski w książce *Polska mafia*, Warszawa 2011.

[7] *AAP-6. Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO*, s. 128, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf, s. 118 [dostęp: 7 II 2019].

w podwójnych agentów lub ściganie ich za szpiegostwo[8]. Jak twierdzi Andrea Groce kontrwywiad, jako działania mające na celu zapobieganie lub uniemożliwianie szpiegowania, zbierania informacji i sabotażu przez obcy podmiot, pełni zarówno funkcję obronną, chroniąc tajniki narodu i majątku przed penetracją obcego wywiadu, jak i funkcję ofensywną, zdobywając informacje o działaniach obcych wywiadów[9]. Z kolei Robert W. Pringle stwierdza, że zadaniami kontrwywiadu, oprócz wcześniej wymienionych, są również dezinformacja, penetracja i udaremnianie wszelkich działań strony przeciwnej, postrzeganych jako zagrożenie państwa[10]. Reasumując, istotą kontrwywiadu są działania, których celem jest identyfikowanie i neutralizowanie obcych działań wywiadowczych.

Kontrwykrywczość w aspekcie kryminalistycznym

Rezultaty działalności wykrywczej organów ścigania i służb państwowych, zarówno krajowych, jak i międzynarodowych, odzwierciedlają m.in. ich profesjonalizm i skuteczność w przeciwdziałaniu, zapobieganiu i zwalczaniu wszelkich form przestępczości. Działalność służb specjalnych[11], wywiadowczych i kontrwywiadowczych, jest oparta – zgodnie z ustawowymi kompetencjami[12] – na pozyskiwaniu, gromadzeniu, przetwarzaniu, analizowaniu i wykorzystywaniu istotnych dla nich informacji o różnym charakterze, w tym kryminalnym.

Wszystkie wymienione czynności służbowe[13], zwłaszcza operacyjno-rozpoznawcze, prowadzone z zastosowaniem wszelkich dostępnych form i metod, podlegają

---

[8] M.A. Turner, *Historical Dictionary of United States Intelligence*, w: *Historical Dictionaries of Intelligence and Counterintelligence*, t. 2, J. Woronoff (red.), Lanham (Maryland)–Toronto–Oxford 2006; także: http://www.lander.odessa.ua/doc/United_States_Intelligence.pdf, s. 41 [dostęp: 7 II 2019].

[9] A. Groce, *Counterintelligence*, 2017, https://usnwc.libguides.com/c.php?g=661096&p=4679144 [dostęp: 7 II 2019].

[10] R. Pringle, *Historical Dictionary of Russian and Soviet Intelligence*, w: *Historical Dictionaries of Intelligence and Counterintelligence*, t. 5, J. Woronoff (red.), Lanham (Maryland)–Toronto–Oxford 2006, s. 57; także: https://www.slideshare.net/Forisson/robert-w-pringle-historical-dictionaries-of-intelligence-and-counterintelligence-series-jon-woronoff-series-editor [dostęp: 7 II 2019].

[11] Zgodnie z art. 11 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (t.j.: DzU z 2020 poz. 27, ze zm.) przez służby specjalne należy rozumieć: Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Służbę Kontrwywiadu Wojskowego, Służbę Wywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne. Przywołana regulacja nie definiuje pojęcia „służba specjalna". Pozostałe organy, służby i instytucje określono mianem „policyjnych".

[12] Ustawy kompetencyjne – akty stanowiące podstawę prawną tworzenia poszczególnych służb specjalnych i policyjnych, w których określa się zasadnicze zagadnienia dotyczące organizacji i funkcjonowania tych służb.

[13] Czynność służbowa – każda czynność mieszcząca się w granicach uprawnień i obowiązków osoby pełniącej funkcję publiczną (przykładowo – funkcjonariusz służb państwowych).

permanentnemu działaniu kontrwykrywczemu stosowanemu przez osoby i podmioty, które są obiektem tych czynności.

W systematyce norm polskiego prawa działalność kontrwykrywcza może się przejawiać w różny sposób, może dotyczyć m.in. jawnych czynności służb państwowych i organów ścigania. Za takie działania uznaje się: utrudnianie prowadzenia czynności dochodzeniowo-śledczych, m.in. przez zastraszanie i nakłanianie do zmian zeznań lub wyjaśnień stron procesowych, niszczenie i ukrywanie materiałów dowodowych, nielegalne (nieuprawnione) pozyskiwanie informacji o planowanych i prowadzonych czynnościach w sprawach oraz informacji zgromadzonych w materiale dowodowym, wpływanie w różny sposób na sędziów, prokuratorów, pełnomocników, funkcjonariuszy realizujących czynności itp.

Wśród działań (przedsięwzięć) kontrwykrywczych istnieje także cała gama czynności techniczno-taktycznych wykorzystywanych w celu przeciwdziałania czynnościom niejawnym (operacyjno-rozpoznawczym) prowadzonym przez uprawnione służby państwowe wobec osób i podmiotów objętych ich zainteresowaniem operacyjnym (rozpracowywanych).

Działalność kontrwykrwycza jest nieodzownym elementem aktywności przestępczej, stanowi jej „filar bezpieczeństwa" i zapewnia grupie bezkarność. Zachowanie daleko idących środków ostrożności oraz stosowanie tzw. samokontroli ma, w przekonaniu członków takiej grupy, gwarantować bezpieczne prowadzenie interesów. Największym osiągnięciem grup przestępczych jest zapewnienie sobie całkowitej anonimowości oraz utajnienie swojej działalności. Opisany system zachowań przestępczych można określić jako technikę i taktykę kontrwykrywczą. Poznanie oraz zdiagnozowanie tych działań przez organy ścigania pozwala na zastosowanie optymalnej techniki i taktyki wykrywczej, zarówno na płaszczyźnie operacyjnej, jak i procesowej.

K o n t r w y k r y w c z o ś ć w znaczeniu przedmiotowym to czynności techniczno-taktyczne polegające na ujawnianiu (dekonspirowaniu[14]) prowadzonych czynności wykrywczo-dowodowych bądź na przeciwdziałaniu im (utrudnianie, unikanie itp.). Do środków technicznych stosowanych podczas działań kontrwykrywczych można zaliczyć wszelkie przedmioty i urządzenia umożliwiające ujawnienie (zidentyfikowanie) prowadzonego równolegle przedsięwzięcia (rzeczowego lub taktycznego) przez służby państwowe lub zakłócenie jego rozpoznania. Stosowana tzw. taktyka przestępcza jest oparta na wypracowanych metodach i zasadach. Wszystkim przedsięwzięciom „wykrywczym" służb państwowych i organów ścigania towarzyszy ich

[14] D e k o n s p i r a c j a – celowe lub nieświadome (czasem przypadkowe) ujawnienie czynności operacyjno-rozpoznawczych (np. niejawnej obserwacji, spotkania z osobowym źródłem informacji, które w świadomości pozostałych członków grupy przestępczej jest przestępcą lojalnym grupie) prowadzonych przez uprawnioną służbę państwową.

maskowanie[15] i legendowanie[16], a także przeciwdziałanie zachowaniom kontrwywiadowczym, o czym będzie mowa w dalszej części artykułu.

Uwarunkowania prawne działalności osobowych źródeł informacji na przykładzie Policji

Zgodnie z art. 1 ust. 2 pkt 3 i 4 *Ustawy z dnia 6 kwietnia 1990 r. o Policji*[17] do podstawowych zadań[18] tej służby należy: wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców, zapobieganie popełnianiu przestępstw i wykroczeń, a także zapobieganie zjawiskom kryminogennym. W myśl art. 14 ust. 1 ustawy o Policji, ta służba – w granicach swoich uprawnień – w celu rozpoznawania i wykrywania przestępstw oraz wykroczeń, a także zapobiegania im, podejmuje czynności dochodzeniowo-śledcze, administracyjno-porządkowe i operacyjno-rozpoznawcze. Czynności operacyjno-rozpoznawcze, określane również jako praca operacyjna, są prowadzone za pomocą ustalonych metod. Według Ewy Gruzy tworzą one zespół powiązanych ze sobą jawnych i niejawnych przedsięwzięć i środków, zastosowanych w sposób mający doprowadzić do osiągnięcia wyznaczonego celu lub wykonania zadania określonego założeniami[19].

W ustawie o Policji, a także w innych ustawach nie podano definicji czynności operacyjno-rozpoznawczych. Przedstawiciele nauk prawnych zajmujący się tą problematyką sformułowali wiele różnych definicji tych czynności. W praktyce stosowanie poszczególnych metod pracy operacyjnej wiąże się zwykle z korzystaniem z tzw. pomocy osób niebędących policjantami, o których mowa w art. 22 ust. 1 ustawy o Policji. W *Zarządzeniu pf-1 Komendanta Głównego Policji z dnia 3 stycznia 2019 r. w sprawie metod i form wykonywania przez Policję czynności operacyjno-rozpoznawczych*[20]

---

[15] Działania maskujące – czynności, których celem jest stworzenie lub wykorzystanie błędnego przeświadczenia osób postronnych co do właściwego znaczenia zdarzeń, przeznaczenia obiektów lub tożsamości osób objętych działaniami policji.

[16] Legendowanie – fałszywe informacje zawierające dane o agencie, tj. jego fałszywą tożsamość, sytuację rodzinną, wykształcenie i zatrudnienie; mogą one zostać wytworzone w krótkim lub dłuższym czasie w zależności od określonej sytuacji operacyjnej.

[17] Tekst jednolity: DzU z 2020 r. poz. 360.

[18] Realizacja tych zadań następuje m.in. na podstawie przepisów: *Ustawy z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (t.j.: DzU z 2020 r. poz. 30, ze zm.), *Ustawy z dnia 24 sierpnia 2001 r. – Kodeks postępowania w sprawach o wykroczenia* (t.j.: DzU z 2019 r. poz. 1120, ze zm.) oraz *Ustawy z dnia 26 października 1982 r. o postępowaniu w sprawach nieletnich* (t.j.: DzU z 2018 r. poz. 969).

[19] Metody pracy operacyjnej – zespół powiązanych ze sobą jawnych i niejawnych przedsięwzięć stosowanych do osiągnięcia wyznaczonego celu lub założonego zadania. Zob. E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2008, s. 64.

[20] Niepublikowane.

wśród tych osób wyodrębniono kilka kategorii osobowych źródeł informacji. Zgodnie z art. 22 ust. 1 ustawy o Policji: *Policja przy wykonywaniu swych zadań może korzystać z pomocy osób niebędących policjantami. Zabronione jest ujawnianie danych o osobie udzielającej pomocy Policji, w zakresie czynności operacyjno-rozpoznawczych*[21]. W przepisie wyraźnie wskazano, że istnieje prawne pozwolenie – na zasadzie *quod lege non prohibitum, licitum est* (czego prawo nie zakazuje, jest dozwolone) – na korzystanie m.in. z pomocy osoby pozyskanej jako osobowe źródło informacji policji. Jest on podstawą prawną współpracy z każdą osobą, np. posłem lub senatorem, niebędącą funkcjonariuszem policji, a pozyskanej jako osobowe źródło informacji. Z tego przepisu wynika również, że osoby udzielające pomocy policji nie mogą być policjantami. Dlatego policjant przekazujący informacje o swoich podejrzeniach czy o przestępstwie nie jest osobowym źródłem informacji w rozumieniu tej ustawy.

Po wnikliwej analizie interpretacyjnej regulacji prawnych[22] dotyczących wszystkich służb państwowych (policyjnych i specjalnych) w Polsce można stwierdzić, że Policja ma najszersze uprawnienia w zakresie pozyskiwania i szeroko pojętej współpracy z OZI, bez ograniczeń statusu zawodowego tych osób.

Obowiązujące, jawne, przepisy prawa nie określają, w jaki sposób dochodzi do werbowania OZI ani w jaki sposób dokumentuje się współpracę z nimi, w tym udzielanie im stosownych pouczeń, m.in. o konieczności zachowania podejmowanych czynności w tajemnicy. Policjant przy wykonywaniu niejawnych czynności służbowych musi poinformować każdą osobę udzielającą mu pomocy o obowiązku zachowania w tajemnicy faktu udzielenia pomocy i wszelkich szczegółów z tym związanych oraz uprzedzić o odpowiedzialności karnej w razie nieuprawnionego ujawnienia informacji stanowiącej tajemnicę państwową lub służbową (obecnie – informację niejawną)[23]. Na tę okoliczność policjant przyjmuje pisemne oświadczenie sporządzone własnoręcznie przez osobę udzielającą pomocy. O konieczności złożenia pisemnego oświadczenia policjant uprzedza taką osobę przed skorzystaniem z jej pomocy.

---

[21] Przewidziany w zdaniu drugim art. 22 ust. 1 ustawy o Policji zakaz ujawniania danych o osobach udzielających pomocy Policji w zakresie czynności operacyjno-rozpoznawczych ma wyłącznie charakter niezupełny względny, a więc przy zachowaniu wymogów określonych prawem jest on możliwy do usunięcia, wyrok Sądu Administracyjnego (dalej: SA) w Łodzi z 24 IX 2009 r., II AKA 140/09, Legalis. Zob. też *Ustawa o Policji – komentarz*, B. Opaliński, M. Rogalski, P. Szustakiewicz (red.), Warszawa 2015.

[22] Ustawy kompetencyjne polskich służb państwowych.

[23] Zgodnie z zapisami *Rozporządzenia Rady Ministrów z dnia 26 lipca 2005 r. w sprawie sposobu postępowania przy wykonywaniu niektórych uprawnień policjantów* (DzU nr 141 poz. 1186 – akt uchylony).
Przywołane rozporządzenie zostało uchylone *Rozporządzeniem Rady Ministrów z dnia 29 września 2015 r. w sprawie postępowania przy wykonywaniu niektórych uprawnień policjantów* (DzU z 2015 r. poz. 1565), które z kolei zostało uchylone *Ustawą z dnia 9 listopada 2017 r. o zmianie ustawy o niektórych uprawnieniach pracowników urzędu obsługującego ministra właściwego do spraw wewnętrznych oraz funkcjonariuszy i pracowników urzędów nadzorowanych przez tego ministra oraz niektórych innych ustaw* (DzU z 2018 r. poz. 106, ze zm.) – przyp. red.

Są to więc działania dobrowolne i OZI musi wyrazić na nie zgodę. Jak już wspomniano, niejawność danych współpracownika policji wynika wprost z art. 22 ust. 1 ustawy o Policji. Te dane będą stanowić materiały niejawne oznaczone klauzulą „ściśle tajne". Wynika to z brzmienia art. 5 ust.1 pkt 5 i 6 *Ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*[24]. W myśl art. 7 tej ustawy dane współpracowników Policji są chronione bez względu na upływ czasu[25].

Osobowe źródła informacji w zależności od charakteru współpracy oraz sposobu pozyskiwania informacji i realizacji zadań można przypisać do różnych kategorii agenturalnych, określanych specjalistycznym nazewnictwem, np.: osoba informująca, informator czy współpracownik. Te kategorie można znaleźć w jawnych przepisach policyjnych[26].

Rola i znaczenie OZI w zwalczaniu przestępczości

Zarówno w przypadku działalności wywiadowczej (wywiad i kontrwywiad), jak i zwalczania przestępczości do pewnych informacji nie sposób dotrzeć bez udziału człowieka, który jest w ich posiadaniu, ma do nich dostęp lub może je zdobyć. Zdaniem Krzysztofa Surdyka pomimo że wiedza pochodząca od źródeł osobowych (tzw. HUMINT, ang. *Human Intelligence*) stanowi od 2 do 5 proc. ogółu informacji uzyskiwanych przez wywiad, to w wielu przypadkach ma ona podstawowe znaczenie[27]. Wiarygodność informacji dostarczanych przez OZI w dużym stopniu zależy od profesjonalizmu osób prowadzących werbunek i dalszą współpracę. Szczególnie istotne jest również to, że korzystanie z pomocy OZI, zarówno podczas zdobywania informacji przez służby wywiadowcze, jak i realizowania przez policję czynności

[24] Tekst jednolity: DzU z 2019 r. poz. 742. Zgodnie z art. 5 ust. 1 ustawy: „Informacjom niejawnym nadaje się klauzulę »ściśle tajne«, jeżeli ich nieuprawnione ujawnienie spowoduje wyjątkowo poważną szkodę dla Rzeczypospolitej Polskiej przez to, że: (…)
5) doprowadzi lub może doprowadzić do identyfikacji funkcjonariuszy, żołnierzy lub pracowników służb odpowiedzialnych za realizację zadań wywiadu lub kontrwywiadu, którzy wykonują czynności operacyjno-rozpoznawcze, jeżeli zagrozi to bezpieczeństwu wykonywanych czynności lub może doprowadzić do identyfikacji osób udzielających im pomocy w tym zakresie;
6) zagrozi lub może zagrozić życiu lub zdrowiu funkcjonariuszy, żołnierzy lub pracowników, którzy wykonują czynności operacyjno-rozpoznawcze, lub osób udzielających im pomocy w tym zakresie".

[25] J. Łyszczek, *Granice legalnej prowokacji w polskim prawie*, s. 22 (materiały niepublikowane).

[26] Zob. *Zarządzenie nr 3 Komendanta Głównego Policji z dnia 18 stycznia 2013 r. zmieniające zarządzenie w sprawie planowania strategicznego, sprawozdawczości i oceny pracy Policji*, załącznik nr 1 (Dz. Urz. KGP poz. 13).

[27] Zob. K. Surdyk, *Wywiad wojskowy jako narzędzie polityki bezpieczeństwa państwa*, http://www.stosunki.pl/?q=content/wywiad-wojskowy-jako-narz%C4%99dzie-polityki-bezpiecze%C5%84stwa-pa%C5%84stwa [dostęp: 18 II 2013].

operacyjnych, pozwala na prowadzenie działań ofensywnych[28]. Jest to związane z tym, że OZI, zdobywając informacje, może działać w sposób aktywny, zadawać pytania i dociekać, a podczas selekcjonowania i porządkowania informacji potrafi formułować sugestie[29]. Funkcjonując w grupie przestępczej, w określonych sytuacjach może również przejmować inicjatywę i przez kreowanie otaczającej rzeczywistości – wpływać na bieg wypadków w sposób pożądany z punktu widzenia strategii i taktyki zadań realizowanych przez policję. Dlatego rzetelną wiedzę o grupach przestępczych i ich działalności oraz, co bardzo ważne, planowanych zamierzeniach można uzyskać dzięki współpracy z OZI. Ten pogląd potwierdzają badania nad czynnikami najbardziej dezorganizującymi i rozbijającymi zorganizowane grupy przestępcze, przeprowadzone przez Zbigniewa Raua wśród świadków koronnych objętych programem ochrony w latach 1998–2009 na podstawie *Ustawy z dnia 25 czerwca 1997 r. o świadku koronnym*[30]. Wynika z nich, że w 2009 r. 65 proc. respondentów z tej grupy wskazało, że elementem najbardziej dezorganizującym działania zorganizowanych grup przestępczych są umieszczani w nich informatorzy policji. W drugiej kolejności (43 proc. wskazań) uznano, że takim czynnikiem jest pozbawienie zysków (konfiskata). Dla porównania – w 2001 r. na te czynniki wskazało odpowiednio: 69 proc. i 74 proc. świadków koronnych. Na dobre wyposażenie techniczne policji jako czynnik dezorganizujący i rozbijający zorganizowane grupy przestępcze wskazało 22 proc. badanych[31].

Współpraca z OZI i pozyskiwanie od nich informacji są stosowane nie tylko do zwalczania zorganizowanych grup przestępczych. Dotyczą także każdej innej pospolitej przestępczości oraz całej gamy infiltracyjno-dezintegrujących przedsięwzięć operacyjnych realizowanych przez policję w sprawach operacyjnych, podejmowanych w ramach kombinacji operacyjnej[32], a dawniej także – gier operacyjnych[33].

---

[28] Z wyjątkiem pasywnego przyjmowania informacji od tzw. osób informujących, które przekazują informacje okazjonalnie, mogą pozostawać anonimowe i którym nie zleca się zadań. Zob. K. Horosiewicz, *Osoby informujące jako wyodrębniona kategoria osobowych źródeł informacji*, „Przegląd Policyjny" 2016, nr 2.

[29] F. Musiał, *Podręcznik bezpieki. Teoria pracy operacyjnej Służby Bezpieczeństwa w świetle wydawnictw resortowych Ministerstwa Spraw Wewnętrznych PRL (1970–1989)*, Kraków 2007, s. 90–91.

[30] Tekst jednolity: DzU z 2016 poz. 1197.

[31] Zob. Z. Rau, *Ocena wykorzystania tajnych metod pracy Policji w kontekście skali społecznej akceptacji ingerencji państwa w sferę prywatności oraz stopień gotowości do współpracy w zwalczaniu przestępczości*, w: *Poczucie bezpieczeństwa obywateli w Polsce. Identyfikacja i przeciwdziałanie współczesnym zagrożeniom*, E.M. Guzik-Makaruk (red.), Warszawa 2011, s. 299.

[32] K o m b i n a c j a o p e r a c y j n a – zaplanowane i przygotowane przedsięwzięcie, realizowane przy użyciu pozostałych metod pracy operacyjnej, wykorzystujące błędne przeświadczenie osób, przeciw którym jest skierowane, co do faktycznego znaczenia zaangażowanych zdarzeń oraz osób w nich występujących, służące osiągnięciu celów pracy operacyjnej. Zob. poselski projekt ustawy o czynnościach operacyjno-rozpoznawczych.

[33] G r a o p e r a c y j n a – najbardziej złożona metoda pracy operacyjnej stanowiąca rodzaj kombinacji operacyjnej charakteryzującej się długofalowością i skomplikowaniem podejmowanych

Nie można mówić o bezpośrednim wykorzystaniu rezultatów takiej współpracy jako dowodu w procesie karnym, jednak współpraca z osobowymi źródłami informacji jako jedna z metod najczęściej używanych w ramach czynności operacyjno-rozpoznawczych dostarcza procesowi karnemu wiedzy, której uzyskanie w inny sposób byłoby utrudnione lub wręcz niemożliwe[34].

Mimo to nie można całkowicie wykluczyć sytuacji, że wyniki czynności operacyjno-rozpoznawczych zostaną – w szczególnych warunkach – bezpośrednio wprowadzone do postępowania dowodowego[35]. W praktyce dotyczy to działań realizonych w ramach tzw. zakupu kontrolowanego.

Charakterystyka przestępczości zorganizowanej

Określenie przestępczość zorganizowana pojawiło się po drugiej wojnie światowej i odnosiło się do międzynarodowych powiązań przestępców działających w poszczególnych krajach ze światem polityki i biznesu oraz do przenikania przestępców do tych sfer życia. W Polsce zwalcza się przestępczość zorganizowaną bez identyfikacji tego zjawiska i bez opisania jego rozmiarów i tendencji. Znamienne jest utożsamianie związku przestępczego z przestępczością zorganizowaną bez względu na to, w jakim przestępstwie ten związek uczestniczy. Jednak nie każde działanie opisywane w art. 258 kk lub 258 § 3 kk jako przejaw przestępczości zorganizowanej jest takim rodzajem przestępczości. To, że grupa osób wspólnie dokonuje przestępstwa, ponieważ tak jest łatwiej i bezpieczniej, nie dowodzi, że mamy do czynienia z przestępczością zorganizowaną. W Polsce przyjęto kryteria identyfikacji zorganizowanej grupy przestępczej oraz przesłanki do wszczęcia wobec niej działań wzorowane na kryteriach wypracowanych przez Europol. Są nimi:

1. Współpraca więcej niż dwóch osób.
2. Wyznaczenie dla każdej z nich określonego zakresu działania w grupie.
3. Dłuższy lub bezterminowy okres współpracy tych osób.
4. Stosowanie wewnętrznej kontroli i środków dyscyplinujących (wewnętrzna i zewnętrzna hermetyczność prowadzonych działań).
5. Podejrzenie popełnienia ciężkich przestępstw.
6. Działanie na płaszczyźnie międzynarodowej.
7. Stosowanie przemocy.

działań. Zob. poselski projekt ustawy o czynnościach operacyjno-rozpoznawczych. W 2003 r. tę metodę pracy operacyjnej usunięto z katalogu działań operacyjno-rozpoznawczych policji. Zob. K. Horosiewicz, *Gra operacyjna, kombinacja operacyjna i dezinformacja jako metody pracy operacyjnej*, „Przegląd Policyjny" 2018, nr 3, s. 45.

[34] K. Horosiewicz, *Współpraca policjantów z osobowymi źródłami informacji*, Warszawa 2015, s. 79–80.

[35] A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006, s. 26.

8. Struktura grupy wzorowana na podmiotach gospodarczych (hierarchiczna), a także pomoc dla członków organizacji i ich rodzin.
9. Zaangażowanie w proces prania brudnych pieniędzy (lokowanie zysków w legalne przedsięwzięcia).
10. Uzyskanie wpływu na gremia polityczne i (lub) gospodarcze, sądownicze, administracyjne.
11. Działanie z chęci zysku i (lub) osiągnięcia wpływu na osoby sprawujące władzę.

Powołane w 1994 r. Biuro do Walki z Przestępczością Zorganizowaną KGP podejmowało działania, gdy stwierdziło, że grupa spełnia przynajmniej osiem takich kryteriów.

Jedną z najważniejszych cech przestępczości zorganizowanej jest jej szybkie dostosowywanie się do zmieniających się warunków, w których działa. Dlatego trudno jest wskazać stałe elementy struktury grupy przestępczej. Ma na nią wpływ wiele zmieniających się czynników[36], nie tylko tych dawno poznanych, jak: zasięg i kierunek działania, skład grupy czy pozycja jej założycieli i liderów. Profesjonalizm w działaniach jest osiągany dzięki poradom i wskazówkom prawników (m.in. adwokatów, radców prawnych), analizie doświadczeń zdobytych przez osoby rozpracowywane i zatrzymane za działalność przestępczą, własnym doświadczeniom zgromadzonym na podstawie obserwacji czynności operacyjnych (m.in.: niejawnej obserwacji, kontroli operacyjnej, transakcji pozornej, ukierunkowanych zadań) stosowanych przez służby.

Volker Foertsch zwrócił uwagę na związki międzynarodowej przestępczości zorganizowanej (ang. *transnational organized crime*, TOC) z agencjami rządowymi i strukturami bezpieczeństwa państwa, które określił mianem symbiozy[37]. Jego zdaniem to zjawisko dotyczy szczególnie tych krajów, na których teren dopiero wchodzą międzynarodowe zorganizowane grupy przestępcze. W początkowym okresie taka grupa działa dyskretnie, aby nie zwracać na siebie uwagi i unikać zagrożeń ze strony służb bezpieczeństwa kraju goszczącego. Jednak wraz ze wzrostem siły ekonomicznej podejmuje działania zmierzające do korumpowania pracowników służb, przenikania do struktur bezpieczeństwa, a następnie do ich kontroli. Z kolei służby bezpieczeństwa państwa, które próbują zwalczać przestępczą organizację, tworzą sojusze z jej poszczególnymi przedstawicielami, upatrując w tym możliwości przeciwdziałania całemu zjawisku. Rezultatem jest rozwój takiej symbiozy. Foertsch dostrzega również podobieństwo międzynarodowych struktur przestępczych do struktur organizacji wywiadowczych i kontrwywiadowczych, a także ich międzynarodowy zasięg[38]. Ponieważ działania kontrwykrywcze grup przestępczych ukierunkowane na przeciwdziałanie infiltracji prowadzonej przez policję przypominają działania kontrwywiadowcze, zostaną omówione przez pryzmat tych działań.

---

[36] Por. W. Mądrzejowski, *Przestępczość zorganizowana – system zwalczania*, Warszawa 2015, s. 55.

[37] S y m b i o z a – okresowe lub stałe współżycie dwóch organizmów (symbiontów) różnych gatunków, przynoszące korzyść co najmniej jednemu z nich, a nieprzynoszące szkód żadnemu, za: https://sjp.pl/symbioza [dostęp: 14 II 2019].

[38] V. Foertsch, *The Role of Counterintelligence in Countering Transnational*…

Typologia działań kontrwykrywczych wykonywanych przez grupy przestępcze ukierunkowanych na przeciwdziałanie infiltracji prowadzonej z wykorzystaniem osobowych źródeł informacji

Podobnie jak podmioty państwowe, również podmioty niepaństwowe, a zwłaszcza organizacje i grupy przestępcze, prowadzą działania kontrwywiadowcze. Te działania nie ograniczają się jedynie do identyfikowania i blokowania kanałów służących organom ścigania do pozyskiwania informacji. Takimi kanałami są źródła osobowe i zdobywanie informacji z wykorzystaniem przedsięwzięć technicznych. Działania kontrwywiadowcze polegają również na zdobywaniu oraz analizowaniu szeroko pojętych informacji o organach ścigania w celu lepszego przygotowania się na wypadek podjęcia przez nie działań wobec grup przestępczych, a także zminimalizowania skutków tych działań. Prowadzenie działań kontrwywiadowczych przez grupy przestępcze wynika z czterech zasadniczych założeń:

1. Grupa przestępcza może być poddana potencjalnej infiltracji przez organy ścigania, co stanowi dla niej realne zagrożenie.
2. Organy ścigania będą usiłowały zdobyć informacje chronione przez grupę przestępczą przez:
   – wykorzystanie osobowych źródeł informacji i podjęcie innych metod pracy operacyjnej, zwłaszcza podsłuchu i obserwacji,
   – identyfikowanie osób wchodzących w skład grupy (lub osób z nią związanych) i nakłanianie ich różnymi sposobami do podjęcia współpracy.
3. Uzyskanie przez organy ścigania informacji o istnieniu grupy przestępczej popełniającej przestępstwa zagrażałoby bezpieczeństwu grupy i jej członkom, utrudniając prowadzenie działań, a w skrajnym przypadku – zmuszając do zaniechania tych działań, co spowodowałoby odcięcie grupy od źródła dochodów.
4. Policja wprowadza do grupy informatorów, co stanowi największe zagrożenie dla istnienia danej grupy.

Można zatem stwierdzić, że jednym z celów działań kontrwywiadowczych grup przestępczych jest przeciwdziałanie potencjalnym i realnym zagrożeniom ze strony organów ścigania[39] dzięki:

- wykrywaniu aktywności organów ścigania skierowanej przeciw grupie przestępczej lub jej działaniom,
- uniemożliwianiu (przeciwdziałaniu) aktywności organów ścigania,
- neutralizacji oraz niweczeniu rezultatów pracy organów ścigania.

W celu przeciwdziałania infiltracji przez osobowe źródła informacji zorganizowane grupy przestępcze dążą do ograniczenia czynników wpływających destrukcyjnie

[39] Por. *Intelligence Practice and Democratic Oversight – a Practitioner's View*, „Occasional Paper" 2003, nr 3, https://www.dcaf.ch/sites/default/files/publications/documents/op03_intelligence-practice.pdf, s. 16 [dostęp: 8 II 2019].

na więzi i zależności pomiędzy swoimi członkami oraz na wewnętrzne funkcjonowanie. Są to działania ukierunkowane m.in. na:

- wzmacnianie identyfikacji z grupą,
- zapewnienie wewnętrznej spójności grupy,
- zaspokojenie indywidualnych potrzeb członków grupy,
- utrzymanie lojalności członków wobec grupy, co przeciwdziała współpracy z organami ścigania,
- docieranie do osób związanych ze służbami zwalczającymi przestępczość zorganizowaną.

Wzmacnianie identyfikacji z grupą jest wynikiem:

- zapewnienia członkom stabilizacji finansowej i wysokiego standardu życia,
- akceptacji społecznej grupy, m.in. w miejscu zamieszkania lub w lokalach, w których bywają członkowie grupy,
- utrzymywania przekonania o wpływach grupy w środowisku przestępczym,
- tworzenia przeświadczenia o „elitarności" grupy,
- odwoływania się do wspólnej symboliki, np. klubu sportowego czy wartości narodowych,
- wzajemnej akceptacji członków grupy,
- utrzymywania przekonania o uznaniu towarzyskim dla lidera grupy.

Wśród działań mających zapewnić wewnętrzną spójność grupy należy wskazać:

- zmuszanie do popełnienia przestępstwa uniemożliwiające skorzystanie ze statusu świadka koronnego,
- unikanie tzw. wałków, czyli uczciwe rozliczanie finansowe wewnątrz grupy,
- unikanie sporów i przestrzeganie hierarchii w grupie,
- prowadzenie dezinformacji na temat rzeczywistej pozycji lidera,
- niedopuszczanie do sytuacji, w której jeden z członków grupy ma zbytnią samodzielność działania,
- unikanie rozgłosu i obnoszenia się z dobrami materialnymi,
- utrzymywanie przekonania, że grupa jest obiektem zainteresowania policji i może być infiltrowana,
- utrzymywanie przekonania, że grupa ma na swoich usługach policjantów, prokuratorów, sędziów,
- podkreślanie zażyłości członków, np. wspólne obchodzenie świąt, wspólne wyjazdy zagraniczne, bycie świadkiem na ślubie,
- właściwy podział zadań przy uwzględnieniu poziomu inteligencji, doświadczenia oraz sprawności psychofizycznej członków grupy.

W ramach zaspokojenia potrzeb indywidualnych członków grupy są podejmowane takie działania, jak m.in. umożliwianie dostępu do środków odurzających.

Utrzymanie lojalności członków wobec grupy i przeciwdziałanie współpracy z organami ścigania wymaga:

- stosowania brutalności wobec nielojalnych członków,
- siły i determinacji w walce z konfidentami,

- kompromitowania rodzin tych członków, którzy poszli na współpracę z policją,
- zapewnienia pomocy prawnej zatrzymanym, podejrzanym lub oskarżonym członkom grupy,
- otaczania opieką rodzin członków grupy, którzy przebywają w aresztach śledczych lub zakładach karnych.

Docieranie do środowisk zwalczających przestępczość zorganizowaną ma zapewnić grupie:

- zdobywanie informacji ze śledztw toczących się wobec jej członków,
- zwiększenie możliwości weryfikacji lojalności członków wobec grupy,
- minimalizowanie strat finansowych związanych z utratą mienia pochodzącego z działalności przestępczej,
- neutralizowanie działań konkurencyjnych grup przestępczych,
- konsultowanie przedsięwzięć przestępczych,
- przedłużanie działań procesowych,
- oddziaływanie na świadków i pokrzywdzonych,
- zdemaskowanie agentury policyjnej.

W celu przeciwdziałania lub neutralizacji infiltracji prowadzonej przez policję przy wykorzystaniu OZI grupy przestępcze rygorystycznie przestrzegają zasady tzw. wiedzy niezbędnej (przekazywanie jedynie niezbędnych informacji potrzebnych do wykonania konkretnego zadania, zarówno w relacjach poziomych – pomiędzy członkami grupy, jak i pionowych – z kierownictwem grupy). Jednocześnie w celu monitorowania i nadawania określonego kierunku i zakresu czynnościom operacyjnym prowadzonym przez policję wykorzystują zwerbowane przez policję źródła informacji, które są wobec niej nielojalne. W rezultacie policja – na podstawie analiz i prognoz otrzymywanych od takiego OZI – podejmuje nieskuteczne przedsięwzięcia lub nie realizuje działań koniecznych, kierując swoje zainteresowanie bądź na obszary niemające istotnego znaczenia, bądź na inne grupy przestępcze, wrogie lub konkurencyjne wobec grupy pozostającej w zainteresowaniu[40].

Podobnie jak w przypadku kontrwywiadu państwowego w działaniach przestępczych ukierunkowanych na przeciwdziałanie lub neutralizację infiltracji prowadzonej przez policję przy wykorzystaniu OZI można wyróżnić dwa główne obszary aktywności: defensywny i ofensywny (aktywny). Działania o charakterze defensywnym polegają na poszukiwaniu środków, które uniemożliwiają uzyskanie dostępu do informacji o grupie przestępczej i jej działalności, nie zwalczają natomiast bezpośrednio zagrożeń wynikających z korzystania przez policję z OZI. Działania kontrwykrywcze o charakterze ofensywnym to określone przedsięwzięcia mające na celu zapobieganie i zwalczanie aktywności OZI policji, a zwłaszcza:

- zbieranie informacji o osobach, miejscach, rodzaju przestępczości, popełnionych przestępstwach itd., które znalazły się w operacyjnym zainteresowaniu policji,

[40] Tamże, s. 17–18.

- neutralizowanie skutków działań OZI realizujących zadania zlecane przez policję (ofensywne przeciwdziałanie infiltracji).

W przypadku działań defensywnych oddanie przez przestępców inicjatywy policji uzależnia ochronę grupy przed infiltracją od profesjonalizmu i skuteczności poczynań policji, co sprowadza się do oczekiwania na popełnienie przez nią błędów, o ile te zostaną w porę dostrzeżone i wykorzystane. Jeżeli jednak policja i OZI wykonujące pracę na jej zlecenie nie popełnią błędów, to tego rodzaju działania ochronne mogą okazać się niewystarczające. Podczas prowadzonego rozpoznania policja zdobywa wiedzę o defensywnych działaniach kontrwykrywczych stosowanych przez grupę i, ucząc się je neutralizować, zwiększa własne szanse na przerwanie działalności przestępczej i dezintegrację grupy. Działania defensywne stosowane przez grupę nie są w stanie wyrządzić policji większej szkody, np. nie dojdzie do dekonspiracji metod wykorzystywanych przez policję lub jej OZI. Stanowi to zachętę dla policji do kontynuowania czynności, ich modyfikowania lub intensyfikowania. W rezultacie działania defensywne są skuteczne jedynie przez krótki czas. Nieuchronność porażki wynikającej z oddania inicjatywy policji, w nadziei, że popełni ona błędy, wymusza na grupach przestępczych konieczność podejmowania działań o charakterze ofensywnym.

Działania ofensywne mają na celu wyprzedzanie aktywności policji. Są one inicjowane przez grupy przestępcze, a ich efektywność zależy w głównej mierze od skuteczności prowadzonych przedsięwzięć, a nie od błędów popełnionych przez policję. Działania ofensywne grup przestępczych polegają przede wszystkim na:

- przenikaniu do struktur policji dzięki:
  - pozyskiwaniu źródeł informacji wśród funkcjonariuszy lub pracowników policji,
  - plasowaniu osób związanych z grupą przestępczą w strukturach policji,
- dezinformowaniu policji.

Wśród ogólnych celów ofensywnych działań kontrwykrywczych można wymienić:

- zdobycie informacji o aktualnym stanie wiedzy policji oraz kierunkach (podmiotach) prowadzonego przez nią rozpoznania,
- rozpoznawanie struktur organizacyjnych policji, jej funkcjonariuszy i pracowników oraz identyfikowanie OZI policji,
- ustalenie metod i środków pracy operacyjnej stosowanych w praktyce przez policję.

Działania kontrwykrywcze grup przestępczych mające charakter ofensywny, podobnie jak działania kontrwywiadowcze, umożliwiają w sprzyjających okolicznościach jednoczesne:

- kontrolowanie działań operacyjnych prowadzonych przez policję i ich udaremnianie,
- zbieranie cennych informacji o policji i stosowanie wobec niej skutecznej dezinformacji.

Dezinformowanie policji jest możliwe dzięki prowadzeniu czynności podobnych do działań określanych w nomenklaturze wywiadu jako gra operacyjna. W ogólnym

ujęciu celem gry operacyjnej jest stworzenie sytuacji, w której przeciwnik nie jest świadomy tego, że bierze udział w działaniach mających na celu udaremnienie jego operacji wywiadowczych. Dzięki temu jego wysiłki stają się nieskuteczne, a nawet – w pewnych przypadkach – wręcz szkodliwe. Elementem warunkującym prowadzenie gry operacyjnej jest tzw. podwójny agent. Podkreślając znaczenie podwójnych agentów i wykorzystywanie ich do dezinformowania przeciwnika, Sun Tzu pisał:

> Trzeba poszukiwać agentów przeciwnika, którzy przybyli nas szpiegować. Kuś ich zyskami, pouczaj i nie wypuszczaj z ręki. W taki sposób pozyskuje się podwójnych agentów. Dzięki zdobytej od nich wiedzy możesz rekrutować szpiegów lokalnych i wewnętrznych. Dzięki zdobytej od nich wiedzy szpiedzy jednorazowi mogą rozgłaszać fałszywe informacje i dezinformować przeciwnika. Dzięki zdobytej od nich wiedzy, gdy nadejdzie czas, będziesz mógł zatrudnić żywych szpiegów. Władca musi znać tych pięć aspektów działalności wywiadowczej. Od takiej wiedzy zależy nawracanie szpiegów; trzeba więc być szczodrym dla podwójnych agentów[41].

Klasyczną metodą pozyskania podwójnego agenta jest wykrycie agenta wywiadu przeciwnika i tzw. odwrócenie go. Podstawowym czynnikiem jest motywacja, która skłoniła go do podjęcia współpracy z wywiadem przeciwnika. Szanse na „odwrócenie" agenta są większe w sytuacji, gdy motywem podjęcia współpracy jest szantaż lub chęć zysku, a mniejsze w przypadku motywacji ideologicznych lub osobistych. Z uwagi na istniejące analogie do działań kontrwywiadowczych niniejsze rozważania zostaną ograniczone do tzw. jednostronnej gry operacyjnej kontrwywiadu.

Podjęcie gry operacyjnej może przebiegać w dwóch wariantach. W pierwszym przeciwnik nie wie, że osoba pozyskana przez niego jest w rzeczywistości tajnym współpracownikiem lub funkcjonariuszem kontrwywiadu, który, działając pod odpowiednią legendą, został mu podsunięty jako tzw. wabik, albo gdy taka osoba, występując jako tzw. oferent, nawiązuje kontakt z kontrwywiadem z własnej inicjatywy[42]. W drugim wariancie to kontrwywiad proponuje współpracę konkretnej osobie. Za wiedzą i zgodą kontrwywiadu osoba zwerbowana rozpoczyna pracę dla obcej służby specjalnej pod nadzorem służb kontrwywiadowczych własnego państwa, stając się w rzeczywistości podwójnym agentem. Korzystanie z pomocy podwójnych agentów w sprzyjających okolicznościach umożliwia jednoczesne: kontrolowanie i udaremnianie działań operacyjnych prowadzonych m.in. przez policję, zbieranie istotnych informacji oraz skuteczne jej dezinformowanie.

Według *Słownika terminów i definicji NATO* dezinformacja to przedsięwzięcia mające na celu wprowadzenie przeciwnika w błąd przez manipulowanie,

---

[41] Sun Tzu, Sun Pin, *Sztuka wojny*…, s. 135–136.

[42] Nawiązanie współpracy z oferentem niesie za sobą wiele zagrożeń. Jeżeli oferentem jest agent pracujący dla obcego wywiadu, który sam zgłasza się jako chętny do współpracy, jest to przykład jednostronnej gry operacyjnej. Dlatego też wiele służb odrzuca złożoną im propozycję współpracy. Najważniejsze jest ustalenie rzeczywistych zamiarów oferenta, jego motywacji, a także porównanie stanu wiedzy oferenta z własnymi informacjami i przeprowadzonymi analizami.

działania pozorujące i preparowanie dowodów, prowokujące działania szkodzące jego własnym interesom[43]. Dezinformacja może mieć wymiar krótkofalowy (tzw. dezinformacja taktyczna) lub długotrwały (tzw. dezinformacja strategiczna). Dezinformacja taktyczna jest prowadzona stosunkowo krótko (kilka dni lub tygodni), a jej celem jest wprowadzenie policji w błąd w jednej lub – ewentualnie – w kilku związanych ze sobą sprawach. Dezinformacja strategiczna to systematyczne przekazywanie fałszywych informacji w celu wykreowania pożądanego obrazu rzeczywistości, a w rezultacie – błędnej oceny sytuacji. Zgodnie ze słowami Ralpha Francisa Benneta, że: (…) *wróg może zostać przekonany do użytecznego błędu tylko wtedy, gdy karmiono go dezinformacją opartą na wiedzy, którą już posiadał, chociaż subtelnie od niej odbiegającą*[44], skuteczna dezinformacja jest możliwa jedynie wówczas, kiedy jest zgodna z wiedzą, którą policja dysponowała wcześniej, czyli gdy fałszywa informacja jest prawdopodobna. W wielu przypadkach podjęcie gry operacyjnej z policją, której skutkiem jest jej dezinformowanie, to rezultat źle przeprowadzonego werbunku – werbowany tylko pozornie zgadza się na podjęcie współpracy z policją. Zwykle do takiej sytuacji dochodzi podczas tzw. werbunku okazjonalnego lub gdy inicjatywa nawiązania kontaktu leży po stronie osoby oferującej współpracę. Przy werbunku okazjonalnym pozornie zawerbowane źródło ujawnia próbę werbunku grupie przestępczej i, w zależności od sytuacji, za jej zgodą podejmuje grę operacyjną. W drugim – oferent, działając z własnej inicjatywy lub realizując zadania zaplanowane przez grupę, przekazuje prawdziwe i niekiedy wartościowe informacje. Jednak w obydwu sytuacjach źródło informacji można (pod pewnymi warunkami) określić mianem „podwójnego agenta". Przekazuje ono bowiem informacje o „konkurencji" lub informacje ogólnikowe, w rzeczywistości uzyskując informacje o metodach działania i zamierzeniach policji. Przykładem może być źle poprowadzona rozmowa (wywiad) podczas spotkania ze źródłem, które zdobytymi informacjami dzieli się następnie z grupą przestępczą lub wykorzystuje je do własnych celów.

Podsumowując, w ramach działań o charakterze defensywnym grupy przestępcze prowadzą analizę:

- sekwencji poszczególnych zatrzymań i innych czynności procesowych oraz łączących je związków przyczynowo-skutkowych;
- okoliczności, w których doszło do wprowadzenia w krąg osób związanych z grupą osoby, która w procesie otrzymała status świadka incognito (w tym osoby, która okazała się policjantem pod przykryciem), oraz analizę osób ją wprowadzających;
- wiedzy, jaką mogli dysponować poszczególni członkowie grupy o miejscu ukrycia dowodów (m.in. narzędziach, przedmiotach pochodzących z przestępstwa

[43] *AAP-6. Słownik terminów i definicji NATO zawierający wojskowe terminy i ich definicje stosowane w NATO*, https://wcnjik.wp.mil.pl/u/AAP6PL.pdf, s. 128 [dostęp: 7 II 2019].

[44] R.F. Bennett, *Behind the Battle: Intelligence in the War with Germany, 1939–45*, London 1994, s. 70.

lub służących do ich popełniania) oraz miejscu przebywania osób, wobec których policja rozpoczęła czynności procesowe;
- obszaru prywatnego przestępców, m.in.: stanu posiadania (mieszkanie, samochód, prowadzona działalność, sklepy, warsztaty), przy założeniu, że zarówno proces karny, jak i pobyt w areszcie śledczym lub zakładzie karnym generują straty (pozbawienie zysków, koszt wynajęcia adwokata, koszt pobytu w zakładzie karnym). Liczba zatrzymań i aresztowań danej osoby, która odbiega od zatrzymań pozostałych członków grupy, czy lepsza sytuacja materialna pozwalają – zdaniem innych przestępców – podejrzewać, że powodem mniej dolegliwego traktowania danej osoby przez policję jest udzielanie przez nią pomocy policji;
- lokalizacji telefonów członków grupy w celu ustalenia, gdzie i kiedy przebywali oraz którymi trasami się poruszali;
- przebiegu ewentualnego pobytu członka grupy w areszcie śledczym lub zakładzie karnym (grypsujący, niegrypsujący, odwiedziny, pomoc udzielana z zewnątrz, wysokość tzw. wypiski, pełnione funkcje – np. kalifaktor, fryzjer, kontakty z ochroną placówki);
- procesu przekazywania informacji przez ewentualnych informatorów policji. Zapobieganie temu zjawisku polega na uniemożliwianiu monitorowania położenia telefonów członków grupy, m.in. wyłączanie telefonów, gromadzenie ich i pozostawianie w bezpiecznym miejscu, np. w lodówce (klatka Faradaya), przechowalni bagażu czy samochodzie;
- rygorystycznego przestrzegania zasady tzw. wiedzy niezbędnej, spowodowanego wspólnym interesem zarówno grupy (bezpieczeństwo), jak i poszczególnych jej członków (eliminacja zagrożeń wynikających ze znalezienia się w kręgu osób branych pod uwagę jako źródło przecieku).

Wśród działań o charakterze ofensywnym można wymienić:
- plasowanie informatorów grupy w policji (jako pracowników lub funkcjonariuszy)[45];
- pozyskiwanie informacji od policjantów i pracowników organów ścigania dzięki:
  - korupcji,
  - szantażowi[46],
  - więzom rodzinnym lub towarzyskim z członkami grup przestępczych[47];

[45] Przyjęcie do policji członka grupy przestępczej, opłacanego dodatkowo przez grupę, która inwestuje w jego rozwój w oczekiwaniu, aż zajmie on stanowisko zapewniające dostęp do potrzebnych informacji.

[46] Na przykład wiedza o tym, że policjant lub pracownik zaopatruje się w wyroby bez akcyzy, narkotyki, przedmioty pochodzące z przestępstwa (elektronika, części i akcesoria samochodowe), bywa w agencjach towarzyskich (zdjęcia i filmy dostępne w internecie po wykupieniu haseł dostępowych, informacje od właścicieli takich lokali), jest hazardzistą.

[47] Znajomość osób z grupy przestępczej z policjantem z tzw. podwórka, ze szkoły, klubu sportowego

- korzystanie z pomocy pracowników salonów sieci telefonii komórkowej (stosowanie korupcji, szantażu bądź po nawiązaniu znajomości) do analizowania bilingów i innych ustaleń dotyczących członków grupy;
- celowe przekazywanie odmiennych informacji wybranym członkom grupy, a następnie sprawdzanie, która z wersji informacji dotarła do funkcjonariuszy policji. W tym celu wykorzystuje się zaprzyjaźnione z grupą osoby, np. paserów, taksówkarzy, właścicieli agencji towarzyskich, przedstawicieli banków, bądź monitoring – istniejący lub zainstalowany w ramach tego przedsięwzięcia. W innym wariancie członkom grupy ujawnia się np. miejsce planowanej transakcji narkotykowej, z tym że poszczególnym członkom grupy podaje się różne godziny jej przeprowadzenia. Miejsce transakcji jest obserwowane i gdy przed określoną godziną pojawią się osoby identyfikowane jako policjanci, znana staje się tożsamość osoby, która przekazała informację policji.

Osoby współpracujące z grupą przestępczą mogą zostać celowo uplasowane w miejscach (np. stacje szyfrów[48], oddziały kancelarii tajnych[49]), w których mają dostęp do newralgicznych, z punktu widzenia ochrony, informacji, otrzymują określone uprawnienia dostępu do policyjnych baz danych, np. do tzw. zastrzeżeń koordynacyjnych, bądź też mogą wykorzystywać kontakt z osobami, które mają takie możliwości.

Legalna prowokacja policyjna a prowokacja przestępcza

W art. 19a ust. 1 i 2 ustawy o Policji ustawodawca zezwolił, w ramach prowadzonych czynności operacyjno-rozpoznawczych, na przeprowadzenie w sposób niejawny legalnej prowokacji. Ten termin odnosi się do wielu różnych czynności, opisanych w tym artykule, wymagających odmiennych zachowań podejmowanych w celu sprawdzenia wcześniej uzyskanych wiarygodnych informacji o przestępstwie. P r o w o k a c j a polega na wprowadzeniu w błąd lub wykorzystaniu błędnego przeświadczenia prowokowanego m.in. co do znaczenia faktów. Prowokację można realizować tylko w określonym celu. Takie wprowadzenie w błąd jest wysoce niebezpieczne z uwagi na możliwość ujawnienia (dekonspiracji) działań operacyjnych policji.

(„od rzemyczka do koniczka"), związana z wykonywanym zajęciem zarobkowym (praca na tzw. bramce, praca w firmie zarejestrowanej na żonę, krewnego itp.); relacja polega na nawiązaniu kontaktu z policjantem i prośbie o „pomoc" lub „o sprawdzenie kogoś".

[48] Proceder ujawniony w 1999 r. w jednym z ówczesnych wydziałów do walki z przestępczością zorganizowaną przy okazji jednej z prowadzonych spraw. Dowody w postaci nagrań z kontroli operacyjnej przekazywano do ówczesnego Inspektoratu KWP z prośbą o niepodejmowanie działań do chwili tzw. realizacji sprawy. Po czasie okazało się, że z uwagi na upływ 12 miesięcy od chwili zakończenia kontroli operacyjnej policjanci Inspektoratu dokonali zniszczenia materiałów.

[49] W 2008 r. uzyskano informacje, że jedna z pracownic oddziału kancelarii tajnej (zarabiająca ok. 1200 zł netto) jest widywana w towarzystwie figurantów spraw operacyjnych.

Wszystkie wymienione czynności mają cechy wspólne – są prowadzone niejawnie, a przy ich realizowaniu wykorzystuje się elementy podstępu. Czynności prowokacyjne są podejmowane w celu spowodowania oczekiwanego zachowania się osoby, wobec której je podjęto, i służą sprawdzeniu wiarygodnych informacji o popełnionym przestępstwie. Tego rodzaju działania, a przynajmniej większość z nich, mają na celu albo doprowadzenie do popełnienia przestępstwa przez osobę prowokowaną, albo sprowokowanie innego zachowania, które ma znaczenie dla przyszłego lub toczącego się procesu karnego. Prowokowanie jest zatem działaniem zmierzającym do wywołania określonego i oczekiwanego przez policję zachowania, które można zweryfikować[50].

Policja współpracująca z OZI nie może dopuścić do zidentyfikowania takiej osoby i ujawnienia współpracy z nią (spotkań, zlecanych zadań, pozyskiwania informacji itp.). Taktyka takich zachowań jest złożoną procedurą maskująco-legendującą (o których wcześniej wspomniano) w celu zapewnienia bezpieczeństwa osobom oraz przedsięwzięciom operacyjno-rozpoznawczym.

Grupy przestępcze od dawna mają świadomość, jakie znaczenie ma wykorzystywanie przez policję metod operacyjnych. Niezbędne dla nich są informacje o czasie, rodzaju i miejscu stosowania konkretnej metody operacyjnej wobec osób, miejsc lub rzeczy związanych z ich działalnością przestępczą. W celu identyfikacji zagrożenia niejednokrotnie wykorzystuje się zachowania prowokujące, służące kontroli. Przykładem może być stosowanie niejawnej obserwacji, kamuflowania i szyfrowania treści przekazu m.in. wobec osób nowo poznanych lub wykazujących ponadprzeciętną inicjatywę i zainteresowanie działalnością przestępczą grupy.

Bardzo istotne w taktyce przestępczej kontrwykrywczości jest uniemożliwienie służbom policyjnym pozyskania wybranego członka grupy jako potencjalnego źródła informacji oraz pośredniego lub bezpośredniego wprowadzenia do grupy kwalifikowanego OZI. W tym celu świadomość organizatorów grupy oraz jej pozostałych członków jest ukierunkowana na permanentną kontrolę i weryfikację osób, których historia życia jest niepotwierdzona i nieugruntowana. Każda osoba niepopełniająca wspólnie z nimi przestępstw, zarówno w przeszłości, jak i planowanych, może być odbierana negatywnie z uwagi na unikanie bezkarności. Przykładowo, usiłowanie popełnienia zbrodni zabójstwa, popełnienie takiej zbrodni lub współudział w niej uniemożliwia takiej osobie potencjalną współpracę z organami ścigania jako „świadek koronny”[51]. Dla zorganizowanych grup przestępczych zajmujących się przestępczością narkotykową charakterystyczne jest zjawisko ograniczania wiedzy

[50] Por. J. Łyszczek, *Granice legalnej prowokacji*…, s. 22.

[51] *Ustawa z dnia 25 czerwca 1997 r. o świadku koronnym* (t.j.: DzU z 2016 r. poz. 1197), art. 4: „Przepisów ustawy nie stosuje się do podejrzanego, który w związku z udziałem w przestępstwie lub przestępstwie skarbowym określonym w art. 1:
1) usiłował popełnić albo popełnił zbrodnię zabójstwa lub współdziałał w popełnieniu takiej zbrodni; 2) nakłaniał inną osobę do popełnienia czynu zabronionego, określonego w art. 1, w celu skierowania przeciwko niej postępowania karnego; 3) kierował zorganizowaną grupą albo związkiem mającymi na celu popełnienie przestępstwa lub przestępstwa skarbowego”.

poszczególnych członków grupy o innych członkach, w tym o liderach grupy (ich dane lub osobisty kontakt z nimi), o miejscach zaopatrywania (dane dostawców, producentów) czy przechowywania towaru, a także o pełnej strukturze grupy i lokowaniu (legalizacji) zysków finansowych pochodzących z działalności przestępczej. Takie zachowania gwarantują przestępcom, że nawet w przypadku dobrze uplasowanego w grupie OZI[52] ma ono ograniczone możliwości pozyskiwania wartościowych informacji, zarówno o samej grupie, jak i jej działalności. W przypadku rozbicia grupy przestępczej i zatrzymania jej członków, takie zachowania kontrwykrywcze uniemożliwiają pozyskanie któregoś z członków grupy do współpracy procesowej (art. 60 kk), z uwagi na brak wiedzy procesowej takiej osoby. Najczęściej ma ona wiedzę jedynie na temat własnych poczynań, m.in. odbierania narkotyków od innej, nieznanej jej osoby i przekazywania ich kolejnej nieznanej osobie.

Grupy przestępcze w celu uniknięcia typowej legalnej prowokacji policyjnej wykorzystują błędne przeświadczenie osób podejrzewanych o współpracę co do prawdziwego znaczenia zdarzeń oraz roli osób w nie zaangażowanych, służące osiągnięciu celów pracy operacyjnej, np. kombinacji operacyjnej. Są to sprawdzone i skuteczne kontrolno-ochronne „zasady kontrwykrywcze". Przykładowym zachowaniem taktycznym stosowanym przez organizacje przestępcze jest „wiązanie" członków grupy, czyli obowiązek uczestnictwa (współuczestnictwa) osoby, która dała „referencje" nowo poznanym osobom, w każdym spotkaniu (transakcji przestępczej), co wyklucza i tym samym uniemożliwia wdrożenie jakichkolwiek czynności[53] w trybie art. 19 ustawy o Policji. W przypadkach „bezreferencyjnego", czyli bez udziału OZI, wdrożenia czynności w trybie art. 19 ustawy o Policji, grupy przestępcze mają świadomość „formalizmu" czynności służbowych, czyli konieczności uzyskania przez policję pisemnych wniosków o realizację przedmiotowych czynności, zatwierdzonych przez różne organy, tj. prokuratury, sądy. Grupy przestępcze w celu „weryfikacji przestępczej" potencjalnego kontrahenta stanowczo domagają się przeprowadzenia transakcji „natychmiast", bez możliwości tzw. zwłoki w czasie.

Zakończenie

Od kilkunastu lat jest widoczne obniżenie poziomu pracy operacyjnej służb policyjnych oraz częstsze korzystanie z tzw. technicznych środków wsparcia pracy operacyjnej. W celach wykrywczych policja coraz powszechniej korzysta z danych telekomunikacyjnych oraz danych z monitoringu. Te zmiany przypominają ewoluowanie

[52] Plasowanie źródła – przedstawienie grupom przestępczym osoby godnej zaufania i wywołania w umyśle jej członków wrażenia „bezpiecznego" kontaktu przestępczego oraz braku jakichkolwiek podejrzeń, że jest to osoba współpracująca ze służbami państwowymi; tym samym jest ona „dobrze rozumiana i odbierana".

[53] Artykuł 19a ustawy o Policji dotyczy różnych zachowań określanych potocznie jako „prowokacja policyjna" (tzw. zakup kontrolowany, kontrolowane wręczenie łapówki).

metod stosowanych przez służby wywiadowcze w systemie rozpoznania po okresie zimnej wojny. Zaczęły wówczas dominować nowoczesne rozwiązania technologiczne – SIGINT oraz IMINT, a HUMINT uznano za przestarzały i mało efektywny.

Po zamachach z 11 września 2011 r. zrozumiano, że system rozpoznania zagrożeń musi zostać zmieniony. W przypadku walki z przestępczością zorganizowaną pomocne dla grup przestępczych są informacje o metodach działania oraz technologiach wykorzystywanych przez organy ścigania, zaczerpnięte przede wszystkim z portali internetowych (np. Niebezpiecznik) lub przekazywanych – świadomie lub nieświadomie – przez aktualnych lub byłych przedstawicieli organów ścigania, w tym detektywów czy właścicieli sklepów ze sprzętem szpiegowskim. Również coraz szerszy dostęp do wiedzy o nowoczesnych technologiach umożliwia neutralizowanie wysiłków organów ścigania, co powoduje, że stosowane przez nie środki są nieskuteczne lub nieprzydatne. Wymusza to na policji powrót do bardziej konwencjonalnych metod zdobywania informacji, a szczególnie – do korzystania z pomocy osobowych źródeł informacji. Równolegle grupy przestępcze, zakładając podejmowanie przez organy ścigania prób infiltracji z wykorzystaniem OZI, w celu przeciwdziałania im stosują przedsięwzięcia kontrwykrywcze. Domeną tych działań jest infiltracja organów ścigania oraz rozpoznanie ich aktualnych przedsięwzięć i zamiarów. Ta wiedza umożliwia przestępcom przewidywanie kolejnych operacji organów ścigania i ich neutralizowanie. Taka sytuacja uzmysławia funkcjonariuszom organów ścigania, że realizowane przez nich czynności operacyjne są narażone na dekonspirację i mogą skończyć się niepowodzeniem oraz że istnieje pewien zakres informacji szczególnie chronionych przez grupy przestępcze, których zdobycie nie zawsze jest możliwe.

Wszelkie przedsięwzięcia kontrwykrywcze stanowią otwarty katalog czynności taktyczno-technicznych, które na bieżąco ewoluują równolegle do rozwijanych czynności wykrywczo-dowodowych.

Bibliografia

Bennett R.F., *Behind the Battle: Intelligence in the War with Germany*, *1939–45*, London 1994, Sinclair-Stevenson.

Groce A., *Counterintelligence*, 2017, U.S. Naval War College, https://usnwc.libguides.com/c.php?g=661096&p=4679144 [dostęp: 7 II 2019].

Foertsch V., *The Role of Counterintelligence in Countering Transnational Organized Crime*, „Trends in Organized Crime" 1999, nr 2, s. 123–142.

Horosiewicz K., *Osoby informujące jako wyodrębniona kategoria osobowych źródeł informacji*, „Przegląd Policyjny" 2016, nr 2, s. 68–78.

Horosiewicz K., *Współpraca policjantów z osobowymi źródłami informacji*, Warszawa 2015, Wolters Kluwer.

Intelligence Practice and Democratic Oversight – a Practitioner's View, „Occasional Paper" 2003, nr 3, https://www.dcaf.ch/sites/default/files/publications/documents/op03_intelligence-practice.pdf [dostęp: 8 II 2019].

Łabuz P., *Zakup kontrolowany jako narzędzie w zwalczaniu przestępczości zorganizowanej*, „Forum Prawnicze" 2012, nr 3, 54–62.

Łabuz P., Safjański T., *Działania kontrwykrywcze grup przestępczych ukierunkowane na ograniczenie skuteczności kontroli operacyjnej oraz procesowej kontroli i utrwalania rozmów*, „Problemy Kryminalistyki" 2017, nr 297, s. 28–35.

Łabuz P., Safjański T., *Działania kontrwykrywcze grup przestępczych ukierunkowane na ograniczenie skuteczności obserwacji prowadzonej w ramach działań operacyjnych*, „Problemy Kryminalistyki" 2017, nr 298, s. 20–27.

Łyszczek J., *Granice legalnej prowokacji w polskim prawie*, materiały niepublikowane.

Mądrzejowski W., *Przestępczość zorganizowana – system zwalczania*, Warszawa 2015, Editions Spotkania.

Musiał F., *Podręcznik bezpieki. Teoria pracy operacyjnej Służby Bezpieczeństwa w świetle wydawnictw resortowych Ministerstwa Spraw Wewnętrznych PRL (1970–1989)*, Kraków 2007, IPN.

Pringle R.W., *Historical Dictionary of Russian and Soviet Intelligence*, w: *Historical Dictionaries of Intelligence and Counterintelligence*, t. 5, J. Woronoff (red.), Lanham (Maryland)–Toronto–Oxford 2006.

Rau Z., *Ocena wykorzystania tajnych metod pracy Policji w kontekście skali społecznej akceptacji ingerencji państwa w sferę prywatności oraz stopień gotowości do współpracy w zwalczaniu przestępczości*, w: *Poczucie bezpieczeństwa obywateli w Polsce. Identyfikacja i przeciwdziałanie współczesnym zagrożeniom*, E.M. Guzik-Makaruk (red.), Warszawa 2011, Wolters Kluwer.

Surdyk K., *Wywiad wojskowy jako narzędzie polityki bezpieczeństwa państwa*, http://www.stosunki.pl/?q=content/wywiad-wojskowy-jako-narz%C4%99dzie-polityki-bezpiecze%C5%84stwa-pa%C5%84stwa [dostęp:18 II 2013].

Turner M.A., *Historical Dictionary of United States Intelligence*, w: *Historical Dictionaries of Intelligence and Counterintelligence*, t. 2, J. Woronoff (red.), Lanham (Maryland)–Toronto–Oxford 2006, The Scarecrow Press.

Abstrakt

W artykule omówiono działalność kontrwykrywczą w aspekcie taktyki przestępczej, ukierunkowanej na identyfikację i rozpoznanie osobowych źródeł informacji udzielają-

cych pomocy policji. Podstawowym celem tej działalności jest zapobieganie infiltracji wywiadowczej grup przestępczych. Autorzy wyjaśniają pojęcie „kontrwykrywczość", a także analizują uwarunkowania prawne i procedury operacyjne służb specjalnych i policyjnych z wykorzystaniem osób udzielających im pomocy w kontekście szeroko pojętego zwalczania przestępczości.

Słowa kluczowe: osobowe źródło informacji, czynności operacyjno-rozpoznawcze, kontrwykrywczość, policja, zwalczanie przestępczości, przestępczość zorganizowana.

Abstract

The article discusses the issue of counter-detecting activities in the aspect of criminal tactics aimed at identifying personal sources of information providing assistance to the police. The primary goal of these ventures is to prevent the intelligence infiltration of criminal groups. The authors explain the notion of "counter-detection" as well as the legal conditions and operational procedures of special and police services with the use of persons providing them with intelligence assistance in the broadly understood scope of combating crime throughout its entire phenomenon spectrum.

Keywords: personal source of information, operational and reconnaissance activities, counter-detection, police, combating crime, organized crime.

Bartosz Jagodziński

Działania i rozwój jednostek specjalnych

Planowanie rozwoju[1] jednostek specjalnych uwzględnia przede wszystkim udoskonalanie podstawowych elementów, które są wspólne dla wszystkich rodzajów tego typu formacji (zarówno w kraju, jak i za granicą). Można do nich zaliczyć:

1) utrzymywanie strat własnych na niskim poziomie, z zachowaniem zdolności bojowej podczas operacji na terytorium wroga;
2) podnoszenie zdolności do ograniczania wpływów nieprzyjaciela wśród ludności cywilnej na obszarze działań;
3) mobilność działań w skrajnie trudnych warunkach, uzyskiwaną przez podnoszenie umiejętności prowadzenia operacji bojowych na lądzie, morzu i w powietrzu (wszędzie tam, gdzie wojska konwencjonalne z różnych przyczyn nie mogą prowadzić operacji);
4) werbowanie żołnierzy sił specjalnych oraz rozwijanie u nich zdolności przywódczych, w tym efektywniejszą rekrutację, selekcję oraz profesjonalne szkolenie, a także oferowanie atrakcyjnych perspektyw członkom kadry dowódczej tych sił;
5) skuteczniejsze wykorzystywanie technologii informacyjnych podczas realizacji różnych zadań specjalnych;
6) udoskonalanie struktur organizacyjnych jednostek specjalnych w celu poprawy współdziałania z regularnymi formacjami wojskowymi, a także krajowymi i międzynarodowymi organizacjami zajmującymi się problemami bezpieczeństwa;
7) wykorzystywanie na jeszcze większą skalę urządzeń satelitarnych i bezzałogowych statków latających w celu usprawnienia działań wywiadowczych;
8) efektywniejsze wykorzystywanie najnowszych zdobyczy techniki niezbędnych do prowadzenia dalekiego rozpoznania i precyzyjniejszej oceny warunków prowadzenia akcji bojowych;
9) rozwój broni o wszechstronnym zastosowaniu.

Jednostki specjalne dzielimy na:

1) lądowe oddziały specjalne,
2) jednostki antyterrorystyczne,

[1] A. Stilwell, *Jednostki specjalne w akcji. Afganistan, Afryka, Bałkany, Irak, Ameryka Południowa*, Warszawa 2009, s. 170.

3) morskie oddziały specjalne,
4) powietrzne oddziały specjalne[2].

Wszystkie wyżej wymienione formacje są powoływane do wykonywania specyficznych zadań z zakresu bezpieczeństwa wewnętrznego oraz międzynarodowego danego państwa. Zadania takich jednostek, jak np. Jednostka Wojskowa GROM (dalej: JW GROM), Navy Seal, Delta Force lub SAS, są bardzo szerokie (z uwagi na ich mobilność, charakter i strefy działania). Jednak nawet wśród nich można wskazać jednostki, które zajmują się tylko i wyłącznie operacjami związanymi z realizacją zadań antyterrorystycznych i kontrterrorystycznych[3].

Mianem jednostek kontrterrorystycznych określa się jednostki specjalne, zarówno wojskowe, jak i policyjne, przeznaczone i wyszkolone do prowadzenia działań związanych z ratowaniem zakładników oraz odbijaniem obiektów stałych i środków transportu zajętych przez wrogie siły. Dodatkowo wyróżnia się tu jednostki wyspecjalizowane w zadaniach związanych wyłącznie z ratowaniem zakładników, tj. *hostage rescue force* – HRF (Jednostka Ratowania Zakładników)[4] lub *hostage rescue operations* – HRO (operacje związane z ratowaniem zakładników).

JW GROM została utworzona jako Hostage Rescue Operations. Będąc strukturą wyspecjalizowaną m.in. w prowadzeniu działań antyterrorystycznych, wkracza do akcji w odpowiedzi na zamach terrorystyczny lub w przypadkach, gdy formacje policyjne nie dysponują wystarczającymi środkami i wiedzą. Natomiast Jednostka Wojskowa Komandosów (dalej: JW Komandosów) została utworzona z myślą o realizacji typowo wojskowych działań specjalnych. Najwięcej spekulacji jest związanych z przeznaczeniem i rozwojem właśnie JW GROM i JW Komandosów. Od kilku lat bowiem zanikają różnice w sprzęcie i w wyposażeniu, jakimi dysponują obie struktury, a szkolenia ich żołnierzy są podobne. Mimo wielu podobieństw te jednostki działają jednak w różny sposób. Jak mówi oficer (pułkownik) JW Komandosów: *Naszym przeznaczeniem jest operowanie w środowisku śródlądowym, priorytet to rozpoznanie specjalne. Najprościej mówiąc, 70% szkolenia naszych ludzi to taktyka zielona, 30% czarna, niebieska i czerwona. W GROM-ie te proporcje są odwrotne. Tam 70% to taktyka czarna. Nie aspirujemy do prowadzenia dużych akcji bezpośrednich ani wykonywania zadań związanych z ratowaniem Polaków potrzebujących pomocy za granicą kraju.*

---

[2] M. Ryan, Ch. Mann, A. Stilwell, *Encyklopedia oddziałów specjalnych. Taktyka, historia, strategia, uzbrojenie,* Warszawa 2003, s. 7–8.

[3] Kontrterroryzm – fizyczne zwalczanie terroryzmu.

[4] Jednostki przeznaczone do wykorzystania w złożonych i niebezpiecznych operacjach uwalniania zakładników przetrzymywanych w każdym możliwym miejscu. Tego typu formacje przeprowadzają akcje ratunkowe w budynkach, autobusach, wieżowcach, samolotach, na platformach wiertniczych, w pociągach, na statkach oraz w innych miejscach potencjalnego ataku terrorystycznego z udziałem zakładników. Głównym celem szkolenia jednostek HRF jest ich przygotowanie do ratowania zakładników. Zob. http://www.special-ops.pl/leksykon/id245,hostage-rescue-force-jednostka-ratowania-zakladnikow-hrf [dostęp: 2 I 2017].

To przeznaczenie naszych kolegów z Warszawy. Oczywiście w sytuacjach awaryjnych od każdej reguły są wyjątki[5].

JW GROM i JW Komandosów dość często działają razem. Podczas wspólnych ćwiczeń ujednoliciły najważniejsze procedury. Było to widoczne m.in. w czasie wspólnych operacji w Afganistanie. W obu jednostkach najważniejsze zadania, czyli rozpoznanie specjalne, akcje bezpośrednie i wsparcie militarne, są realizowane na podobnym poziomie. Inaczej wygląda to w przypadku skomplikowanych akcji z dużą liczbą zakładników i terrorystów. Dla przykładu można przytoczyć dwie sytuacje – w teatrze na Dubrowce i w szkole w Biesłanie. Gdyby drogi podejścia i punkty wejścia do obiektów w obu tych przypadkach dodatkowo zablokowano materiałami wybuchowymi, a po drugiej stronie znajdowali się terroryści samobójcy, to zdecydowanie należałoby tam wysłać JW GROM. Dysponuje ona bowiem wyspecjalizowanym sprzętem, a ponadto stosuje techniki, taktykę i procedury niezbędne do przeprowadzania tego typu operacji.

Spośród jednostek polskich tylko JW GROM jest przygotowana do uwalniania zakładników z obiektów ruchomych, czyli pociągów naziemnych, podziemnych, samolotów czy pojazdów kołowych, a jej Zespół Bojowy B jest szczególnym ogniwem w polskim systemie bezpieczeństwa. Jest to jedyny pododdział w Polsce, biorąc pod uwagę zarówno wojsko, policję, jak i inne służby, w pełni wyposażony w odpowiedni sprzęt, wyszkolony i proceduralnie przygotowany do prowadzenia operacji uwalniania zakładników z obiektów pływających na pełnym morzu[6].

JW GROM i JW Komandosów są skuteczne tylko wtedy, gdy ich operatorom przydziela się właściwe zadania. W Iraku JW GROM odnosiła duże sukcesy, gdyż wykorzystywano ją tam w większości do realizacji „taktyki czarnej". W Afganistanie JW Komandosów była doceniana przez amerykańskich i brytyjskich dowódców jednostek specjalnych z tego samego powodu.

JW Komandosów specjalizuje się m.in. we wsparciu militarnym sił lokalnych, czyli w priorytetowym dla ISAF współdziałaniu w czasie operacji z siłami lokalnymi oraz w rozpoznaniu specjalnym. W ramach rozpoznania specjalnego samodzielnie zbudowała potężną bazę danych biometrycznych osób podejrzewanych o współpracę z rebeliantami oraz systematycznie uzupełnia listę JPEL[7].

---

[5] J. Rybak, *Lubliniec.pl. Cicho i skutecznie*. *Tajemnice najstarszej jednostki specjalnej Wojska Polskiego*, Warszawa 2013, s. 382 i nast. (e-book).

[6] Tamże, s. 389.

[7] *Join Priority Effects List* – priorytetowa lista celów ISAF, która wyznacza ramy operacji typu „dopaść lub zabić" (ang. *capture or kill*). W praktyce oznacza to nocne rajdy na wcześniej zidentyfikowane kryjówki rebeliantów, w tym ich dowódców. U jej podstaw leży przekonanie, że likwidacja bądź uwięzienie lokalnych szefów podziemnych struktur doprowadzi na pewien czas do paraliżu tych struktur, ich miejsca bowiem będą zajmować nowi, mniej doświadczeni ludzie, https://books.google.pl/books?id=Tie8BQAAQBAJ&pg=PT42&lpg=PT42&dq=list%C4%99+JPEL&source=bl&ots=AbauaDPyW3&sig=U7hvAf2KECOaeVyIupM3AM5CvFU&hl=pl&sa=X#v=onepage&q=list%C4%99%20JPEL&f=false [dostęp: 16 VII 2017] .

Zgodnie z narodową doktryną operacji specjalnych DD/3.5[8] jednostki specjalne realizują pełne spektrum operacji specjalnych, które obejmują trzy podstawowe rodzaje zadań bojowych: akcje bezpośrednie, rozpoznanie specjalne i wsparcie militarne. Taki sposób klasyfikowania tych operacji jest zgodny z zapisami wyżej wymienionej doktryny, przyjętej dla wszystkich państw członkowskich NATO. Wojskowymi operacjami specjalnymi określa się tu operacje prowadzone przez specjalnie do tego celu wyznaczone, zorganizowane, wyszkolone i wyposażone siły, które stosują taktykę, techniki operacyjne oraz zasady ich wykorzystania wykraczające poza standardy obowiązujące w wojskach konwencjonalnych.

Operacje specjalne są prowadzone w czasie konfliktu i w czasie pokoju, samodzielnie lub we współdziałaniu czy w koordynacji z wojskami konwencjonalnymi, dla osiągnięcia celów politycznych, militarnych, informacyjnych i ekonomicznych. Względy polityczno-militarne mogą wymagać prowadzenia działań bez rozgłosu, z zastosowaniem skrytych lub dyskretnych technik oraz przy akceptacji stopnia fizycznego i politycznego ryzyka, nieakceptowalnego w operacjach sił konwencjonalnych[9].

Z powyższej definicji wynika, że operacje specjalne są operacjami wojskowymi i leżą wyłącznie w obszarze działań wojska. W tym miejscu należy zaznaczyć, że żadne inne służby mundurowe: Policja, Straż Graniczna czy ABW, nie realizują operacji specjalnych. Dokument doktrynalny jasno precyzuje, że przeprowadzanie tego typu operacji jest domeną jednostek specjalnych.

Operacje specjalne na przykładzie polskich jednostek specjalnych

Zadania JW GROM ściśle się wiążą ze specjalnym charakterem tej jednostki. Wysoki poziom trudności przewidywanych zadań wymaga od jej operatorów dużej siły fizycznej oraz zgrania zespołów bojowych, utrzymania koleżeńskich więzi i wzajemnego zaufania. Muszą oni przejść także odpowiednie szkolenie, które rozpoczyna się od kursu

[8] W dniach 27–28 VIII 2015 r. w Dowództwie Komponentu Wojsk Specjalnych (DKWS) odbyło się spotkanie robocze dotyczące opracowania drugiego projektu studyjnego dokumentu doktrynalnego *Operacje specjalne. DD/3.5*. W spotkaniu uczestniczył przedstawiciel Inspektoratu Wojsk Specjalnych (IWS) Dowództwa Generalnego Rodzajów Sił Zbrojnych, pełniącego obowiązki KKJ (kierownika jednostki organizacyjnej odpowiedzialnej za obszar tematyczny określony danym dokumentem standaryzacyjnym NATO), przedstawiciele DKWS (głównego odbiorcy dokumentu) oraz Centrum Doktryn i Szkolenia Sił Zbrojnych (odpowiedzialnego za opracowanie dokumentu). Głównym celem spotkania było uzgodnienie zapisów dokumentu doktrynalnego DD/3.5 oraz niezbędnych uzupełnień i modyfikacji (w stosunku do pierwszego projektu studyjnego) wynikających ze zmian organizacyjno-strukturalnych oraz funkcjonalnych wojsk specjalnych. Dodatkowo ustalono kierunki i terminy dalszych prac oraz zaprezentowano stanowisko i propozycje CDiSZ SZ dotyczące dalszego współdziałania z IWS oraz DWKS w zakresie opracowywania dokumentów na poziomie polityczno-wojskowym oraz innych dokumentów NATO z obszaru wojsk specjalnych, http://cdis.wp.mil.pl/pl/1_285.html [dostęp: 15 I 2017].

[9] Definicja pochodzi z dokumentu doktrynalnego *Operacje specjalne*. *DD/3.5*, Kraków 2011.

podstawowego (wielomiesięcznego szkolenia z taktyki działań specjalnych i przeciwterrorystycznych). Ten kurs wszechstronnie przygotowuje operatorów jednostki do prowadzenia operacji specjalnych. Zadania JW GROM oscylują wokół trzech głównych obszarów, zwanych taktykami, tj. „taktyki czarnej", „taktyki zielonej" i „taktyki niebieskiej"[10]. Dodatkowo operatorzy wykonują również zadania specjalistyczne, wymagające przygotowania w zakresie spadochroniarstwa, nurkowania, operowania na wysokościach, a także przygotowania pirotechnicznego, medycznego i paramedycznego. Szczególne umiejętności operatorów są niezbędne do realizacji wielu wyjątkowo trudnych zadań, często niemożliwych do przewidzenia.

Natomiast operatorzy JW Komandosów mają umiejętność prowadzenia działań specjalnych w ramach „taktyki zielonej", działań w terenie zabudowanym w ramach „taktyki czarnej", działań na akwenach śródlądowych w ramach „taktyki niebieskiej" oraz umiejętność w zakresie ratownictwa medycznego na polu walki, określonego jako „taktyka czerwona". Głównym zadaniem operatorów JW Komandosów jest prowadzenie działań zaliczanych to „taktyki zielonej". Jednostka wykonuje zadania specjalne z zakresu rozpoznania specjalnego, działań niekonwencjonalnych, akcji bezpośrednich, odzyskiwania zaginionego lub uprowadzonego personelu z terenów objętych działaniami, zwalczania przeciwnika asymetrycznego (kontrterroryzm), wsparcia militarnego, szkolenia wojsk sojuszniczych, prowadzenia akcji ratowniczo-poszukiwawczych, prowadzenia operacji reagowania kryzysowego, operacji ratowania zakładników, a także ochrony osobistej VIP-ów.

Do najważniejszych zadań, do których jest przeznaczona JW Komandosów, należy realizacja zadań o charakterze specjalnym na lądzie, w odniesieniu do celów o znaczeniu operacyjnym i strategicznym, zarówno na terenie państwa, jak i poza jego granicami, oraz prowadzenie rozpoznania specjalnego (rozpoznanie środowiska, ocena zagrożeń i celów oraz skutków wykonywanych działań). Operatorzy JW Komandosów są gotowi do wykonywania akcji bezpośrednich prowadzonych w krótkim czasie i ograniczonym zakresie. Zespoły bojowe mogą realizować takie akcje samodzielnie lub przy pomocy wojsk konwencjonalnych (rajdy, zasadzki, uwalnianie i odzyskiwanie personelu, precyzyjne niszczenie, przejmowanie i opanowywanie obiektów nawodnych)[11]. JW Komandosów jest przygotowana również do przeciwdziałania terroryzmowi i zwalczania tego zjawiska[12].

Kolejna jednostka wojskowa – AGAT – jest docelowo priorytetową jednostką szturmową lekkiej piechoty o charakterze powietrznodesantowym i cechach piechoty górskiej, przeznaczoną do prowadzenia operacji specjalnych. Specjalizuje się w wykonywaniu z zaskoczenia akcji bezpośrednich na wskazane cele, na tyłach i w ugrupowaniu przeciwnika. JW AGAT może prowadzić akcje samodzielne lub przez wydzielanie swoich sił do składu innych zadaniowych zespołów bojowych

[10] B. Pacek, *Wojska Specjalne Sił Zbrojnych RP*, Siedlce 2019, s. 87 i nast.

[11] Tamże, s. 103–104.

[12] http://cisiiskuteczni.pl/jestem-komandosem/zadania-jednostki [dostęp: 4 I 2017].

jako wsparcie dla jednostek specjalnych, zwłaszcza podczas ich precyzyjnych działań antyterrorystycznych (ratowanie zakładników, zatrzymywanie i neutralizacja HVT[13], likwidacja wytwórni i składów uzbrojenia oraz materiałów wybuchowych), a także odzyskiwania personelu i sprzętu o specjalnym znaczeniu. Natomiast podczas działań w ramach zespołów bojowych priorytetem jednostki jest izolowanie szturmowanego obiektu od zewnątrz i uniemożliwienie udzielenia wsparcia przeciwnikowi, a równocześnie – umożliwienie siłom własnym zdominowanie przeciwnika znajdującego się w obiekcie i zdobycie obiektu. Do specjalności jednostki należy błyskawiczne opanowywanie lotnisk i lądowisk oraz ochrona wysuniętych baz operacyjnych jednostek specjalnych. Zadaniem operatorów JW AGAT jest także przeprowadzanie rajdów pod hasłem „zniszczyć" oraz „znaleźć i zniszczyć", mających na celu dezorganizację ruchów wrogich wojsk, opanowanie bądź zniszczenie ważnych obiektów, organizowanie napadów i zasadzek[14].

Z kolei JW NIL została powołana do realizacji zadań w zakresie wsparcia informacyjnego i dowodzenia oraz zabezpieczenia logistycznego i medycznego działań i operacji specjalnych prowadzonych przez wojska specjalne w kraju i za granicą. Najważniejszym obszarem działalności tej jednostki jest udzielanie wsparcia informacyjnego i pomocy w dowodzeniu oraz zabezpieczeniu logistycznym operacji specjalnych realizowanych w układzie narodowym i sojuszniczym. Zadaniem priorytetowym tej jednostki jest realizacja przedsięwzięć związanych z prawidłowym funkcjonowaniem systemu dowodzenia wojskami specjalnymi. JW NIL udziela wsparcia informacyjnego m.in. podczas prowadzenia operacji specjalnych. Polega ono na wydzielaniu elementów rozpoznawczych do zadaniowych zespołów bojowych lub komponentów wojsk specjalnych[15]. System zabezpieczenia logistycznego JW NIL jest integralną częścią systemu logistycznego wojsk specjalnych.

7 Eskadra Działań Specjalnych realizuje zadania za pośrednictwem zespołów bojowych bądź sekcji bojowych wojsk specjalnych. Operacyjnie podlega określonemu dowódcy wojsk specjalnych. Jej główne zadania to:

- transport operatorów zespołów bojowych (sekcji) wojsk specjalnych (w tym na miejsce podejmowanych działań);
- wsparcie ogniowe operatorów wojsk specjalnych działających na lądzie w czasie trwania operacji, włącznie z niszczeniem określonych celów;
- prowadzenie rozpoznania specjalnego;
- ewakuacja operatorów wojsk specjalnych z miejsca operacji;
- transport zaopatrzenia dla zespołów bojowych.

[13] Ang. *High Value Target* – cel o dużym znaczeniu. W terminologii amerykańskiej wysoki rangą członek rządu (sił) przeciwnika lub organizacji terrorystycznej, www.special-ops.pl (przyp. red.).

[14] B. Pacek, *Wojska Specjalne*…, s. 123–124.

[15] Tamże, s. 130.

Żołnierze 7 Eskadry Działań Specjalnych są przygotowani do działania w zakresie:
- wykonywania lotów w trudnych (nawet ekstremalnych) warunkach pogodowych;
- wykonywania lotów w dzień i w nocy (z użyciem noktowizji);
- wykonywania lotów w górach, nad terenami gęsto zabudowanymi i akwenami na niskich wysokościach;
- lądowania, na platformach i w miejscach trudno dostępnych;
- podejmowania działań w sytuacjach awaryjnych[16].

Do operacji specjalnych, realizowanych zarówno przez polskie, jak i zagraniczne jednostki specjalne, należą[17]:

- SR (ang. *special reconnaissance*) – rozpoznanie specjalne, czyli m.in.: zdobywanie na terenie przeciwnika istotnych informacji (dotyczących nastrojów społecznych, rodzaju oraz ilości sprzętu i uzbrojenia posiadanego przez przeciwnika, lokalizacji zgrupowań wojsk przeciwnika), pozyskiwanie dokumentów wojskowych, nowego typu uzbrojenia oraz ocena skutków działań wojsk własnych;
- DA (ang. *direct action*) – akcje bezpośrednie, czyli: przygotowywanie zasadzek, zdobywanie i niszczenie wskazanych obiektów lub pojazdów przewożących broń, sabotaż na lotniskach i w portach przeciwnika; likwidacja stanowisk dowodzenia, węzłów komunikacyjnych, łączności i energetycznych, prowadzenie akcji dywersyjnych paraliżujących poczynania przeciwnika (m.in. minowanie terenu, wywoływanie paniki). Akcje bezpośrednie w porównaniu z działaniami konwencjonalnymi przewyższają je poziomem ryzyka fizycznego i politycznego, techniką wykorzystywaną podczas akcji oraz poziomem weryfikacji i precyzji użycia siły do osiągnięcia wyznaczonych celów. JW GROM ma za zadanie wywoływanie paniki i paraliżowanie poczynań przeciwnika[18]. DA charakteryzują takie działania, jak[19]:
  - rajdy, zasadzki i ataki bezpośrednie – są one elementami operacji, których siły konwencjonalne niekiedy nie mają możliwości prowadzić. Takie operacje zazwyczaj obejmują ataki na cele krytyczne, niszczenie linii komunikacyjnych wykorzystywanych przez wrogie strony lub niszczenie innych systemów będących celami, pojmanie wyznaczonego personelu lub przejęcie materiałów i zajęcie, zniszczenie bądź neutralizację urządzeń albo pozbawienie przeciwnika pewnych możliwości,
  - ataki z dużych odległości – niszczenie lub zdobywanie wytypowanych obiektów. Realizacja zadań dywersyjnych oraz sabotażowych w portach

[16] Tamże, s. 133–134.

[17] http://pl.wikipedia.org/wiki/Jednostka_Wojskowa_GROM [dostęp: 1 IX 2019].

[18] B. Pacek, *Wojska Specjalne*…, s. 88.

[19] http://www.formacjasgo.pl/portfolio-view/akcje-bezposrednie-da-rodzaje-i-charakter/ [dostęp: 1 IX 2019].

i na lotniskach przeciwnika, przygotowywanie zasadzek; atakowanie za pomocą systemów uzbrojenia lub operacji informacyjnych. Mogą być przeprowadzane jako działania samodzielne[20]. Niektóre z polskich jednostek specjalnych (np. JW GROM) zajmują się także likwidacją stanowisk dowodzenia przeciwnika, węzłów komunikacyjnych, infrastruktury energetycznej oraz łączności. Dodatkowo wprowadza się działania związane z wywoływaniem paniki oraz paraliżujące działania przeciwnika,

– naprowadzanie uderzeń lotnictwa oraz operacje naprowadzania lotnictwa – działania zmierzające do identyfikacji i precyzyjnego raportowania lokalizacji celów, aby skutecznie wykorzystać przeciw nim uzbrojenie z wykorzystaniem GPS, wskaźników laserowych, urządzeń sygnalizacyjnych, innych środków prowadzenia bądź naprowadzania uderzeń lotnictwa oraz naprowadzania lotnictwa. Naprowadzanie uderzeń lotnictwa obejmuje kontrolę manewru i zgodę na użycie uzbrojenia przez atakujący samolot. Operacje naprowadzania lotnictwa natomiast obejmują każdą komunikację elektroniczną, mechaniczną, głosową lub wizualną, która dostarcza podchodzącemu samolotowi lub uzbrojeniu dodatkowe informacje dotyczące określonej lokalizacji lub celu. *Terminal attack control* (TAC) różni się od *terminal guidance operations* (TGO) tym, że pierwsza opcja obejmuje uprawnienia do wydania zgody na użycie uzbrojenia przez samolot, druga zaś takich uprawnień nie obejmuje. Dlatego TAC wymaga udziału osób wykwalifikowanych – kontrolerów naprowadzania uderzeń połączonych (ang. *joint terminal attack controllers*), a TGO – nie,
– operacje odzyskiwania (ewakuacji) personelu – polegają one na zlokalizowaniu, odnalezieniu, zidentyfikowaniu, uratowaniu i ewakuowaniu personelu, wrażliwego wyposażenia lub innych rzeczy, krytycznych dla bezpieczeństwa narodowego. Misje jednostek specjalnych w zakresie odzyskiwania (ewakuacji) charakteryzują się szczegółowym planowaniem oraz gruntownymi analizami wywiadowczymi. W tych operacjach wykorzystuje się niekonwencjonalną taktykę i technikę, tajne poszukiwania, możliwe wsparcie tubylcze i często używa się lądowych elementów bojowych,
– operacje precyzyjnego zniszczenia – operacje, w których przypadku skutki (zniszczenia) muszą być zminimalizowane. Wymagają użycia wyrafinowanej broni i (lub) kontrolowanej detonacji określonej ilości materiałów wybuchowych umieszczonych we właściwych miejscach, aby osiągnąć cele misji. Operacje precyzyjnego zniszczenia mogą być prowadzone wtedy, gdy precyzyjna amunicja kierowana nie gwarantuje sukcesu w pierwszym uderzeniu lub kiedy „zawartość" obiektu musi być zniszczona bez uszkadzania samego obiektu,

[20] https://specjalsi.wordpress.com/2013/08/22/leksykon-specjalsow-akcje-bezposrednie/ [dostęp: 3 VI 2017].

  - operacje przeciw celom powierzchniowym – operacje przeciwko morskim celom powierzchniowym przeciwnika. Obejmują m.in.: inspekcję, abordaż, przeszukanie i zajęcie, które są pokładowymi operacjami abordażu oraz zajęcia współpracujących, niewspółpracujących lub wrogich wykrytych obiektów budzących zainteresowanie;
- MS (ang. *military support*) – wsparcie militarne, szkolenie wojsk sojuszniczych w czasie pokoju, a także realizacja zadań w zakresie doradztwa i wsparcia sojuszników podczas kryzysu i wojny[21];
- MOOTW (ang. *military operations other than war*) – reagowanie kryzysowe, prowadzenie operacji wojskowych innych niż wojna, w tym tzw. *non-combatment evacuation*, tj. sprawne, bezpieczne i szybkie ewakuowanie osób z rejonów objętych walkami oraz z miejsc naruszenia porządku publicznego;
- HR (ang. *hostage rescue*) – odbijanie zakładników. JW GROM jest odpowiedzialna za realizację tego zadania poza granicami kraju, na terytorium zajętym przez przeciwnika;
- CT (ang. *counterterrorism*) – fizyczne zwalczanie terrorystów. JW GROM wkracza do akcji po zamachu terrorystycznym. Dodatkowo podejmuje działania wspierające policję, gdy nie dysponuje ona siłami wystarczającymi do udzielenia odpowiedzi na zamach;
- PR (ang. *personnel recovery*) – uwalnianie osób przetrzymywanych lub przebywających na zagrożonych terenach (np. w ambasadach). Do tego typu zadań zalicza się także prowadzenie bojowych akcji ratowniczo-poszukiwawczych (ang. *combat search and rescue*, CSAR), obejmujących całe spektrum zadań związanych z ratowaniem i poszukiwaniem osób zaginionych (w tym ewakuację pilotów zestrzelonych nad terytorium przeciwnika)[22];
- UW (ang. *unconventional warfare*) – działania niekonwencjonalne, tj. działania nietypowe dla wojsk konwencjonalnych. Można tu zaliczyć m.in. przenikanie do okrążanych oddziałów oraz prowadzenie działań nieregularnych, walk partyzanckich i działań przeciwdywersyjnych[23].

Jako najważniejsze z działań specjalnych wymienia się rozpoznanie specjalne. Jego celem jest uzyskanie terminowych i dokładnych danych o przeciwniku na szczeblu operacyjnym lub strategicznym. Prowadząc rozpoznanie specjalne, komandosi wykorzystują pełny zakres technik, taktyk i procedur oraz różnego rodzaju sprzęt.

Cechą charakterystyczną rozpoznania specjalnego jest stosowanie technik, które często są bliższe służbom wywiadowczym niż siłom wojskowym. W przypadku tego typu rozpoznania komandosi mogą współpracować – i często współpracują – z wywiadem wojskowym oraz działają w całkowitym oderwaniu od wojsk własnych.

[21] B. Pacek, *Wojska Specjalne*…, s. 89.

[22] Tamże, s. 88.

[23] Tamże, s. 89.

Drugim ważnym rodzajem działań są akcje bezpośrednie. To nic innego jak operacje ofensywne, cechujące się precyzją oraz ograniczeniem rejonu i czasu działania.

Trzecim głównym rodzajem działań specjalnych jest wsparcie militarne. Jego celem jest udzielanie pomocy siłom sprzymierzonym w czasie pokoju, kryzysu i wojny. Głównymi obszarami, w których dochodzi do wsparcia militarnego, są szkolenie i doradztwo uznanych, sojuszniczych sił militarnych i paramilitarnych. Mieszczą się tu również przedsięwzięcia związane z wyposażaniem i wspieraniem szkolonych formacji.

Dokumenty doktrynalne wymieniają ponadto takie działania realizowane przez jednostki specjalne, jak[24]:

- wsparcie przeciwdziałania siłom nieregularnym, których głównym zadaniem jest prowadzenie działań kontrterrorystycznych;
- przeciwdziałanie rozprzestrzenianiu broni chemicznej, biologicznej i nuklearnej;
- uwalnianie zakładników;
- morskie operacje specjalne (operacje specjalne prowadzone w środowisku wodnym przez specjalne pododdziały Marynarki Wojennej, a także wodne zespoły bojowe JW GROM);
- powietrzne operacje specjalne (operacje specjalne realizowane przez specjalne pododdziały sił powietrznych).

Aby móc przeprowadzać i udoskonalać wyżej wskazane operacje, jednostki specjalne tworzą system szkolenia operatorów oparty na prowadzeniu trzech głównych rodzajów działań:

1) przeciwterrorystycznych działań lądowych („taktyka czarna")[25]. Są to działania polegające na bezpośredniej walce z przeciwnikiem, walce w budynkach, na terenie zurbanizowanym i ogólnie w obiektach zamkniętych. Należą do nich: uwalnianie zakładników z obiektów stałych (domy, wieżowce) i pojazdów (samochody, samoloty, pociągi naziemne i podziemne), ochrona VIP-ów i obiektów, przeciwdziałanie operacjom nieregularnym oraz zabezpieczanie działań i operacji innych służb wojskowych i pozamilitarnych. Ten rodzaj taktyki można podzielić na:
   - operacje wojskowe przeprowadzane na terenie zurbanizowanym, czyli zbiór technik odnoszących się do działań militarnych na terenach miejskich (ang. *military operations in urban terrain*, MOUT);

[24] https://www.cisiiskuteczni.pl/akademia/trzy-kolory-czarny-zielony-i-niebieski [dostęp: 4 II 2017].

[25] Kolor czarny („taktyka czarna") oznacza prowadzenie działań ofensywnych w terenie zurbanizowanym. Nazwa pochodzi od koloru ubrań ochronnych (mundurów) pododdziałów antyterrorystycznych amerykańskiej policji (typu *Special Weapons and Tactics teams* – SWAT teams). Z czasem to pojęcie poszerzono o działania przeprowadzane poza miastem, związane z walką z przeciwnikiem znajdującym się w budynku lub innym obiekcie (samolot, pociąg naziemny, pociąg podziemny, samochód), https://www.cisiiskuteczni.pl/akademia/trzy-kolory-czarny-zielony-i-niebieski [dostęp: 11 II 2017].

– walkę na bezpośrednim dystansie, traktowaną jako ostateczna faza eliminacji przeciwnika podczas operacji MOUT (*Close Quarters Battle*, CQB).

Innym rodzajem działań wchodzących w zakres „taktyki czarnej" są operacje antyterrorystyczne prowadzone przez oddziały policyjne na terenie własnego kraju. Ich cechą charakterystyczną jest udział zakładników i obecność terrorystów. Szczególnym przypadkiem operacji antyterrorystycznych są operacje realizowane przez jednostki wojskowe za granicą;

2) działań poza terenem zurbanizowanym („taktyka zielona"). Nazwa pochodzi od dominującego koloru lasu i mundurów maskujących. Podstawowymi zadaniami w ramach tej taktyki są: patrolowanie, obserwacja, organizowanie zasadzek, rajdy oraz inne rodzaje działań ofensywnych. Określenie „taktyka zielona" może jednak okazać się złudne, gdyż działania prowadzone na pustyni czy na kole podbiegunowym również są zaliczane do tego typu taktyki. „Taktyka zielona" jest stosowana zarówno podczas konwencjonalnego konfliktu zbrojnego, działań partyzanckich, działań przeciwpartyzanckich, jak i w sytuacjach szczególnych, np. podczas wykonywania czynności policyjnych. Może być wykorzystywana przez grupy rozpoznawcze, dywersyjne lub prowadzące inne działania, np. działania długotrwałe, i wymagać szczególnej troski o kamuflowanie obecności grupy specjalnej oraz ochrony jej funkcjonowania na obcym terenie[26];
3) morskich działań przeciwterrorystycznych[27] („taktyka niebieska"). Do tego typu działań zalicza się: zwalczanie terroryzmu na styku ląd–morze, a także na obiektach pływających i platformach, przeprowadzanie działań na wodzie i pod wodą[28], stosowanie technik przerzutu grup specjalnych przez wody (łodziami, kajakami, pojazdami podwodnymi), działania na obiektach pływających i nadbrzeżnych, prowadzenie rozpoznania wybrzeży i morskich operacji anty- i kontrterrorystycznych[29]. „Taktyka niebieska" mieści w sobie przede wszystkim prowadzenie rozpoznania specjalnego i akcji bezpośrednich, choć nie wyklucza realizacji wsparcia militarnego w środowisku wodnym.

W składowe „taktyki niebieskiej" wpisują się morskie operacje specjalne. Z uwagi na specyfikę środowiska działań wykonywanych przez jednostki specjalne wyodrębnia się morskie jednostki specjalne. Stanowią one niekonwencjonalną część sił zbrojnych, przeznaczoną do prowadzenia działań specjalnych (akcji, misji, operacji). Należą do nich: JW FORMOZA oraz pododdział JW GROM – Zespół Bojowy B, zwany potocznie „wodą". Wymienione jednostki prowadzą działania w morskiej

[26] http://www.special-ops.pl/leksykon/id127,zielona-taktyka [dostęp: 24 VII 2017].

[27] K.K. Soyka, K. Kotowski, *Cel za horyzontem. Opowieść snajpera GROM-u*, Wołowiec 2015, s. 105.

[28] M. Łukaszewicz, *Płk Roman Polko. Gromowładny*, Kraków 2005, s. 97.

[29] http://www.special-ops.pl/leksykon/id97,niebieska-taktyka [dostęp: 24 VII 2017].

strefie przybrzeżnej oraz na otwartym morzu i wodach śródlądowych. Są to niewielkie, mobilne pododdziały działające z morza, na morzu lub pod jego powierzchnią. Operacje przez nie prowadzone charakteryzują się skrytością, szybkością i precyzją[30]. JW FORMOZA rozwija zdolności bojowe, umożliwiające efektywne wykorzystanie tej jednostki w sytuacji narastania kryzysu lub wystąpienia konfliktu zbrojnego. Podczas narodowej operacji obronnej, w przypadku operacji połączonej, morskie siły specjalne działają na korzyść komponentu morskiego sił zbrojnych. JW FORMOZA jest jednostką specjalną przeznaczoną do realizacji pełnego spektrum morskich operacji specjalnych w układzie narodowym, sojuszniczym i koalicyjnym. Jej operatorzy są szkoleni, wyposażeni i uzbrojeni zgodnie z jej charakterem i przewidywanymi zadaniami. Ta formacja może prowadzić działania samodzielnie lub wspierać i zabezpieczać działania innych sił, organizacji lub instytucji[31]. Natomiast w okresie pokoju i w zasadniczej fazie kryzysu (dwa momenty skrajne), w przypadku zwiększenia skali zagrożenia JW FROMOZA jest zdolna do przyjęcia zadań stawianych przed JW GROM[32].

Natomiast Zespół Bojowy B JW GROM, jako drugi komponent morskich sił specjalnych, rozwija swoje zdolności bojowe związane ze zwalczaniem terroryzmu i piractwa na morzu. W trakcie realizacji zadań zespół współdziała z Marynarką Wojenną RP. Jest zdolny do samodzielnego prowadzenia operacji wysokiego ryzyka i osiągania celów politycznych podczas konfliktów w okresie pokoju i w zasadniczej fazie kryzysu, a także do aktywnego uczestniczenia w wojnie (czego przykładem jest operacja przeprowadzona w porcie Umm Kasr w Iraku)[33]. Zdolności ekspedycyjne umożliwiają Zespołowi Bojowemu B operowanie na otwartym morzu w każdym zakątku ziemi, gdzie są zagrożone bezpieczeństwo obywateli RP lub interes państwa.

Każda profesjonalna jednostka specjalna musi mieć w swoich strukturach zespół bojowy złożony z płetwonurków. Dlatego już w połowie lat 90. XX w. w Lublińcu została utworzona kompania specjalna, licząca około 80 żołnierzy, która weszła w skład batalionu dywersyjno-rozpoznawczego. Przygotowanie tego typu grup specjalnych koordynuje sekcja zabezpieczenia nurkowania pionu szkoleniowego[34].

Morze to ogromna przestrzeń, dlatego operujących tu żołnierzy jednostek specjalnych trudniej jest niespodziewanie zaatakować. Z kolei rzeki z jednej strony ułatwiają jednostkom specjalnym niezauważalne przemieszczanie się, ale z drugiej umożliwiają przygotowanie zasadzki.

Wśród operacji specjalnych prowadzonych przez morskie jednostki specjalne należy wyróżnić morskie operacje specjalne. Charakteryzują się one skrytością,

---

[30] *Operacje Specjalne*. *DD/ 3.5*, pkt 2012.

[31] B. Pacek, *Wojska Specjalne*…, s. 111–112.

[32] *Wojska specjalne w systemie obronnym RP – aspekty organizacyjne, doktrynalne i modernizacyjne*, B. Pacek (red.),Warszawa 2013, s. 103 i nast.

[33] http://historia.org.pl/2013/03/08/szturm-na-terminal-grom-w-porcie-umm-kasr/ [dostęp: 11 II 2017].

[34] http://www.polska-zbrojna.pl/home/articleshow/28871# [dostęp: 25 VIII 2019].

szybkością ich realizacji, a także precyzją. Są przeprowadzane przez wyselekcjonowane, zorganizowane, wyszkolone oraz odpowiednio wyposażone siły, gotowe do podjęcia zadań bojowych na powierzchni morza otwartego lub pod jego powierzchnią, w strefie przybrzeżnej oraz na lądzie – w odległości do 50 km od brzegu morskiego, w tym na terenie portów morskich i w ujściach rzek do morza. Takie działania zmierzają do bezpośredniego osłabienia potencjału militarno-ekonomicznego przeciwnika i służą zebraniu danych niezbędnych do zapewnienia informacji w czasie rzeczywistym podczas działań wojsk własnych (rozpoznanie odcinka do desantu morskiego lub ocena skutków uderzeń).

W ramach morskich operacji specjalnych wyróżnia się:

1) podwodne działania bojowe – działania prowadzone pod powierzchnią morza przez zespoły nurków bojowych (samodzielnie lub za pomocą wielozadaniowych łodzi bojowych, pojazdów podwodnych lub okrętów podwodnych), z zastosowaniem niestandardowych i niekonwencjonalnych taktyk, technik i procedur;
2) nawodne działania bojowe – działania prowadzone na powierzchni morza oraz na jednostkach pływających i w obiektach hydrotechnicznych usytuowanych na morzu przez obsady łodzi bojowych oraz dodatkowo wydzielonych nurków bojowych (z wykorzystaniem łodzi bojowych, wielozadaniowych łodzi bojowych, okrętów podwodnych oraz innych nawodnych jednostek pływających, w tym także środków przerzutu powietrznego), z wykorzystaniem niestandardowych i niekonwencjonalnych taktyk, technik i procedur;
3) morskie zintegrowane działania bojowe – działania prowadzone w strefie przybrzeżnej i na lądzie, w odległości 50 km od brzegu morskiego, w tym na terenie portów morskich i w ujściach rzek do morza, przez obsady łodzi bojowych oraz nurków bojowych (z wykorzystaniem łodzi bojowych, wielozadaniowych łodzi bojowych, okrętów podwodnych oraz innych nawodnych jednostek pływających, w tym także środków przerzutu powietrznego i lądowego), z zastosowaniem niestandardowych i niekonwencjonalnych taktyk, technik i procedur;
4) morskie przeciwterrorystyczne działania bojowe – działania prowadzone na powierzchni morza oraz na jednostkach pływających i w obiektach hydrotechnicznych usytuowanych na morzu przez obsady łodzi bojowych oraz dodatkowo wydzielonych operatorów jednostek specjalnych, w sytuacjach zagrożenia terrorystycznego w okresie pokoju oraz kryzysu.

Istotnymi elementami realizacji zadań bojowych prowadzonych przez morskie siły specjalne są: dynamizm oraz precyzja działań – dzięki właściwie dobranym operatorom, wyposażeniu o parametrach dostosowanych do specyfiki działań morskich oraz właściwie zaplanowanemu, przygotowanemu i przeprowadzonemu szkoleniu z zachowaniem zasady realizmu, tzn. jak największego zbliżenia do rzeczywistych

działań bojowych. Zdaniem kmdr. Radosława Tokarskiego[35] to właśnie odpowiednie zdolności bojowe umożliwiają realizację zadań stawianych morskim siłom specjalnym, a jednym z nich jest prowadzenie rozpoznania specjalnego, tj.:

- ustalanie miejsca postoju okrętów, identyfikacja ich klas i stopnia gotowości operacyjnej,
- ustalanie systemu ochrony i obrony przeciwdesantowej,
- rozpoznawanie baz morskich i portów przeciwnika,
- śledzenie aktywności na morskich liniach komunikacyjnych,
- rozpoznawanie funkcjonowania systemu dowodzenia i łączności oraz punktów kierowania ogniem przeciwnika w strefie bojowej,
- lokalizacja infrastruktury energetycznej, paliwowej, urządzeń radioelektrycznych, węzłów łączności i dowodzenia,
- ustalanie warunków hydrometeorologicznych.

Kolejnym zadaniem morskich sił specjalnych jest przeprowadzanie akcji bezpośrednich, w tym:

- dokonywanie zniszczeń w bazach morskich i portach przeciwnika,
- blokowanie wejść do baz morskich i portów należących do przeciwnika,
- niszczenie okrętów przeciwnika znajdujących się w bazach morskich, portach i na kotwicowiskach,
- opanowanie lub niszczenie obiektów o znaczeniu strategicznym i operacyjnym,
- dezorganizacja funkcjonowania systemu dowodzenia i łączności.

Do zadań podstawowych należy również udzielanie wsparcia militarnego (szkolenie okrętowych grup abordażowych i ochrona okrętów w trakcie ich pobytu w rejonach niebezpiecznych, w których występuje zagrożenie terrorystyczne i dywersyjne).

Specyfikę zadań morskich sił specjalnych można określić, odnosząc ją do relacji sił wspierających i wspieranych. Jako siły wspomagające komandosi (operatorzy) mogą bowiem realizować zadania w ramach operacji blokadowej przez abordaż na jednostkę, której kapitan odmawia współpracy i nie odpowiada na sygnały zatrzymania. Innym zadaniem jest wsparcie zespołu wykrywania broni masowego rażenia podczas przeszukania jednostki pływającej wytypowanej do kontroli. Żołnierze morskich sił specjalnych mogą także oceniać skutki uderzeń sił własnych, w celu potwierdzenia rzeczywistych zniszczeń i potrzeby ponownego ataku. Jako siły wspierające korzystają ze zdolności, jakie mają siły konwencjonalne w zakresie funkcjonowania wysuniętej bazy operacyjnej na morzu.

Podobnie jak w przypadku zadań z zakresu operacji specjalnych, wyżej podane trzy rodzaje taktyk („czarna", „zielona", „niebieska") nie wyczerpują pełnego spektrum kolorów taktyk stosowanych przez komandosów. Istnieje bowiem połączenie innych elementów z wyżej wymienionymi taktykami, tworzące swoiste uzupełnienie

[35] Komandor Radosław Tokarski jest dowódcą JW FORMOZA, https://formoza.wp.mil.pl/pl/pages/kierownictwo-2017-01-16-4/ [dostęp: 25 VIII 2019].

już istniejących. Jednym z takich połączeń jest „taktyka czerwona". Kojarzy się ona z krwią i czerwonym krzyżem – medycznym znakiem rozpoznawczym. Jest to skojarzenie jak najbardziej słuszne, ponieważ ten rodzaj taktyki obejmuje procedury i techniki udzielania pierwszej pomocy na polu walki oraz ewakuacji medycznej. Co istotne, sama w sobie nie jest taktyką odrębną, lecz uzupełnia wszystkie pozostałe rodzaje taktyk, zapewniając im to, co najważniejsze – wsparcie medyczne. Biorąc pod uwagę powyższe, „taktyka czerwona" jest wykorzystywana we wszystkich operacjach specjalnych.

Kolejno można wyróżnić „taktykę szarą", która jest odmianą taktyki stosowanej w przypadku ochrony osób (zwanej potocznie „ochroną VIP"), i „taktykę białą". „Taktyka szara" obejmuje zasady i procedury bezpośredniej ochrony fizycznej, ochrony przeciwsnajperskiej, jazdy ofensywnej i ochrony przed inwigilacją. „Taktyka biała" natomiast jest przez wielu znawców tematu uważana za najtrudniejszą i najbardziej wyczerpującą. Jej nazwa pochodzi od koloru papieru biurowego i dotyczy realizacji czynności biurokratycznych, niezbędnych do prowadzenia każdego rodzaju działań w każdym możliwym zakresie[36].

Poszczególne jednostki specjalne profesjonalizują się w zadaniach związanych ze specyfiką środowisk misji, w których uczestniczą. JW FORMOZA doskonali się w prowadzeniu operacji w środowisku morskim i przybrzeżnym, JW Komandosów – operacji specjalnych w środowisku lądowym i przybrzeżnym, JW GROM natomiast – jako najbardziej uniwersalny komponent wojsk specjalnych – operacji w każdym środowisku (Zespoły Bojowe A, B i C). Pozostałe Jednostki Wojskowe: NIL, AGAT oraz 7 Eskadra Działań Specjalnych wspierają operacje prowadzone w każdym środowisku walki. Szkolenie i wyposażenie jednostek specjalnych zapewnia możliwość prowadzenia operacji we wszystkich strefach klimatycznych, włącznie z rejonami występowania warunków ekstremalnych[37].

Kierunki rozwoju wojsk specjalnych nakreślono w dokumencie *Plan Rozwoju Wojsk Specjalnych 2009–2018*[38]. W modelu na 2022 r. jednostki specjalne będą opierać swoją zdolność bojową na pięciu jednostkach organizacyjnych oraz eskadrze działań specjalnych. Zakłada się, że kandydaci do służby w tych wojskach będą ją rozpoczynać w JW AGAT, gdzie będą poddawani selekcji i szkoleniu bazowemu – testowi ich zdolności do dalszego rozwoju. Wyższy poziom wtajemniczenia będzie stanowić służba w JW Komandosów oraz w JW FORMOZA. Służba w tych jednostkach bowiem będzie pełniona przez kandydatów dobieranych na podstawie wyników uzyskanych w ramach służby w jednostkach NIL i AGAT. Najwyższy szczebel jednostek specjalnych będzie zajmować JW GROM. Służbę w niej będzie pełnić jedynie wąskie grono żołnierzy.

---

[36] https://www.cisiiskuteczni.pl/akademia/trzy-kolory-czarny-zielony-i-niebieski [dostęp: 29 I 2017].

[37] B. Pacek, *Wojska Specjalne*…, s. 45.

[38] Dokument dostępny pod adresem: www.rocznikbezpieczenstwa.dsw.edu.pl/fileadmin/user_upload/.../2011_12.pdf [dostęp: 15 I 2017].

Charakterystykę i zadania polskich jednostek specjalnych można odnieść do misji sił zbrojnych:

- W ramach pierwszej misji polskich sił zbrojnych, jaką jest zagwarantowanie obrony państwa i przeciwstawianie się agresji, jednostki specjalne przygotowują się do udziału w strategicznej operacji obronnej. Ten udział jest realizowany w ścisłym współdziałaniu z pozostałymi komponentami Rodzajów Sił Zbrojnych, w wymiarze narodowym i sojuszniczym.
- W ramach uczestnictwa w budowaniu stabilizacji międzynarodowej oraz udziału w operacjach humanitarnych jednostki specjalne pozostają w gotowości do udziału w pełnym spektrum operacji sojuszniczych w każdym środowisku geograficznym i klimatycznym.
- Misja wspierania bezpieczeństwa wewnętrznego i pomocy społeczeństwu jest realizowana przez jednostki specjalne w ramach sił i środków przeznaczonych do systemu reagowania kryzysowego. Tego rodzaju zadania obejmują reagowanie na incydenty o podłożu terrorystycznym zarówno w kraju, jak i za granicą.

Należy wskazać, że jednostki specjalne realizują powyższe zadania w ścisłym współdziałaniu z wieloma podmiotami, m.in. ze służbami wywiadu i kontrwywiadu[39].

Bibliografia

Łukaszewicz M., Polko R., *Płk Roman Polko. Gromowładny*, Kraków 2005, Wydawnictwo M.

Operacje Specjalne. DD/3,5, Kraków 2011, Dowództwo Wojsk Specjalnych.

Pacek B., *Wojska Specjalne Sił Zbrojnych RP*, Siedlce 2019, Oficyna Wydawnicza RYTM.

Rybak J., *Lubliniec pl. Cicho i skutecznie*, Warszawa 2011, CREATIO PR.

Soyka K.K., Kotowski K., *Cel za horyzontem. Opowieść snajpera GROM-u*, Wołowiec 2015, Wydawnictwo Czarne.

Stilwell A., *Jednostki specjalne w akcji. Afganistan, Afryka, Bałkany, Irak, Ameryka Południowa*, Warszawa 2009, MUZA.

Stilwell A., Ryan M., Mann Ch., *Encyklopedia oddziałów specjalnych. Taktyka, historia, strategia, uzbrojenie*, Warszawa 2003, Bellona.

Wojska Specjalne w systemie obronnym RP. Aspekty organizacyjne, doktrynalne i modernizacyjne, Warszawa 2013, AON (raport z konferencji zorganizowanej przez Akademię Obrony Narodowej, Dowództwo Wojsk Specjalnych i Polskie Lobby Przemysłowe im. E. Kwiatkowskiego).

[39] B. Pacek, *Wojska Specjalne*…, s. 47.

Strony internetowe

https://books.google.pl/books?id=Tie8BQAAQBAJ&pg=PT42&lpg=PT42&dq=list%C4%99+JPEL&source=bl&ots=AbauaDPyW3&sig=U7hvAf2KECOaeVyIup-M3AM5CvFU&hl=pl&sa=X#v=onepage&q=list%C4%99%20JPEL&f=false [dostęp: 16 VII 2017].

http://cdis.wp.mil.pl/pl/1_285.html [dostęp: 15 I 2017].

https://www.cisiiskuteczni.pl/akademia/trzy-kolory-czarny-zielony-i-niebieski [dostęp: 29 I 2017, 4 II 2017].

http://cisiiskuteczni.pl/jestem-komandosem/zadania-jednostki [dostęp: 4 I 2017].

http://www.formacjasgo.pl/portfolio-view/akcje-bezposrednie-da-rodzaje-i-charakter/ [dostęp: 1 IX 2019].

https://formoza.wp.mil.pl/pl/pages/kierownictwo-2017-01-16-4/ [dostęp: 25 VIII 2019].

http://historia.org.pl/2013/03/08/szturm-na-terminal-grom-w-porcie-umm-kasr/ [dostęp: 11 II 2017].

http://www.polska-zbrojna.pl/home/articleshow/28871# [dostęp: 25 VIII 2019].

www.rocznikbezpieczenstwa.dsw.edu.pl/fileadmin/user_upload/.../2011_12.pdf [dostęp: 15 I 2017].

http://www.special-ops.pl/leksykon/id245,hostage-rescue-force-jednostka-ratowania-zakladnikow-hrf [dostęp: 2 I 2017].

http://www.special-ops.pl/leksykon/id97,niebieska-taktyka [dostęp: 24 VII 2017].

http://www.special-ops.pl/leksykon/id127,zielona-taktyka [dostęp: 24 VII 2017].

https://specjalsi.wordpress.com/2013/08/22/leksykon-specjalsow-akcje-bezposrednie/ [dostęp: 3 VI 2017].

https://weaponsandwarfare.com/2018/09/21/joint-special-operations-command/ [dostęp 25 VIII 2019].

http://pl.wikipedia.org/wiki/Jednostka_Wojskowa_GROM [dostęp: 1 IX 2019].

Abstrakt

W pierwszej części artykułu dotyczącego jednostek specjalnych przedstawiono działania oraz rozwój tego typu formacji, a także ich podział na lądowe oddziały specjalne, jednostki antyterrorystyczne, morskie oddziały specjalne oraz powietrzne oddziały

specjalne. Następnie opisano struktury operacji specjalnych przeprowadzanych przez jednostki specjalne, z podziałem na poszczególne działania, takie jak: rozpoznanie specjalne, akcje bezpośrednie, wsparcie militarne, reagowanie kryzysowe, odbijanie zakładników, fizyczne zwalczenie terroryzmu, uwalnianie osób przetrzymywanych lub przebywających na zagrożonych terenach, działania niekonwencjonalne.

W dalszej części opisano morskie działania specjalne oraz jednostki specjalne, które je realizują. Zaprezentowano również rodzaje taktyk stosowanych przez wojska specjalne, tj.: „taktykę czarną", „taktykę zieloną", „taktykę niebieską", a także „taktykę czerwoną", „taktykę szarą" i „taktykę białą".

Słowa kluczowe: wojska specjalne, operacje specjalne, jednostki specjalne, taktyki, planowanie i realizacja operacji specjalnych, „taktyka czarna", „taktyka niebieska", „taktyka zielona", „taktyka czerwona".

Abstract

Another article about special units. The first part of the text mentions the activities and development of special units, as well as the division of special units into land special units, anti-terrorist units, special naval units and air special units. Next, the article contains, among others, a description of the structure of special operations, which are carried out by special units, divided into individual operations. Special operations carried out by Polish special units are discussed, with the specification of individual special units such as special reconnaissance, direct actions, military support, crisis response, taking back hostages, physical combat of terrorism, release of persons held or present in endangered areas, unconventional activities.

The following section describes special naval activities and the special units that carry them out. It also presents the types of tactics used by special forces, such as "black tactics", "green tactics", "blue tactics", as well as "red tactics", "grey tactics" and "white tactics".

Keywords: special forces, special operation, special units, tactics, planning and implementation of special operations, black tactic, blue tactic, green tactic, red tactic.

II

RECENZJE

REVIEWS

Krzysztof Izak

Magdalena El Ghamari, *Cool jihad*[1]

W 2018 r. na rynku księgarskim ukazało się kilka książek polskich autorów na temat Państwa Islamskiego. Do recenzji wybrałem publikację Magdaleny El Ghamari[2]. Autorka, jak pisze w notce biograficznej, jest kierownikiem Pracowni Bezpieczeństwa Kulturowego Collegium Civitas, fundatorem i prezesem Fundacji El-Karama, wykładowcą akademickim i szkoleniowcem, autorką tekstów z zakresu bezpieczeństwa międzynarodowego, międzykulturowości oraz kultury arabsko-muzułmańskiej. Jest członkiem licznych organizacji, w tym: Stowarzyszenia Euro-Atlantyckiego, European Association for Security, Stowarzyszenia Kombatantów Misji Pokojowych ONZ, Polskiego Towarzystwa Nauk o Bezpieczeństwie, Polskiego Towarzystwa Studiów Międzynarodowych, Towarzystwa Polsko-Albańskiego, International Institute for Private i Commercial and Competition Law w Tiranie. Zasiada w redakcjach magazynów: „e-Terroryzm", „Securitologia" i „Security Review". Szkoliła uczestników polskich kontyngentów wojskowych w zakresie środowiska prowadzenia operacji oraz obszarów wysokiego ryzyka. Współpracuje z wieloma uniwersytetami w Polsce i za granicą, w tym z uniwersytetami w Tiranie (Albania) i Prisztinie (Kosowo), gdzie prowadzi wykłady oraz konferencje. Jako szkoleniowiec współpracuje także z Centrum Współpracy Cywilno-Wojskowej (CCOE) przy NATO w Holandii[3].

Na początku swojej książki autorka zapowiada wieloaspektową prezentację doktryny dżihadu w ujęciu historycznym, psychologicznym i propagandowym. Zamiast wstępu na kilku stronach rozwija tezę: „wojna nieprawdopodobna, pokój niemożliwy", sformułowaną po raz pierwszy w 1948 r. przez francuskiego filozofa i politologa Raymonda Arona (1905–1983), wielokrotnie cytowaną w celu zdefiniowania stosunków międzynarodowych panujących w okresie zimnej wojny (1945–1991)[4]. Magdalena

---

[1] M. El Ghamari, *Cool jihad*, Warszawa 2018, Difin, s. 247.

[2] Zob. też inne książki poświęcone Państwu Islamskiemu wydane w 2018 r. przez wydawnictwo Difin: O. Wasiuta, S. Wasiuta, P. Mazur, *Państwo Islamskie ISIS. Nowa twarz ekstremizmu*, Warszawa; A. Wejkszner, *Samotne wilki kalifatu? Państwo Islamskie i indywidualny terroryzm dżihadystyczny w Europie Zachodniej*, Warszawa.

[3] Więcej informacji na temat Magdaleny El Ghamari można znaleźć w wywiadzie, którego udzieliła w 2017 r. magazynowi „Fronda". Zob. http://www.fronda.pl/a/dr-magdalena-el-ghamari-dla-frondy-europa-w-tym-polska-bedzie-muzulmanska-chyba-ze-wyciagniemy-wnioski-z-blednej-polityki-zachodu,88519.html [dostęp: 3 III 2017].

[4] Raymond Aron jako tytułu pierwszej części pracy *Le grand Schisme* (*Wielka Schizma*) z 1948 r. użył sformułowania *Paix impossible, guerre improbable* (*Pokój niemożliwy, wojna nieprawdopodobna*).

El Ghamari cytuje tę sentencję (bez podania autora) m.in. w celu ukazania obecnego stanu permanentnego zagrożenia terroryzmem i dżihadem jako zjawiska modnego i atrakcyjnego (ang. *cool*) dla młodego pokolenia muzułmanów, którzy z dumą propagują symbolikę i hasła Państwa Islamskiego. Są oni również bojownikami i uczestnikami wojny pomiędzy światem islamu a Zachodem. Walka stała się dla nich szansą na zmianę sposobu życia, przejawem buntu i sposobem odreagowania frustracji. Uczestniczą w niej jako obrońcy wyidealizowanego systemu społeczno-polityczno-religijnego, jakim jest najnowsza forma kalifatu.

Historyczne ujęcie dziejów kalifatu jest treścią pierwszego rozdziału pt. *Powrót do przeszłości – muzułmański czy islamski kalifat?* Trudno zrozumieć, w jakim celu autorka postawiła pytajnik i dlaczego używa dwóch różnych przymiotników mających to samo znaczenie. Być może miała na myśli „islamistyczny kalifat". Byłoby to jednak określenie mało poprawne. Autorka nam tego nie wyjaśnia. Pisze natomiast, że skupi się na początkach powstania kalifatu i pojawieniu się koncepcji dżihadu, poruszy także zagadnienie dotyczące istoty męczeństwa w islamie. Wymienia dziesięć kalifatów istniejących w przeszłości i w czasach współczesnych, a wśród tych ostatnich – cyt.: *Państwo Islamskie (2014–...)?* oraz *Ahmadidżę (1908–2014)*. Autorka miała zapewne na myśli kalifat Ahmadijja (Ahmadiyya) ustanowiony w 1908 r. po śmierci Mirzy Ghulama Ahmada, założyciela wspólnoty Ahmadijja. Ten kalifat istnieje do chwili obecnej, dlatego też niewłaściwe jest wskazanie daty końca jego istnienia (2014 r.). Autorka nie podała źródła tych informacji, lecz najprawdopodobniej zaczerpnęła je z artykułu Sylwestra Szafarza *Narodziny nowego kalifatu islamskiego*, zamieszczonego w „Przeglądzie Socjalistycznym"[5]. Brakuje daty wydania tego magazynu, ale z treści artykułu wynika, że został on napisany w 2014 r., po ogłoszeniu przez Abu Bakra al-Bagdadiego restytucji kalifatu jako Państwa Islamskiego (26 czerwca). Również Szafarz popełnił w swoim artykule kilka kardynalnych błędów, m.in. podając rok 1447 jako datę założenia rodu Saudów przez Muhammada ibn Sauda, co tak naprawdę miało miejsce w XVIII w., oraz wymieniając Indie i Chiny jako mocarstwa islamskie.

Kontynuując wątek historycznych kalifatów, El Ghamari pisze na s. 21: *Rozważania należałoby zacząć od pierwszego tworu, do którego odwołują się współcześni bojownicy kalifatu, mianowicie od Wielkiego Kalifatu Islamskiego – państwa powstałego po śmierci Muhammada w 632 roku. Rządzone było do 661 roku przez kalifów, nazywanych prawowiernymi. Wielki Kalifat Islamski upadł wraz z podbojem Egiptu przez imperium osmańskie w 1517 r.* W tym fragmencie dostrzegam poważną niekonsekwencję: skoro Wielki Kalifat Islamski był rządzony do 661 r. przez kalifów prawowiernych (sprawiedliwych), to nie mógł trwać do 1517 r. Po kalifach prawowiernych nastąpił okres panowania kalifów z dynastii Umajjadów (661–750) i Abbasydów (750–1258). Następnie egipscy mamelucy do 1517 r. utrzymywali w Kairze spadkobierców kalifatu. Ten sam błąd i brak logicznej ciągłości istnienia kalifatu znajduje się również w haśle „Kalifat", zamieszczonym w Wikipedii: *Wielki Kalifat*

[5] http://przeglad-socjalistyczny.pl/opinie/sprawy-midzynarodowe/1051-szafarz [dostęp: 24 I 2016].

Islamski – państwo powstałe po śmierci Mahometa w 632 roku, rządzone do 661 roku przez kalifów prawowiernych; upadło wraz z podbojem Egiptu przez Imperium Osmańskie w 1517 roku[6]. Niepoprawna wydaje się sama nazwa „Wielki Kalifat Islamski", w dodatku pisana dużą literą, gdyż nie precyzuje ona, o który kalifat tak naprawdę chodzi. Odniesienie tej nazwy do okresu zawartego między datami 632–1517 jest nonsensem, gdyż po zdobyciu Bagdadu przez Tatarów w 1258 r. kalifat właściwie przestał istnieć. Co prawda mamelucki sułtan Bajbars w 1260 r. przeniósł do Kairu obalony kalifat Abbasydów w celu legitymizacji swoich rządów i gościł w swojej stolicy kalifa, ale był on marionetką odgrywającą niewielką rolę w życiu religijnym państwa mameluków[7].

Autorka małą literą pisze „imperium osmańskie", dużą „Imperium Rzymskie", mimo że wspominając czasy muzułmańskiego podboju, należałoby raczej używać określenia Cesarstwo Bizantyjskie. Myli rody z plemionami. Kurajszyci według niej to ród, a nie plemię, do którego należał ród proroka Muhammada – Haszymici. Następnie pisze: *Usman ibn Affan należał do plemienia Omajjadów, które było gałęzią rodu Kurajszytów*. Zdanie poprawnie powinno brzmieć: *Usman ibn Affan należał do rodu Omajjadów, który należał do plemienia Kurajszytów*. Prozelitami kilkakrotnie nazywa towarzyszy proroka Muhammada nawróconych na islam, choć bardziej stosowne byłoby określenie „neofici".

Autorka zamieściła na s. 22 schemat, podpisany jako opracowanie własne, obrazujący pochodzenie Muhammada, którego wywodzi od Abrahama. Podobne informacje znajdują się w załączniku nr 2 zamieszczonym na końcu książki, zawierającym rozbudowane drzewo genealogiczne Muhammada, którego bardzo dalekim przodkiem miał być Adam[8]. Szkoda, że zabrakło słów komentarza, że ta genealogia jest głęboko zmitologizowana i nie znajduje żadnego potwierdzenia w źródłach historycznych. Nie mogę się zgodzić z twierdzeniem autorki, która pisze o Usmanie, że był dobrym kalifem dbającym o państwo i muzułmanów. W rzeczywistości był to pierwszy kalif, który najważniejsze stanowiska w państwie obsadzał członkami swojego rodu, co zresztą przyczyniło się do jego śmierci w 656 r.

Błędne jest stwierdzenie: *W 909 roku w Kairze Fatymidzi, ród szyitów*, *stworzył własny kalifat, konkurencyjny w stosunku do sunnickiego*. Rok 909 jest dopiero początkiem panowania dynastii Fatymidów. Jej założyciel Ubajd Allah w tym właśnie roku obalił charydżycką dynastię Rustamidów w Taharcie (obecnie Tiaret, Algieria), i dynastię Aghlabidów w Tunezji. Dopiero w 969 r. wojska czwartego fatymidzkiego kalifa Al-Mu'izza (panował w latach 953–975) przybyły do Egiptu. W tym samym roku wódz jego wojsk, Dżawhar al-Sikilli, założył obóz wojskowy, zamieniony następnie w miasto garnizonowe położone na północny wschód od istniejących już miast Fustat,

[6] https://pl.wikipedia.org/wiki/Kalifat [dostęp: 3 X 2018].

[7] W 1412 r. władzę w Egipcie przejął na krótko abbasydzki kalif Al-Musta'in, ale po kilku miesiącach został obalony przez Mameluka Mu'ajjada Szajcha.

[8] https://en.wikipedia.org/wiki/File:Family_Tree_of_Prophets.png [dostęp: 3 X 2018].

Al-Askar i Al-Katai (obecnie dzielnica Stary Kair), które z łatwością zdobył po obaleniu lokalnej dynastii Ichszydydów (935–969). Cztery lata później kalif Al-Mu'izz przeniósł dwór z Mahdiji w Tunezji do nowo zbudowanego miasta, ogłosił je stolicą swego kalifatu i nazwał Al-Kahira. Później tę nazwę zniekształcono do formy: Cairo, od której pochodzi współczesna nazwa Kairu. Są to szczegóły, ale moim zdaniem istotne, tym bardziej że podobnych pomyłek dotyczących dat, miejsc i zdarzeń jest więcej. Nie powinny się one znaleźć w książce o charakterze naukowym lub popularnonaukowym.

Rozdział drugi nosi tytuł *Allahu Akbar!!! – wojna i jej sakralizacja*. Autorka odniosła się w nim do męczeństwa w islamie, które to zagadnienie – zgodnie ze wstępną zapowiedzią – powinno być omówione w rozdziale pierwszym. El Ghamari potraktowała ten temat bardzo wybiórczo i skrótowo, co zupełnie nie oddaje idei męczeństwa wyznawców islamu. Znalazło się tu więcej informacji na temat dżihadu niż istoty męczeństwa, mimo że problematyka dotycząca dżihadu jest poruszana także w innych rozdziałach. To rozproszenie negatywnie wpływa na treść publikacji. Jasność przekazu burzy krótki, *ad hoc* wtrącony wykład na temat *Koranu*, zasad wiary i filarów islamu. Autorka niepotrzebnie też połączyła męczeństwo i dżihad z *takiyyą* (*takijją*), czyli ukrywaniem własnego wyznania, nie oddając przy tym historycznego znaczenia tego pojęcia, związanego z szyizmem. W celu opisania wymienionego zjawiska, w kontekście współczesnego dżihadyzmu, bardziej stosowne jest określenie *tawrijja* – religijnie usankcjonowane kłamstwo, a nawet sprzeniewierzenie się własnej religii czy też jej porzucenie jako taktyka walki z wrogami islamu. Do takich postaw zachęcało Państwo Islamskie, publikując w 2015 r. instruktaż *How to Survive in the West. A Mujahid Guide* mówiący o tym, jak skutecznie wtopić się w europejską społeczność, o czym El Ghamari nie wspomniała. Trudno też pogodzić się z niektórymi poglądami, na przykład z porównaniem dżihadu do wojny sprawiedliwej, ważniejszej roli dżihadu ducha, czyli walki z własnymi przywarami i słabościami (*dżihad al-akbar* – dżihad większy), niż dżihadu miecza (*dżihad al-asghar*). A przecież to walka zbrojna była w dziejach islamu dżihadem większym. Ten pogląd podzielają autorzy krytyczni wobec islamu, którzy zwracają uwagę na to, że dżihad duchowy był mało istotny w historii muzułmanów. To muzułmańscy apologeci i zwolennicy dialogu międzyreligijnego starają się ukazywać pokojowy charakter dżihadu, pozbawiony przemocy. Jednocześnie, jeśli weźmie się pod uwagę, że okrucieństwo czynione w imię Chrystusa było wypaczeniem jego nauk, to w odróżnieniu od islamu, w którym walka prowadzi do zbawienia, trudno zgodzić się ze stwierdzeniem, że: (…) *doktryna dżihadu jest wręcz bardziej humanitarnym rozwiązaniem niż praktykowane średniowieczne bulle papieskie. Bulle papieskie nakazywały prześladowania i mordowanie wszystkich heretyków* (…). Dla usprawiedliwienia autorki należy wyjaśnić, że nie jest to jej opinia, lecz cytat z książki Moniki i Udo Tworuschka pt. *Religie świata – Islam* (Warszawa 2009, s. 135). Do zorganizowania wyprawy krzyżowej wzywał w 1095 r. papież Urban II, a nie Urban IX (s. 46).

Zwraca uwagę brak zachowania jednolitej pisowni słowa „*jihad*", „dżihad" oraz angielski zapis słowa „*Takiyya"/„takiyya"* raz dużą, raz małą literą. Małą literą

powinno być również pisane słowo „hadisy". Słowo „sunna" autorka też pisze raz dużą, raz małą literą, przy czym używa także liczby mnogiej: „Sunny". Jednak to słowo występuje wyłącznie w liczbie pojedynczej (*sunna*) i oznacza „drogę", w tym przypadku drogę proroka Muhammada, na którą składają się hadisy, czyli opowieści dotyczące wypowiedzi i czynów proroka. W szerszym ujęciu sunna to praktyka, obyczaj, tradycja, ustanowiona przez proroka Muhammada na podstawie jego czynów, wypowiedzi, a nawet przemilczeń, czyli zachowań, na które zezwalał, które aprobował lub których zakazywał. Sunna jest po *Koranie* drugim źródłem szariatu.

Chaos i brak zakończenia poruszanych tematów są widoczne na dalszych stronach książki. W podrozdziale *Idżtihad i wahi ekstremistów islamskich* autorka powraca do problematyki męczeństwa, tym razem w odniesieniu do współczesnych operacji męczeńskich. Wymienia publikację Braci Muzułmanów: *Al-Amalijjat al-istiszhadijja hua al-hall* (*Operacje męczeńskie są rozwiązaniem*) i książkę Nawwafa at-Takruriego: *Al-Amalijjat al-istiszhadijja fi al-mizan al-fikhi* (*Operacje męczeńskie w systemie prawnym*), wydaną w 2003 r. w Damaszku. W tej ostatniej publikacji autor opisał 16 udanych zamachów samobójczych i wskazał na zasadność ich przeprowadzenia z uwagi na olbrzymią przewagę przeciwnika. Wymienił również fatwy (orzeczenia o zgodności postępowania z normami islamu), które uzasadniały te działania.

Autorka poświęciła zbyt mało uwagi islamskim organizacjom ekstremistycznym, przy czym ograniczyła się wyłącznie do Afryki, zapominając jednocześnie o somalijskim Harakat asz-Szabab al-Mudżahidin (Ruch Młodych Mudżahedinów). Nie ustrzegła się kolejnych, mało precyzyjnych sposobów zapisu nazw własnych i niejasnych sformułowań. Na przykład w zdaniu na s. 77: *Tuaregowie domagający się utworzenia na Saharze własnego państwa, tak zwany AZAWAD, początkowo połączyli się z grupami bliskimi ideologicznie Al-Kaidzie z Islamskiego Maghrebu (AQIM)*. Użycie wersalików w słowie „AZAWAD" może oznaczać, że jest to akronim, podczas gdy jest to nazwa regionu w północnej części Republiki Mali. Przekonanie o tym, że jest to akronim, wzmacnia użycie wersalików do zapisu akronimu nazwy organizacji Al-Kaida Islamskiego Maghrebu (*Al-Qaeda in the Islamic Maghreb*, AQIM). W następnym zdaniu informuje: *Wśród nich wymienia się m.in. Mujao, czyli zachodnioafrykański odłam AQIM Ansar Dine (Obrońcy Wiary), który politycznie skorzystał na rebelii Tuaregów*. Należy sprostować, że słowo „Mujao" jest akronimem nazwy organizacji (Ruch na rzecz Jedności i Dżihadu w Afryce Zachodniej), powinno więc być zapisane wersalikami. Ponadto AQIM i Ansar Dine (lub Ansar ad-Din) to dwie różne organizacje – ich nazwy powinny być rozdzielone przecinkiem lub spójnikiem „i". Dodatkowo: MUJAO nie była odłamem AQIM, lecz niezależnym ugrupowaniem, które w październiku 2011 r. oddzieliło się w Mali od AQIM. W następnym akapicie skrót „MUJAO" jest zapisany poprawnie, wyjaśniono też, czego dotyczy, ale brakuje rozwinięcia nazwy tej organizacji w języku francuskim, ponieważ do niej odnosi się ten akronim – Mouvement pour l'unicité et le jihad en Afrique de l'Ouest. I jeszcze jedna ważna uwaga. El Ghamari, pisząc o tych organizacjach, używa czasu teraźniejszego, podczas gdy Ansar ad-Din (Obrońcy Wiary) w 2013 r. uległo rozłamowi, w wyniku

którego powstał Islamski Ruch Azawad (Mouvement islamique de l'Azawad). W tym samym roku podpisał on porozumienie kończące walki między Tuaregami i malijskimi siłami rządowymi. Z kolei MUJAO w sierpniu 2013 r. połączyło się z organizacją Katibat al-Mulassamin (Zamaskowany Batalion), zwaną też Muwaka'un bi ad-Dima (Podpisani Krwią), założoną w grudniu 2012 r. przez Mochtara Belmochtara, i utworzyło ugrupowanie Al-Murabitun (Strażnicy). Belmochtar był wcześniej jednym z dowódców AQIM, ale nieporozumienia w gronie kierownictwa organizacji skłoniły go do utworzenia własnych sił. Natomiast w 2014 r. z AQIM wydzieliła się Dżund al-Khilafa fi Ard al-Dżazira (Armia/Żołnierze Kalifatu w Algierii) z Abdelmalekiem Gurim na czele. W maju 2015 r. od Al-Murabitun odłączyła się grupa pod dowództwem Adnana Abu Walida as-Sahrawiego, wcześniej rzecznika MUJAO, który złożył przysięgę lojalności Państwu Islamskiemu. Ugrupowanie As-Sahrawiego zostało nazwane Ad-Dawla al-Islamijja fi as-Sahara al-Kabira (l'Etat islamique dans le Grand Sahara – EIGS, Państwo Islamskie Wielkiej Sahary). Jest ono aktywne w północnej części Republiki Mali. Natomiast Belmochtar, którego śmierć ogłaszano kilka razy (w styczniu 2016 r. Departament Stanu usunął nazwisko Belmochtara z listy terrorystów, za których wyznaczono wysokie nagrody), pozostał wierny Al-Kaidzie. W marcu 2017 r. nastąpiło połączenie organizacji Al-Murabitun, Ansar Din, OAKIM i Front de liberation du Macina, FLM (Front Wyzwolenia Maciny). W wyniku tego sojuszu powstała Dżama'at Nusra al-Islam wa al-Muslimin (Grupa Wsparcia Islamu i Muzułmanów). Tych ważnych informacji w książce, niestety, już nie znajdziemy. Wygląda więc na to, że przedstawianie problematyki dżihadu w Afryce Zachodniej autorka zakończyła na wydarzeniach z 2012 r., które zresztą opisała bardzo ogólnikowo.

W analizie zjawiska, jakim jest fundamentalizm islamski (zawartej w następnym podrozdziale), znalazła się kolejna nieścisłość (zdanie na s. 81): *Około roku 1910–1915 dwóch pastorów w Stanach Zjednoczonych zaczęło wydawać serie broszur zatytułowanych „The Fundamentals". Były one rozdawane wśród wiernych kościoła* (...). Opisana działalność rzeczywiście miała miejsce w latach 1910–1915. W tym okresie wydano serię 12 broszur zatytułowanych *The Fundamentals: A Testimony to the Truth* lub po prostu *The Fundamentals*. Zawierały one 90 artykułów, w których czołowi amerykańscy konserwatywni teolodzy tłumaczyli dogmaty protestantyzmu, dotyczące m.in.: nieomylności *Pisma Świętego* i jego niepodważalnego charakteru, narodzenia Jezusa z Dziewicy, odpokutowania przez Chrystusa na krzyżu ludzkich grzechów, jego cielesnego zmartwychwstania, realności czynionych przez niego cudów czy absolutnej pewności paruzji (ponownego nadejścia Chrystusa jako Zbawiciela). Nieścisłość dotyczy informacji o osobach je wydających, gdyż publikację broszur finansowali bracia Lyman i Milton Stewartowie, milionerzy i filantropi (majątku dorobili się na wydobyciu ropy naftowej), a nie dwaj pastorzy. Łącznie opublikowano ponad 3 mln broszur, które rozsyłano pastorom i kaznodziejom, osobom świeckim, szkołom i uczelniom religijnym w całych Stanach Zjednoczonych. Kontynuując rozważania na temat fundamentalizmu, autorka wymienia teksty starożytne, których przekaz jest znany również z *Biblii*. Pisze o nich: *Manuskrypty z Sumeru, Babilonii, Asyrii*

i Mezopotamii wykazywały istotne podobieństwa do tekstów biblijnych (s. 88). Jednak nie były to manuskrypty, lecz słynne tabliczki z wypalonej gliny pokryte pismem klinowym, a wymienione starożytne królestwa: Sumer, Babilonia i Asyria były położone na terenie Mezopotamii. Nieprawdziwe jest również stwierdzenie: *Kolejno od lat 80.* (XX w. – przyp. red.) *fundamentalizm religijny objął wszystkie najważniejsze religie*. Fundamentalizmy: chrześcijański, islamski, hinduistyczny czy sikhijski upowszechniły się jednak znacznie wcześniej. Najmłodszy z nich to fundamentalizm judaistyczny, który zaczął wywierać duży wpływ na scenę polityczną w Izraelu po zakończeniu wojny sześciodniowej w 1967 r. Od lat 80. ubiegłego wieku wzrasta natomiast liczba aktów przemocy motywowanych religią. W kilku zdaniach, których treść dotyczy fundamentalizmu w Turcji, autorka też popełniła błędy. Partia Dobrobytu (Refah Partisi) została zdelegalizowana w styczniu 1998, a nie w 1999 r., Partia Cnoty (Fazilet Partisi) powstała w grudniu 1997 r. zanim zdelegalizowano Partię Dobrobytu, którą w styczniu 1998 r. zastąpiła na scenie politycznej. Partię Cnoty rozwiązano w czerwcu 2001 r., a nie w 2000 r. Z kolei Partię Sprawiedliwości i Rozwoju (Adalet ve Kalkinma Partisi, AKP) powołano do życia w połowie sierpnia 2001 r., a już w następnym roku wygrała ona wybory parlamentarne i rozpoczęła samodzielne rządy trwające do chwili obecnej. Od kilku lat AKP przestała realnie zabiegać o przystąpienie Turcji do Unii Europejskiej, mimo starań czynionych od 2005 r. W związku z tym nieprawdziwe jest stwierdzenie na s. 97: *W 2003 r. rząd w Turcji utworzył Partię Sprawiedliwości i Rozwoju (Adalet ve Kalkinma Partisi), także o tendencjach fundamentalistycznych, ale bardziej liberalną – i to ona obecnie prowadzi zabiegi mające na celu wprowadzenie Turcji do EU, co może się wydawać paradoksalne, gdyż fundamentaliści zazwyczaj bywają wrogo nastawieni wobec świata zachodniego*.

Przyznam, że musiałem przetrzeć oczy i ochłonąć ze zdumienia po przeczytaniu następującego fragmentu na s. 102: *Po wydarzeniach z 11 września 2001 r. obraz muzułmanów oraz samego islamu może nie tyle się zmienił, co został wzmocniony. Wcześniej straszono islamem, a był on na tyle daleko, że nikt z nas nawet o tym nie myślał. Po ataku na Amerykę wiele się zmieniło, a najbardziej zakres oddziaływania tak zwanego islamu. Trudno bowiem mówić o atakach z 11 września i używać jednocześnie synonimu religii muzułmańskiej, bowiem zamachu dokonała radykalna grupa terrorystyczna, która ma niewiele wspólnego z islamem. Świadczy to nawet już o prawach wojny, które zostały wymienione w poprzednim rozdziale. Żadna z zasad prowadzenia wojny nie zgadza się z zasadami Koranu i nimi nie jest*. Pomijam styl, zwracam natomiast uwagę na pokrętne rozumowanie. Jeśli sprawcami zamachów w USA we wrześniu 2001 r. nie byli muzułmanie, to kto? Przecież przed tym aktem terroryzmu dochodziło już do poważnych ataków w Egipcie, Jemenie, Somalii, Arabii Saudyjskiej, Pakistanie, Kenii, Tanzanii, Francji, nie wspominając już o wojnach domowych w Algierii, Afganistanie, Bośni i Hercegowinie. Opinii publicznej nie trzeba było straszyć islamem, bo on już przed zamachami z 11 września 2001 r. był źródłem poważnych obaw i lęku społeczeństw w krajach zachodnich. Potęgowały go wystąpienia radykalnych kaznodziejów w meczetach w Wielkiej Brytanii oraz

Francji, którzy wzywali do zniszczenia Zachodu. Oczywiście trudno znaleźć zależność islamskich ataków przeprowadzanych przez terrorystów od zapisów zawartych w *Koranie*, gdyż diametralnie zmieniły się metody, sposoby i środki prowadzenia wojny. Jednak terroryzm to nic innego jak kontynuacja dżihadu w nowej formie, a dżihad jest usprawiedliwiany przez wielu islamskich teologów, znajdujących jego uzasadnienie w *Koranie* i sunnie. Nieco dalej – na s. 116 – autorka, zaprzeczając sobie w kolejnych zdaniach, powraca do tej obłudnej retoryki, bo jak inaczej można określić następujące opinie: *Organizacje islamskie wykorzystują sojusze z innymi ugrupowaniami, których spoiwem jest jedna, ale bardzo silnie wyznawana religia. W obliczu sytuacji zapomina się, że to* [,] *co wyznają ekstremiści islamscy, to nie islam, to nie nakazy Boga, a tym bardziej nie dobro pojedynczego człowieka. Islam stał się jednym z wielu narzędzi terrorystów, ekstremistów oraz fundamentalistów islamskich. Nawet sama ich nazwa wskazuje już na związki z religią. Za zasłoną religii muzułmańskiej ugrupowania islamistyczne organizują się, mobilizują, szkolą, werbują ludzi, a co gorsza szerzą strach, przerażenie oraz śmierć niewinnych ludzi*. Pozostawiam ten fragment bez komentarza, do „przetrawienia" przez uważnego czytelnika. Mam tylko małą uwagę: czyżby autorka zapomniała, że w islamie nie przywiązuje się uwagi do dobra pojedynczego człowieka, lecz do dobra *ummy*, czyli społeczności muzułmańskiej?

Strony od 107 do 111 El Ghamari poświęca zagranicznym operacjom wojskowym w kontekście międzykulturowym, a więc problematyce, którą wykładała żołnierzom wyjeżdżającym na misje do Iraku i Afganistanu, ale zupełnie niezwiązanej z tematem książki. Ten wątek, burzący narrację, należałoby całkowicie pominąć. Zamiast niego byłoby wskazane poszerzenie kolejnego podrozdziału, noszącego niezrozumiały tytuł: *Nikt nie widział nikt nie słyszał – czyli fronty fundamentalistyczne na Bliskim Wschodzie do 2011 roku.* Wyjaśnienia, dlaczego nikt nie widział i nikt nie słyszał, trudno szukać w tekście. Jeśli chodzi o ataki terrorystyczne, to wiadomo, kto je przeprowadzał. Także kolejne miejsca pobytu Osamy bin Ladena oraz innych przywódców islamskich organizacji ekstremistycznych były znane, przynajmniej w przybliżeniu. Poza tym Bin Laden urodził się 10 marca 1957 r. w Rijadzie, w Arabii Saudyjskiej, a nie w Jemenie, jak podaje autorka, która niepotrzebnie ponownie powraca do problematyki fundamentalizmu. Na s. 115 pisze: *Organizacje terrorystyczne, które działały czy też działają w Europie, to między innymi IRA czy też Irlandzka Armia Republikańska.* IRA jest akronimem Irish Republikan Army, czyli Irlandzkiej Armii Republikańskiej. Według autorki: *Jedyną drogą ratunku, upatrywaną przed destabilizacją w krajach arabskich, Pakistanie, Jemenie i Afganistanie, jest ponowne objęcie władzy w kraju przez wojskowych*. *Dokonanie zamachu stanu i obalenie obecnego cywilnego rządu. Sam fakt wydaje się niedorzeczny, bo przecież „będzie jeszcze gorzej", ale coraz częściej taki scenariusz jest postrzegany jako jedyna szansa dla tego regionu. Osobiście również popieram taki scenariusz, upatrując w nim jedynego w miarę sensownego rozwiązania. Nie tylko dla ratowania kraju przed rządami fundamentalistycznymi, ale i dostaniem się w ręce terrorystów arsenału nuklearnego – co jest najgorsze – do ocalenia państwowości tych krajów oraz żyjących tam ludzi*. Jemen jest również

państwem arabskim, więc niepotrzebnie został wymieniony obok Pakistanu i Afganistanu. Ponadto cytowany fragment nie jest jednak zgodny z prawdą, ponieważ wojskowi dyktatorzy w krajach muzułmańskich nie byli i nie są w stanie ochronić obywateli przed atakami terrorystycznymi, a niektórzy z nich prowadzili politykę reislamizacji społeczeństwa. Przykładem są rządy prezydenta gen. Muhammada Zia ul-Haqa w Pakistanie (1977–1988), a w Egipcie – gen. Anwara as-Sadata (1970–1981). Zamach stanu przeprowadzony przez wojskowych w Algierii w 1992 r. doprowadził do wieloletniej krwawej wojny domowej. W Afganistanie po obaleniu w 1973 r., w wyniku bezkrwawego zamachu stanu, ostatniego króla Muhammada Zahera (Zahira) Chana, tylko pierwszy prezydent, Muhammad Daud Chan (1973–1978) był wojskowym, natomiast dwaj następni: Nur Muhammad Taraki (1978–1979) i Hafizullah Amin (wrzesień–grudzień 1979 r.) – sprawujący tę funkcję do czasu wkroczenia armii radzieckiej do Afganistanu w grudniu 1979 r., byli politykami cywilnymi. Arabska Wiosna w 2011 r. pokazała, że społeczeństwo potrafi obalić władzę wojskowych dyktatorów i w wyniku wyborów oddać władzę religijnym ekstremistom. Przykładem są Tunezja i Egipt. W tym drugim kraju autorytarna władza prezydenta Abda al-Fattaha as-Sisiego (3 lipca 2013 r. przeprowadził zamach stanu, w latach 2013–2014 był wicepremierem, a od 2014 r. jest prezydentem Egiptu) nie jest w stanie przeciwdziałać zamachom terrorystycznym, mimo wprowadzenia nadzwyczajnych środków bezpieczeństwa.

Autorka myli się zupełnie, jeśli chodzi o sprawcę (…) *udanego zamachu samobójczego, mającego miejsce 30 grudnia 2009 r. w prowincji Chost w Afganistanie na bazę CIA. Najfatalniejszym jest jednak to, że zamachowcem był oficer afgańskiego rządowego wojska, sponsorowanego i szkolonego przez Amerykanów* (s. 117). Otóż tym zamachowcem nie był żaden wojskowy, lecz zradykalizowany jordański lekarz, Humam Khalil Abu-Mulal al-Balawi alias Abu Dudżan al-Chorasani. W przeprowadzonym przez niego zamachu w bazie Chapman, w afgańskiej prowincji Chost, zginęło dziewięć osób, w tym siedmiu agentów CIA. Odsyłam Magdalenę El Ghamari do książki Joby'ego Warricka *Potrójny agent*[9]. Nie do przyjęcia jest też opinia autorki na temat braku możliwości położenia kresu terroryzmowi w systemie demokratycznym. Według niej można to uczynić jedynie (…) *redukując prawa demokracji, a może nawet odchodząc od niej zupełnie. Jedynym sposobem na pokonanie terroryzmu byłoby przejęcie funkcji terrorysty przez państwo, ale nie o to przecież chodzi*. Czy na pewno? Jeśli weźmie się pod uwagę działalność terrorystycznych organizacji lewackich i skrajnie prawicowych w krajach demokratycznych Europy Zachodniej w latach 70. i 80. XX w., nazywanych latami ołowiu, to zdecydowana reakcja służb specjalnych i policji doprowadziła do znacznego spadku aktywności tych ugrupowań, o ile nie do całkowitego ich wyeliminowania. Niewątpliwie przyczyną było również odwrócenie się społeczeństwa od idei głoszonych przez te ugrupowania. Z pewnością istnieje związek między systemami społeczno-politycznymi a terroryzmem, jednak ten ostatni może zagościć w każdych warunkach, nie wyłączając państw autorytarnych. ETA powstała przecież

[9] J. Warrick*, Potrójny agent. Kret Al-Kaidy, który oszukał CIA*, Kraków 2013.

w czasach dyktatorskich rządów gen. Francisca Franco (1892–1975). Terroryzm w Egipcie też trzyma się mocno. Przewrót wojskowy w Algierii dokonany w 1992 r. wywołał krwawą wojnę domową z islamistami. Wiele niedemokratycznych krajów Ameryki Łacińskiej również zostało naznaczonych terroryzmem.

Nie do końca zrozumiała jest treść trzeciego akapitu znajdującego się na początku rozdziału trzeciego pt. *Daesh – współczesny islamski kalifat* (s. 123). Postanowiłem zacytować i przeanalizować: *Mamy rok 2015, czy w obliczu kończących się operacji militarnych (Irak, Afganistan) nie nadeszła pora, by sporządzić bilans owej trwającej od 2001 roku wojny z terroryzmem? Nie odpowiem na pytanie, kiedy to się skończy, ale rola świadomości międzynarodowej naszego społeczeństwa jest jednym ze sposobów walki z tym zjawiskiem*. Czytając książkę, odniosłem wrażenie, że tak naprawdę została ona napisana trzy lata przed datą wydania (2018 r.), natomiast zdecydowana większość literatury, z której korzystała autorka, oraz wszystkie artykuły prasowe są datowane na pierwszą dekadę XXI w., a więc nie odpowiadają czasowo wydarzeniom przedstawianym w książce. Z tą opinią może się kłócić przypis nr 216 na s. 224, noszący datę dostępu 20 kwietnia 2017 r., oraz informacja na s. 227 o zamachu w Brukseli, bez podania daty (22 marca 2016 r.), ale to jedyne wzmianki, które wykraczają poza rok 2015. Czy w tym właśnie roku kończyły się operacje militarne, jak stwierdza autorka? Z końcem 2011 r. Amerykanie oraz ich sojusznicy wycofali swoje siły z Iraku, a trzy lata później – większość wojsk z Afganistanu, mimo to walki w tych krajach trwają nadal. Bilanse amerykańskiej obecności w Iraku i Afganistanie zostały już sporządzone przez różne think tanki i wypadły niekorzystnie dla USA, by nie powiedzieć – wstrząsająco. Na przykład interwencja w Iraku okazała się najbardziej spektakularną i krwawą militarną porażką Stanów Zjednoczonych w dziejach. Absolutnie nie zgadzam się ze stwierdzeniem autorki, że świadomość międzynarodowa naszego społeczeństwa (rozumiem, że ma ona na myśli społeczeństwo polskie) jest jednym ze sposobów walki z terroryzmem. „Świadomość międzynarodowa" jest, jak sądzę, skrótem myślowym autorki odnoszącym się do świadomości sytuacji międzynarodowej lub wiedzy na ten temat. Jednak jeśli chodzi o „nasze" społeczeństwo, to nie jest ona duża i z pewnością nie przekłada się na walkę z terroryzmem. Nie zmienia tego faktu obecność polskich kontyngentów wojskowych w Iraku i Afganistanie.

Na kolejnych stronach rozdziału trzeciego, tak jak dwóch poprzednich i następnego, zwracają uwagę powtórzenia tych samych treści oraz niepotrzebnie poruszone, niedokończone tematy, które są kontynuowane na dalszych stronach, burząc w ten sposób tok narracji. Na przykład informacje dotyczące genezy Państwa Islamskiego są podawane bez chronologicznego porządku na stronach 129–133, a następnie pojawiają się znowu w podrozdziale *„Oto Kalifat" – królestwo w ciągłej ekspansji*, na stronie 139 i następnych. Należy też poprawić kilka błędnych informacji. Muammar Kaddafi nie został zamordowany wiosną, lecz jesienią 2011 r. (dokładnie – 20 października). Nie istnieje „pustynia saharyjska". Na mapie nr 12 (s. 143) błędnie zaznaczono miasto Ramadi – kilkaset kilometrów na północny zachód od jego właściwego położenia.

Mało wiarygodna jest genealogia Abu Bakra al-Bagdadiego opracowana przez autorkę. Po pierwsze – dlatego że nie jest potwierdzona żadnymi źródłami, a po drugie – wskazuje na szyickie pochodzenie samozwańczego kalifa. W tym przypadku można zrozumieć autorkę, ponieważ Al-Bagdadi ogłosił się nie tylko kalifem, lecz także imamem, a tym samym – przywódcą wszystkich wyznawców Allaha na świecie[10]. Nie można mu zatem odmówić bujnej wyobraźni i megalomanii. W przedostatnim zdaniu na s. 150 autorka, pisząc o Abu Bakrze al-Bagdadim, stwierdza: *Zajmował się przerzucaniem przez granicę zagranicznych bojowników, następnie zaś został samozwańczym emirem Rawy*. Po czym w pierwszym zdaniu na s. 151 informuje: *Z czasem został emirem Rawy i jednocześnie przewodniczącym sądu muzułmańskiego*. W tym samym akapicie znajduje się zdanie: *Al-Baghdadi został zabity 19 kwietnia 2010 r. w wiosce As-Sarsar* (…) oraz kolejne: *Schedę po nim objął Abu Bakr al-Baghdadi*. Słowo „Baghdadi" autorka raz pisze z literą „h", innym razem już bez tej litery. Czytelnik nieznający dokładnie genezy Państwa Islamskiego z pewnością zada sobie pytanie, o co tu chodzi. Autorka, pisząc o śmierci Al-Bagdadiego na s. 151, zapomniała podać jego pełnych danych personalnych, czyli Abu Omar al-Bagdadi (wł. Hamid Dawud Muhammad Khalil az-Zawi, były oficer armii irackiej), o którym wcześniej nie pisała. Trudno zatem zrozumieć, jeśli nie zna się historii powstania Państwa Islamskiego, o kogo chodzi. O Abu Omarze al-Bagdadim pisze dopiero na s. 158, gdy wraca do przerwanego wątku na temat Al-Kaidy w Iraku. Dalej stwierdza, mijając się z prawdą, że kary obowiązujące w kalifacie są niedozwolone w prawie koranicznym. Wprost przeciwnie, kary cielesne, z obcinaniem rąk i dekapitacją włącznie, obowiązują – zgodnie z hanbalicką wykładnią szariatu – w Arabii Saudyjskiej. Stosowane są także w Iranie. Na s. 157 zostały zamieszczone mało wiarygodne wykresy, które przedstawiają udział zagranicznych bojowników w walkach w Syrii (poprawnie podpis powinien brzmieć: w Syrii i Iraku), pochodzących z krajów Europy i USA oraz z państw muzułmańskich. Podano na nich nieprawdziwe liczby *foreign fighters* z poszczególnych krajów, którzy uczestniczyli w walkach na Bliskim Wschodzie w 2015 r. Ponadto El Ghamari nie jest autorką tego wykresu, podobnie jak wspomnianej wyżej mapki, przeniosła je z internetu, powinna jednak uważnie przyjrzeć się ich treści, a nie bezrefleksyjnie zamieszczać je w swojej publikacji. W jednym akapicie na s. 163 rażą czytelnika trzy błędy ortograficzne: „na bliskim wschodzie", „państw Europejskich", „Nie mniej jednak". Na dwóch następnych stronach są podane informacje na temat wydarzeń, do których doszło w maju, nie wiadomo jednak, którego roku. Z kontekstu można się domyślić, że chodzi o rok 2014. Nie da się natomiast wskazać, którego roku dotyczą wydarzenia opisane na s. 171. Autorka przy opisywaniu terrorystycznej działalności Boko Haram stwierdza: *Tylko w ciągu pięciu miesięcy tego roku odnotowano*

[10] Należy odróżnić imama w sunnizmie od imama w szyizmie. Ten pierwszy najczęściej prowadzi jedynie modlitwę i zarządza meczetem. Imam szyicki natomiast jest przywódcą całej społeczności. Imamami nazywano potomków Alego ibn Abu Taliba, zięcia proroka i czwartego kalifa sprawiedliwego. Imamem tytułowano również ajatollaha Chomeiniego.

27 zamachów samobójczych, w porównaniu z 26 w ciągu całego ubiegłego roku. Podobne sformułowanie – „rok temu", bez podania daty, znajduje się poniżej, w kontekście wydarzeń w belgijskim Liège. A w następnym rozdziale fragment zdania: (…) *wydarzenia z ostatnich tygodni*, znowu bez informacji o roku, w którym one nastąpiły.

Na początku czwartego rozdziału zatytułowanego *Cool jihad – propaganda kalifatu* autorka wymienia kolejno elementy działań terrorystycznych islamskich fundamentalistów[11] i stawia tezę, z którą trudno się zgodzić. Stwierdza mianowicie, że terroryzm (…) *jest możliwy tylko w społeczeństwach demokratycznych i wręcz nierealny w państwach niedemokratycznych*. Jako przykład wymienia zamach terrorystyczny w Madrycie z 11 marca 2004 r., zapomina natomiast o zamachach terrorystycznych w Iranie, Arabii Saudyjskiej, Egipcie oraz Maroku, a więc w państwach, które trudno uznać za demokratyczne.

Na kolejnych stronach El Ghamari podaje błędne daty i nazwy organizacji. Państwo Islamskie w Iraku i Lewancie (Islamic State of Iraq and the Levant – ISIL) nie powstało w 2003 r., lecz 8 kwietnia 2013 r., kiedy Abu Bakr al-Bagdadi ogłosił zmianę nazwy organizacji Ad-Dawla al-Irak al-Islamijja – Islamskie Państwo w Iraku, zwanej też Al-Kaidą w Iraku, na Ad-Dawla al-Islamijja fi al-Irak wa asz-Szam – Islamskie Państwo w Iraku i Lewancie. Osama bin Laden nie zginął w 2010 r., lecz w 2011 r. (2 maja), a po jego śmierci ISIL nie mogło zostać rozbite, ponieważ jeszcze nie istniało. Al-Kaida ani żadna z jej filii nie została rozbita po śmierci przywódcy. Organizacja Al-Shabab (Harakat asz-Szabab al-Mudżahidin – Ruch Młodych Mudżahedinów) nie przyłączyła się do Państwa Islamskiego, ponieważ jako jedna z niewielu dochowała wierności Al-Kaidzie. Nieprawdziwe są również informacje dotyczące magazynu „Inspire" o rozpoczęciu działalności publicystycznej w 2003 r. oraz opisaniu w tym internetowym periodyku w 2005 r. taktyki „tysiąca ciosów", ponieważ pierwszy jego numer ukazał się dopiero w lipcu 2010 r. Mało logiczna jest treść następujących zdań na s. 201: *W 2012 r. odnotowano najwyższą liczbę śmiertelnych ofiar konfliktów zbrojnych w Afryce od 1997 r., przede wszystkim ze względu na intensyfikację przemocy w Somalii i Nigerii*, a także: *W 2012 r. najwięcej zdarzeń o charakterze zbrojnym zarejestrowano w Mali i Kenii*.

Autorka mija się z prawdą, pisząc na s. 217: *Dzisiejszy cool jihad ma niewiele wspólnego z jego odpowiednikami europejskimi z lat 70. Małe grupy ekstremistyczne, takie jak włoskie Czerwone Brygady czy niemieckie Baader-Meinhof Group, były stanowczo zupełnie inną formą „mody" na działania partyzanckie. Składały się z kilku lub*

[11] W tym schemacie działania autorka wymienia:
- „atak na często przypadkowy cel,
- ujawnienie się za pomocą mediów (przyznanie się do czynu, wymienianie nazwy organizacji, która przeprowadziła atak, przedstawianie motywów i celów działania),
- sformułowanie ponownej groźby ataku,
- postawienie żądań i warunków, których spełnienie nie spowoduje dalszych ataków,
- informacja, że niedopełnienie żądań pociągnie za sobą dalsze ataki".

kilkunastu osób i nie miały tak wielkiego wpływu na innych. Przede wszystkim Czerwone Brygady (Rote Armee Fraktion – RAF, Frakcja Czerwonej Armii) i Grupa Baader-Meinhof nie były żadnymi odpowiednikami grup prowadzących dżihad i nie miały nic wspólnego z islamem. Były lewackimi organizacjami terrorystycznymi. O ile RAF można uznać za małe ugrupowanie, o tyle Czerwone Brygady – wprost przeciwnie. Ponadto obie organizacje miały wielki wpływ na włoską i niemiecką młodzież (dwie generacje Czerwonych Brygad, trzy generacje RAF) oraz stanowiły poważne zagrożenie bezpieczeństwa w obu krajach.

I jeszcze jedno pozbawione sensu zdanie na s. 227: *Tak samo jak naziści, fanatycy z IS są antysemitami, przekonanymi o własnej wyższości rasowej*. Członkowie Państwa Islamskiego nie mogą być przekonani o swojej wyższości rasowej, ponieważ jego bojownikami są przedstawiciele wszystkich ras. Uważają natomiast, że jedynie ich interpretacja islamu jest słuszna, dokonali podziału społeczności muzułmańskiej na „ludzi raju" i „ludzi piekła", czyli wszystkich pozostałych, którzy nie zgadzają się z ich ideologią. Niedorzeczne są zdania na s. 234: *Z drugiej strony RFN, za sprawą IUD, jest wymieniane, jako najbardziej prawdopodobny atak islamskich ekstremistów. Choć w rzeczywistości nie wydaje się, aby Niemcy były atrakcyjnym celem dla Al-Kaidy* oraz *Z perspektywy działania Al-Kaidy w Europie, Polska jest ciągle atrakcyjnym obiektem ataku*. Po porównaniu tych zdań można wywnioskować, że Polska jest bardziej atrakcyjnym celem dla terrorystów niż Niemcy. I podobnie: *Zaś porwanie i uśmiercenie polskiego inżyniera w Pakistanie było pierwszym poważnym sygnałem, że Polska coraz bardziej znajduje się w zainteresowaniu Al-Kaidy*. Przede wszystkim inż. Piotra Stańczaka nie porwała (28 września 2008 r.) Al-Kaida i nie ona dokonała jego mordu 7 lutego 2009 r. Zagrożenie atakiem terrorystycznym w Polsce ze strony islamskich ekstremistów i sympatyków Al-Kaidy pojawiło się już w 2003 r. Zostało ono zlikwidowane dzięki operacji Agencji Bezpieczeństwa Wewnętrznego pod kryptonimem „Miecz". W lipcu 2004 r. w internecie zostało zamieszczone ostrzeżenie skierowane do władz Polski i Bułgarii z żądaniem wycofania kontyngentów wojskowych z Iraku pod groźbą przeprowadzenia zamachu terrorystycznego, jak ten, do którego doszło 11 marca 2004 r. w Madrycie. Do 2008 r. terroryści jeszcze kilkakrotnie wysuwali groźby pod adresem Polski.

Kończąc, muszę stwierdzić, że Magdalena El Ghamari nie dołożyła należytej staranności podczas pisania *Cool jihad*. Błędy ortograficzne, stylistyczne, duża liczba literówek, niektóre mylące – w rodzaju „Iran" zamiast „Irak", różna pisownia tych samych wyrazów, często powtarzające się informacje, nawet na tej samej stronie, przerywane wątki dotyczące jednego tematu i kontynuowane w różnych miejscach książki, to tylko niektóre krytyczne uwagi dotyczące recenzowanej publikacji. Ze względu na mało komunikatywny język i niski poziom toku narracji, jej przeczytanie wymaga dużego wysiłku umysłowego. Jednak najbardziej istotna według mnie jest jej dezaktualizacja już w roku wydania – 2018, ponieważ najnowsze wydarzenia w niej opisane dotyczą lat 2014–2015. Nie przypuszczam, aby wydawnictwo trzy lata zwlekało z publikacją. Należy raczej sądzić, że autorka nie podjęła wysiłku uzupełnienia informacji

i przeprowadzenia analizy wydarzeń dotyczących Państwa Islamskiego i dżihadu po 2015 r. Dlatego też stanowczo nie zgadzam się z krótką recenzją książki napisaną przez Tomasza R. Aleksandrowicza, prof. nadzw. Wyższej Szkoły Policji w Szczytnie, zamieszczoną na czwartej stronie okładki: *Czytelnik otrzymuje solidną dawkę wiedzy na temat kalifatu i pojęcia jihadu, co jest niezbędne do zrozumienia dzisiejszej sytuacji i fenomenu Państwa Islamskiego (Daesh, ISIS/ISIL). Autorka nie ogranicza się przy tym do samego opisu, lecz analizuje ten fenomen w szerokim kontekście politycznym i kulturowym, rozprawiając się – niejako mimochodem – z szeregiem pokutujących w społeczeństwach Zachodu nieporozumień i wręcz mitów*. Jest wprost przeciwnie. Autorka poruszyła w książce w sposób chaotyczny tyle różnych wątków niezwiązanych ze sobą, że trudno mówić o solidnej dawce wiedzy. Poza tym popełniła wiele błędów faktograficznych i podała nieprawdziwe informacje. Moim zdaniem zupełnie nie wywiązała się z postawionego sobie celu, którym miał być opis genezy i analiza dżihadu oraz najnowszej formy kalifatu. Nie potrzeba mieć wiedzy badacza i eksperta, by podczas lektury dostrzec liczne rażące błędy i twórcze „niedoróbki". Wiele do życzenia pozostawia także korekta. Odniosłem wrażenie, że publikacja była jej zupełnie pozbawiona. Muszę przyznać, że nie pamiętam, aby w moich rękach znalazła się gorzej napisana i wydana książka na temat terroryzmu czy islamskiego ekstremizmu. Z żalem stwierdzam, że po raz pierwszy jestem zmuszony do wystawienia tak negatywnej recenzji. Po prostu szkoda czasu na lekturę tej pozycji.

Robert Borkowski

Dwugłos o przesłuchaniach. John R. Schafer, Joe Navarro, *Zaawansowane techniki przesłuchań. Sprawdzone strategie dla organów ścigania, wojska i personelu bezpieczeństwa*[1]. Rafał Kwasiński, *Przesłuchanie podejrzanego w sprawach przestępstw o charakterze terrorystycznym. Pozytywny wymiar kooperacji negatywnej*[2]

Problematyka związana z przesłuchaniem, zwłaszcza zagadnienia dotyczące skutecznych metod i taktyk jego prowadzenia, jest przedmiotem dociekań zarówno kryminalistyki[3], jak i psychologii oraz psychiatrii sądowej[4]. Truizmem jest stwierdzenie, że wartość dowodów zebranych w toku przesłuchania zależy w dużej mierze od poziomu profesjonalizmu, rzetelności (w tym odporności na naciski przełożonych czy polityków) oraz zdolności intelektualnych osoby, która je prowadzi. Jednym z czynników warunkujących profesjonalizm przesłuchującego jest jego wiedza psychologiczna, zwłaszcza gdy jest poparta wieloletnim doświadczeniem i praktyką[5].

W ostatnim czasie na polskim rynku wydawniczym pojawia się coraz więcej książek z zakresu psychologii kryminalnej, śledczej i sądowej, w tym dość dużo tłumaczeń literatury obcojęzycznej[6]. W odstępie kilkunastu miesięcy ukazały się dwie pozycje

---

1 J.R. Schafer, J. Navarro, *Zaawansowane techniki przesłuchań. Sprawdzone strategie dla organów ścigania, wojska i personelu bezpieczeństwa*, Toruń 2017, Wydawnictwo Naukowe Uniwersytetu Mikołaja Kopernika, s. 196.

2 R. Kwasiński, *Przesłuchanie podejrzanego w sprawach przestępstw o charakterze terrorystycznym. Pozytywny wymiar kooperacji negatywnej*, Warszawa 2019, Difin, s. 324.

3 Zob. D. Jagiełło, *Przesłuchanie jako czynność dowodowa*, Warszawa 2017.

4 Zob. np. B. Hołyst, *Psychologia kryminalistyczna – diagnoza i praktyka*, Warszawa 2018. Autor książki szeroko omawia aspekty psychologiczne oraz taktyki przesłuchania. Por. także: M. Cieślak, K. Spett, A. Szymusik, W. Wolter, *Psychiatria w procesie karnym*, Warszawa 1991.

5 Por. B.W. Wojciechowski, *Psychologiczne uwarunkowania i ocena wartości dowodowej zeznań świadków*, Warszawa 2015 lub M. Kuźmiński, *Taktyka i metody przesłuchania świadka w postępowaniu przygotowawczym*, „Resocjalizacja Polska (Polish Journal of Social Rehabilitation)" 2014, nr 8, s. 119–130.

6 Zob. np. K. Daynes, *Oko w oko ze złem. Prawdziwe historie z akt psycholożki sądowej*, Kraków 2019.

dotyczące psychologicznych aspektów przesłuchań. Należy to przyjąć z zadowoleniem, gdyż stan rodzimej literatury poświęconej tej problematyce nie jest imponujący[7].

Pierwszą z nich, wydaną przez oficynę wydawniczą toruńskiego uniwersytetu, jest przekład amerykańskiego poradnika[8] na temat technik i metod prowadzenia przesłuchań autorstwa Johna R. Schafera i Joego Navarro, emerytowanych pracowników Federalnego Biura Śledczego. Ten drugi autor jest znany polskiemu czytelnikowi z książek na temat tzw. *body language*, wydanych przez popularne wydawnictwo Burda[9]. Z kolei wydawnictwo Difin, które wyraźnie aspiruje do pozycji lidera na rynku publikacji z dziedziny szeroko rozumianego bezpieczeństwa, udostępniło drukiem monografię Rafała Kwasińskiego, stanowiącą kompendium wiedzy o przesłuchiwaniu terrorystów.

Toruńska edycja *Zaawansowanych technik przesłuchań* ukazała się w Polsce 14 lat po pierwszym wydaniu amerykańskim. Niezrozumiałe jest, dlaczego polski wydawca przy tłumaczeniu korzystał z pierwszego wydania tej książki pochodzącego z 2003 r. (notabene na stronie redakcyjnej znajduje się nieprawdziwa informacja – jako datę pierwszej edycji, sygnowanej przez Charles C. Thomas Publisher, Ltd., podano 2004 r.), a nie z późniejszych. Na rynku amerykańskim już od 2016 r. jest dostępne wydanie trzecie, zaktualizowane i rozszerzone, które liczy 174 strony (pierwotna wersja ma 143 strony). Nie jest to jednak najpoważniejszy zarzut, a upływ czasu nie jest na tyle duży, by tłumaczył negatywną ocenę tej książki.

Lektura już kilkunastu początkowych stron wystarczy, by uświadomić sobie, że ma się do czynienia z pozycją nie najlepszej jakości. Układ treści poradnika oraz kolejność zaprezentowanych wątków tematycznych nie budzą zastrzeżeń. Problemem jest niski poziom merytoryczny publikacji i niezdefiniowanie kręgu jej odbiorców.

Pierwsze trzy rozdziały książki zostały poświęcone przygotowaniom do przeprowadzenia przesłuchania, a więc jego planowaniu, aranżowaniu miejsca oraz organizowaniu potrzebnych rekwizytów. Warto dodać, że pod pojęciem p r z e s ł u c h a n i e autorzy (a za nimi tłumacze) rozumieją także działalność operacyjną w terenie, a więc prowadzenie wywiadu i wszelkie rozmowy z oskarżonymi, podejrzanymi i świadkami (zatem policyjna czynność rozpytania byłaby zaliczana do działań nazywanych w języku angielskim *interview*, przesłuchanie podejrzanego określa się natomiast słowem *interrogation*, s. 17). Przemyślenia autorów, przybierające formalnie postać zwięzłych akapitów liczących najczęściej kilka zdań, często sprowadzają się do prostych,

---

[7] Zob. Z. Marten, *Psychologia zeznań*, Warszawa 2012; J.M. Stanik, A. Roszkowska, *Psychologia zeznań świadków (w ćwiczeniach)*, Katowice 2009; W. Pasko-Porys, *Przesłuchiwanie i wywiad. Psychologia kryminalistyczna*, Warszawa 2007; E. Gruza, *Ocena wiarygodności zeznań świadków w procesie karnym. Problematyka kryminalistyczna*, Kraków 2003. Zob. także: F. Arntzen, *Psychologia zeznań świadków*, Warszawa 1989.

[8] Tytuł oryginału: *Advanced Interviewing Techniques: Proven Strategies for Law Enforcement, Military, and Security Personnel* (przyp. red.).

[9] Zob. J. Navarro, *Mowa ciała*, Warszawa 2011; tenże, *Mowa ciała w pracy*, Warszawa 2015; J. Navarro, P.T. Sciarra, *Niebezpieczne osobowości*, Warszawa 2015.

banalnych, a czasami nawet wątpliwych stwierdzeń. Z książki można się na przykład dowiedzieć, że rano ludzie są czujni, a po południu zmęczeni (s. 27). Nie jest to do końca prawda, jeśli weźmie się pod uwagę różnice międzyosobnicze w rytmach czuwania i snu oraz ich wpływ na sprawność psychofizyczną człowieka i co za tym idzie – istnienie odmiennych typów aktywności dobowej[10]. Wiele porad dotyczących przygotowania przestrzeni, w której odbędzie się przesłuchanie, ma charakter praktycznych zaleceń. Bazują one na wiedzy psychologicznej, ale są podane w sposób nacechowany naiwnością. Przykładowo, autorzy radzą, żeby podczas ustawiania krzeseł zadbać o to, by nie siedzieć twarzą w twarz z przesłuchiwanym mężczyzną (czy to oznacza, że policjant spisujący zeznania ma siedzieć bokiem do rozmówcy?), gdyż mogłoby to wzbudzać jego agresję wobec przesłuchującego. Nie ma natomiast takich wskazań w przypadku przesłuchiwania kobiet. Z kolei doradzając, jak utrudnić działanie adwokatowi przesłuchiwanego, autorzy sugerują, by krzesło przeznaczone dla mecenasa postawić nieco z boku i z tyłu krzesła przesłuchiwanego (s. 37). Zapominają przy tym, że obrońca ma prawo zmienić ustawienie krzesła zarówno swojego, jak i mandanta[11].

W kolejnych trzech rozdziałach książki autorzy prezentują przemyślenia dotyczące oceny przesłuchiwanego, sposobów uzyskania dominacji nad nim, a także przebiegu interakcji podczas przesłuchania. Według Schafera i Navarro przesłuchujący mogą zyskać przewagę przez naruszenie anglosaskich dobrych obyczajów, brak punktualności i skłonienie przesłuchiwanego i jego adwokata do oczekiwania przez 10 minut na rozpoczęcie przesłuchania. Podwojenie tego czasu do 20 minut jest – według autorów – sposobem na silne zdominowanie przesłuchiwanego (s. 59).

Najkrótszy, czterostronicowy rozdział siódmy jest w istocie lapidarnym zreferowaniem tzw. praw Mirandy, czyli praw przysługujących osobom zatrzymanym w USA przez policję. Pierwsze z nich to prawo do milczenia, drugie wskazuje na obowiązek funkcjonariusza polegający na przekazaniu zatrzymanemu ostrzeżenia, że wszystko, co powie, może być użyte przeciwko niemu podczas procesu, trzecie – to prawo do obecności adwokata przy przesłuchaniach i czwarte – prawo do adwokata z urzędu, jeśli oskarżony nie ma wystarczających środków finansowych (s. 97–98).

Tematyka kolejnych trzech rozdziałów, stanowiących jedną trzecią (54 strony) objętości książki, dotyczy rozpoznawania werbalnych i niewerbalnych sygnałów kłamstwa. W rozdziale ósmym, poświęconym detekcji kłamstwa, autorzy podkreślają, że jest to proces złożony z dwóch etapów. W pierwszym śledczy powinien rozpoznać dziwne zachowania osoby przesłuchiwanej, a w drugim – poprawnie je zinterpretować. Zdarza się bowiem, że ktoś prawdomówny, kto czuje, że się mu nie wierzy, okazuje podobne emocje jak osoba kłamiąca (s. 102). Na dalszych stronach został przedstawiony

[10] Por. M. Saganowska, *Oddziaływanie rytmów biologicznych na sprawność psychofizyczną*, „Problemy Nauk Stosowanych" 2014, t. 2, s. 179–184.

[11] Mandant (łac. *mandans* – powierzający, zleceniodawca) – ktoś, kto powierza pełnomocnikowi mandat (czyli zlecenie) prowadzenia sprawy w sądzie (przyp. red.).

czteroobszarowy model wykrywania kłamstwa (s. 107–117), w którym prowadzący przesłuchanie ma na podstawie obserwacji gestów, mimiki i kontaktu wzrokowego ocenić komfort bądź dyskomfort odczuwany przez przesłuchiwanego. Zdaniem Schafera i Navarro bardzo przydatna jest przy tym ocena zachowań niewerbalnych związanych z podkreślaniem znaczenia wypowiadanych treści oraz umiejetność wychwytywania prób manipulacji ze strony przesłuchiwanego. Zachowaniom niewerbalnym szerzej został poświęcony rozdział dziewiąty. Jego treść to w większości cytaty z prac z zakresu psychologii społecznej. Ich autorzy reprezentują różne perspektywy badawcze i mają inne poglądy, a sposób, w jaki Schafer i Navarro je przedstawiają, powoduje, że czytelnik ich książki ma wrażenie niespójności. W dodatku niektóre tezy nakreślone w tym miejscu stoją w sprzeczności z treściami rozdziału poprzedniego. Omawiając zachowania niewerbalne, autorzy jedynie zdawkowo wspominają o obowiązującym w nauce podziale tych zachowań (proksemika[12]; mowa ciała – postawa, gesty, mimika; okulezja[13]; tło werbalne). Rozdział dziesiąty został poświęcony werbalnym oznakom kłamstwa. W tej części książki również są widoczne niekonsekwencje. Na przykład autorzy wskazują, że dłuższy namysł przed udzieleniem odpowiedzi oraz odpowiednia intonacja (nie podają jednak jej cech) to oznaki kłamstwa (s. 131), aby w kolejnych akapitach stwierdzić, że kłamca na ogół odpowiada szybko, aby nie stwarzać wrażenia opóźniania odpowiedzi (s. 133). Została opisana również strategia nazwana przez autorów „poligrafem biedaka", która polega na szybkim zadawaniu serii pytań. Jej celem jest wytrącenie przesłuchiwanego z równowagi przez zmuszenie go do intensywnego myślenia nad utrzymaniem spójności prezentowanej wersji. Metoda opiera się na założeniu, że zwiększony wysiłek umysłowy przeciąża mózg, co może skutkować popełnieniem błędu (s. 145–147). Na koniec autorzy zalecają stosowanie podczas przesłuchań tzw. drugiego pożegnania, czyli zadanie dodatkowego, a w istocie najważniejszego, pytania już po zakończeniu przesłuchania i pożegnaniu się z przesłuchiwanym. Podczas lektury tego rozdziału czytelnik po raz kolejny może odnieść wrażenie, że jest to niedopracowana kompilacja cytatów z uznanych prac o tematyce psychologicznej.

Cztery krótkie rozdziały zamykające książkę, liczące w sumie 40 stron, zawierają lapidarne porady dotyczące taktyki przesłuchań i rozmów. Całość została wzbogacona materiałem ilustracyjnym w postaci 18 fragmentów stenogramów z przykładowych przesłuchań.

W podsumownaiu należy podkreślić, że ze względu zarówno na odmienności kulturowe i mentalne między społeczeństwem amerykańskim a społeczeństwami krajów europejskich, jak i fundamentalne różnice między anglosaską a łacińską kulturą

[12] Proksemika – nauka zajmująca się badaniem wpływu relacji przestrzennych między osobami lub między osobami a materialnym otoczeniem. Głównym założeniem proksemiki jest postrzeganie dystansu interpersonalnego jako wskaźnika relacji społecznych. Tym terminem określa się także „przestrzenne" zachowania ludzkie, takie jak np. utrzymywanie czy skracanie dystansu fizycznego, reakcje na zajmowaną przez kogoś przestrzeń (przyp. red.).

[13] Okulezja – wykorzystywanie kontaktu wzrokowego w procesie komunikacji interpersonalnej (przyp. red.).

prawną, przydatność tego rodzaju poradników na gruncie europejskim nie jest duża. Tłumacze, którzy dokonali bardzo dobrego przekładu pod względem językowym, podkreślają wprawdzie odmienność amerykańskiego systemu prawnego, który narodził się i ewoluował w innym środowisku kulturowym, społecznym i przestępczym, lecz czynią to wyłącznie we wstępie. W całej pracy nie ma komentarzy ani odnośników sygnalizujących konkretne rozbieżności w procedurach oraz w prawach zatrzymanego czy świadka w krajach europejskich i w USA. Polskiego odbiorcę książka może więc jedynie utwierdzić w przekonaniu o odmienności kulturowej Nowego Świata i Starego Kontynentu (przeczyta on m.in. o szczególnej, bliskiej ideałom współczesnej ekologii, duchowości Indian północnoamerykańskich, typowym dla Afroamerykanów unikaniu kontaktu wzrokowego czy o preferencji Arabów do poruszania tematów dotyczących zdrowia na początku rozmowy, a nie pod jej koniec).

Najpoważniejszym mankamentem polskiej edycji tej książki jest brak bibliografii. Publikacja zawiera 289 odnośników, w tym do prac znanych autorów, jak Elliot Aronson, Allan Pease, Edward Hall, Robert Cialdini, Gavin de Becker czy Daniel Goleman. Zastosowanie w tekście przypisów harwardzkich[14] powoduje jednak, że polski czytelnik nie ma możliwości sprawdzania źródeł, z których korzystali autorzy.

Po lekturze tej publikacji rodzi się pytanie, do kogo jest ona skierowana. Książka nie jest bowiem pracą naukową, nie można jej również uznać za fachowy poradnik na temat realizacji procedur przesłuchania. Podczas jej czytania profesjonalista będzie się zżymać, a laik może wyrobić sobie fałszywy obraz warsztatu śledczego. Z pewnością nie należy jej zalecać studentom prawa czy policyjnym adeptom, gdyż jej wartość poznawczą można porównać do przydatności pod tym względem seriali typu „CSI: Kryminalne zagadki Las Vegas" itp. Szkoda więc, że przed rozpoczęciem prac zespół redakcyjny nie podjął trudu oceny poziomu merytorycznego tego poradnika. Widać, że koncepcja wydania książki nie została gruntownie przemyślana, a jej opracowanie edytorskie jest niestaranne (np. błędy w nazwiskach przywoływanych autorów), co czyni tę pozycję jeszcze mniej wartościową. Trudno zatem zrozumieć, dlaczego zdecydowano o przyznaniu grantu na tak słabą publikację.

W przeciwieństwie do amerykańskiego poradnika praca Rafała Kwasińskiego to monografia, która łączy w sobie walor zarówno rozprawy naukowej, jak i pomocnego kompendium wiedzy na temat problematyki przesłuchiwania terrorystów oraz członków zorganizowanych grup przestępczych. To sytuuje ją w obszarze stosowanych nauk społecznych. Lekturę tego poradnika można polecić w ramach doskonalenia warsztatu zawodowego zarówno funkcjonariuszom specjalizującym się w prowadzeniu przesłuchań, jak i prokuratorom. Książka liczy 324 strony i w sposób logiczny została podzielona na wprowadzenie, cztery rozdziały tematyczne oraz zakończenie.

[14] System harwardzki – system podawania źródeł bezpośrednio w tekście. W nawiasie wskazuje się jedynie nazwisko autora, rok wydania i ew. stronę cytowanej publikacji, a pełny opis bibliograficzny zamieszcza się w bibliografii na końcu pracy (przyp. red.).

Całości dopełnia dziesięciostronicowa bibliografia (złożona głównie z pozycji książkowych) oraz wykaz rysunków zamieszczonych w pracy.

We wprowadzeniu autor wyjaśnia cel pracy i jej główne założenia. Wyolbrzymia przy tym skalę zagrożenia terroryzmem, prognozując jego rozwój w następstwie kryzysu migracyjnego w Unii Europejskiej (s. 7). Tego rodzaju przewidywania okazały się mylne, a podsycanie nastrojów antyimigranckich oraz strachu przed terroryzmem było w rzeczywistości motywowanym politycznie wzniecaniem paniki moralnej w polskim społeczeństwie[15]. Autor podkreśla również groźbę wzrostu nastrojów ksenofobicznych na naszym kontynencie, co faktycznie się dzieje i jest wywołane nie tylko katastrofą humanitarną spowodowaną wojnami na Bliskim Wschodzie. Po krótkiej serii zamachów terrorystycznych związanych z falą dżihadyzmu ISIS sytuacja w Europie jest jednak – w świetle statystyk (np. Global Terrorism Database) – stabilna i nic nie zapowiada wzrostu poziomu zagrożenia. Podobnie nieaktualne wydaje się odniesienie do sprawy Agrobombera (s. 8), gdyż autor podaje tylko informację o jego zatrzymaniu pochodzącą z 2012 r. i nie wzmiankuje o finale tej sprawy. Te oraz inne partie tekstu sprawiają wrażenie, że książka powstawała przez dłuższy okres i nie wszystkie fragmenty zostały zaktualizowane przed złożeniem jej do druku.

Rozdział pierwszy (obejmujący 53 strony) jest poświęcony metodyce przesłuchania podejrzanego, w tym zarysowaniu celu przesłuchania, jego planowaniu, przygotowaniu i etapom, a także czynnikom decydującym o wyborze metody jego przeprowadzenia. Autor daje klarowny i spójny wywód, podczas którego prezentuje poglądy najwybitniejszych kryminologów i wyjaśnia istotę procedury przesłuchania. Na gruncie prakseologii definiuje istotę kooperacji negatywnej (s. 18). Wyróżnia cztery etapy przesłuchania: wstępno-obserwacyjny, spontanicznych wyjaśnień, indagacyjny oraz dokumentowania przesłuchania. W opisie przygotowania i planowania przesłuchania są zawarte konkretne wskazówki praktyczne. Dotyczą one między innymi konieczności napisania precyzyjnego planu przesłuchania (s. 44–48), gdyż śledczy nie może improwizować i opierać się wyłącznie na swojej pamięci. Kwasiński podkreśla znaczenie materiału dowodowego oraz materiału osobopoznawczego (s. 50). Autor w sposób interesujący i przystępny omawia metody prowadzenia przesłuchań. Dzieli je na: racjonalne (metoda dawkowania dowodów, metoda kumulatywnego ujawniania dowodów, metoda argumentacji, metoda wyczekującej postawy prowadzącego przesłuchanie, metoda odwracania uwagi podejrzanego, metoda wykrywania logicznych sprzeczności, metoda obojętności), emocjonalne (metoda ujawniania motywu przestępstwa, metoda rozbicia solidarności przestępczej) oraz kontrowersyjne (metoda krzyżowych pytań, metody oddziaływania na stany emocjonalne i uczucia podejrzanego, metoda wszechwiedzy). Wydaje się, że w naszym kraju przesłuchujący najczęściej wykorzystują podatność emocjonalną osoby tymczasowo aresztowanej, nadużywając przy tym

[15] Por. R. Borkowski, *Performans zbrodni strachu (współczesny terroryzm jako fenomen paniki moralnej)*, w: *Bezpieczeństwo Polski w XX i XXI wieku*, H. Ćwięk, M. Siewier (red.), Częstochowa 2018, s. 211–228; S.P. Hier, *Moral Panic and the Politics of Anxiety*, London–New York 2011.

tzw. aresztu wydobywczego (co jest przedmiotem licznych skarg polskich obywateli składanych do Europejskiego Trybunału Praw Człowieka), celowo posługują się również wiedzą o prywatnym życiu podejrzanego zgromadzoną przez śledczych. Rozdział pierwszy kończy krótka refleksja na temat czynników determinujących wybór metody i taktyki przesłuchania.

Rozdział drugi, liczący aż 133 strony i dotyczący psychologicznych aspektów prowadzenia przesłuchań, jest najobszerniejszy i składa się z dwóch części. W pierwszej z nich autor omawia uwarunkowania psychologiczno-taktyczne przesłuchania podejrzanego w sprawach przestępstw o charakterze terrorystycznym. Duża część rozważań została poświęcona problematyce psychospołecznych aspektów terroryzmu, w tym koncepcji tzw. osobowości terrorystycznej. Wyniki licznych badań dowodzą jednak, że ta koncepcja jest błędna i nie znajduje potwierdzenia w nauce[16]. Zarówno o s o b o w o ś ć t e r r o r y s t y, jak i r a d y k a l i z a c j a (która ma status kategorii analitycznej) to nie są pojęcia syndromatyczne[17], a co najwyżej konceptualizacje.

Autor książki podbudowuje swoje rozważania częstymi odwołaniami do prac Johna Horgana, jednego z najwybitniejszych znawców problematyki psychologii terroryzmu i klasyków amerykańskiej literatury przedmiotu[18]. Ma do tego prawo i robi to w sposób konsekwentny, ale momentami bezkrytyczny. Dobrze byłoby, gdyby wspomniał, że istnieją różne poglądy, niejednokrotnie odmienne od teorii Horgana (s. 73–84), dotyczące psychologicznych uwarunkowań podejmowania działalności terrorystycznej oraz prewencji i zwalczania terroryzmu, a w nauce (zarówno w psychologii, jak i kryminologii) nie ma zgodności co do koncepcji amerykańskiego naukowca.

W drugiej części tego rozdziału Kwasiński przedstawia taktyczne uwarunkowania przesłuchania podejrzanego. Pisze m.in. o kontekście kulturowym, który może mieć duże znaczenie na przykład podczas przesłuchiwania obcokrajowca z odmiennego kręgu kulturowego. Wspomina przy tej okazji o ważnej roli tłumacza w przesłuchaniu (s. 117–120). Prezentuje również praktyczne wskazówki dotyczące opracowania precyzyjnego planu przesłuchania, wyboru miejsca i doboru osoby przesłuchującej. W interesujący i zrozumiały sposób omawia znaczenie umiejętności komunikacyjnych przesłuchującego oraz przeprowadzania analizy zachowań behawioralnych i werbalnych przesłuchiwanego. Wielu cennych informacji dostarcza lektura podrozdziału poświęconego analizie behawioralnej zachowań przesłuchiwanego (s. 167–192). Autor, opisując schematy zachowań osób przesłuchiwanych, które próbują oszukać przesłuchującego,

---

[16] Por. R. Borkowski, *Teoremat radykalizacji w prewencji antyterrorystycznej*, w: *Perspektywy bezpieczeństwa narodowego w XXI wieku*, M. Kubiak, A. Smarzewska (red.), Biała Podlaska 2014, s. 59–67.

[17] Obejmujące pełną treść pojęcia, tj. zespół symptomów występujących razem i współzależności między nimi (przyp. red.).

[18] Por. J. Horgan, *Psychologia terroryzmu*, Warszawa 2008, s. 73–83. Zob. też: B. Bolechów, *Terroryzm – aktorzy, statyści, widzowie*, Warszawa 2010; I.R. Borum, *Psychology of Terrorism*, Tampa 2004; *The Psychology of Terrorism. Coping with the Continuing Threat*, t. 1–3, C.E. Stout (red.), Westport, London 2002.

opiera się na pracach znakomitych badaczy, takich jak Paul Ekman czy Aldert Vrij. Jest to bez wątpienia jedna z najlepszych partii książki Kwasińskiego, będąca w istocie krótkim wykładem na temat psychologii kłamstwa. Końcowa część rozdziału jest poświęcona zwięzłemu przedstawieniu metod wykrywania kłamstw.

Rozdział trzeci (63 strony) zawiera opisy różnych metod przesłuchiwania podejrzanego w sprawach dotyczących przestępczości terrorystycznej, które są stosowane w Stanach Zjednoczonych oraz w Wielkiej Brytanii. Są to państwa, które z zagrożeniem terrorystycznym borykają się od dziesięcioleci, więc ich aparat śledczy ma bogate doświadczenie w tej materii. Autor omawia kontrowersje związane ze sposobem prowadzenia globalnej wojny z terroryzmem i stosowaniem przez CIA tortur podczas przesłuchań. Wspomina, że wiele działań USA ocenionych negatywnie było skutkiem posunięć sekretarza obrony Donalda Rumsfelda, który głosił konieczność narzucenia światu nowej amerykańskiej polityki, wykorzystującej nowe metody i nową narrację polityczną (ang. *to fashion a new vocabulary*). Autor podkreśla też znaczenie polityki prezydenta Baracka Obamy i utworzenia w FBI zespołu ekspertów, których zadaniem było wypracowanie efektywnych technik prowadzenia śledztw, ale bez łamania praw człowieka (s. 200–201). Spośród amerykańskich sposobów przesłuchań stosowanych obecnie autor omawia trzy metody: Reida, Wicklandera-Zulawskiego oraz *Kinesic Interview and Interrogation*. Charakteryzuje również brytyjską strukturalną metodę przesłuchania (s. 202–243). Ta część książki jest niezwykle interesująca i znacznie wzbogaca oraz porządkuje wiedzę o taktyce przesłuchań.

W rozdziale czwartym zostaje omówiona autorska metoda przesłuchań „PRO-A®T", określona przez Kwasińskiego jako metoda strukturalnego proaktywnego przesłuchania podejrzanego. Przesłankami do jej opracowania były pogłębione studia nad literaturą przedmiotu oraz wykorzystanie dorobku ekspertów FBI, portugalskiej jednostki zajmującej się zwalczaniem terroryzmu, a także polskich służb. Omawiana metoda składa się z trzech etapów – przygotowania i planowania, rozmowy zasadniczej oraz ewaluacji przesłuchania. Autor kładzie szczególny nacisk na błędy, jakie mogą popełnić śledczy, niejednokrotnie już we wczesnej fazie przesłuchania. Zalicza do nich: przedwczesne zamknięcie, defensywne unikanie czy też potwierdzone uprzedzenie. Podkreśla tym samym, że niepanowanie nad emocjami czy też uleganie streotypom może negatywnie wpłynąć na wynik przesłuchania (s. 264–265). Za bardzo ważny element tworzenia charakterystyki podejrzanego autor uznaje profilowanie, rozumiane jako opisanie go pod względem ideowym, religijnym czy kulturowym (np. zaklasyfikowanie jako nacjonalistę, fundamentalistę). Wydaje się, że termin p r o f i l o w a n i e jest tu zastosowany w sposób nieadekwatny i niepotrzebnie nadużywany (s. 271–275). W kryminalistyce „profilowanie" odnosi się na ogół do tworzenia – na podstawie dostępnych danych – indywidualnej charakterystyki anonimowego sprawcy. Nie jest to zatem ocena i klasyfikacja cech osobniczych podejrzanego, którego tożsamość jest znana. Na zakończenie autor podsumowuje najistotniejsze cechy metody PRO-A®T. Stwierdza przy tym, że w publikacji przedstawia jedynie zarys jej podstawowych założeń psychologicznych i taktycznych oraz zaznacza, że metoda

wymaga dalszych pogłębionych badań w celu zoptymalizowania poszczególnych jej komponentów (s. 312). Rafał Kwasiński słusznie podkreśla, że terroryzm jest zjawiskiem skomplikowanym i złożonym, a więc do jego rozpoznawania i zwalczania są potrzebne zróżnicowane, wysoce specjalistyczne metody (s. 310). Po lekturze książki trudno jednak jednoznacznie odpowiedzieć na pytanie, czy metoda autora spełnia wszystkie kryteria nowatorstwa w porównaniu z innymi metodami prowadzenia przesłuchań, czy też jest to kompilacja znanych taktyk i technik, które już wcześniej stosowano w śledztwach. Ta wątpliwość oraz drobne niedociągnięcia edytorskie nie umniejszają jednak wartości merytorycznej omawianej pozycji.

III

WYBRANE ARTYKUŁY W JĘZYKU ANGIELSKIM

SELECTED ARTICLES IN ENGLISH

Dariusz Gradzi

Fintech/Regtech. The risk of money laundering and terrorist financing resulting from new technologies in the area of electronic payments

In the first quarter of 2019, over 1.2 billion debit card transactions and over 100 million credit card transactions were recorded[1]. In the second quarter of 2019, the total number of non-cash transactions amounted to 1.43 billion, and their value nearly PLN 93 billion[2]. Research shows that the most popular payment instruments are payment card, bank account with online account access and PayPal account[3]. In the era of continuous and irreversible digitization of the financial sector, it is particularly vulnerable to the risks associated with criminal activities, including terrorist activities. For this reason, legislative work has been carried out for many years, resulting in new regulations in this area. They are intended to respond to identified threats. In practice, however, it is different, because the length of the legislative process means that as soon as the implemented legal acts are in force, they are not adapted to reality.

Anti-money laundering (AML) and terrorist financing (TF) in financial institutions are regulated by the Fourth Anti-Money Laundering Directive (AMLD4).[4] It integrates the AML/CTF (counter terrorist financing) system with the international money laundering (ML) and terrorist financing standards adopted by the Financial Action Task Force (FATF).[5] According to these standards, AMLD4 adopts as a rule

---

[1] *Information on payment cards. I quarter 2019*, https://www.nbp.pl/systemplatniczy/karty/q_01_2019.pdf, p. 6, 15 [access: 4 XII 2019].

[2] *Information on payment cards. II quarter 2019*, https://www.nbp.pl/systemplatniczy/karty/q_02_2019.pdf p. 16, 17 [access: 4 XII 2019].

[3] See *Report. 'Płatności cyfrowe' 2019*, https://eizba.pl/wp-content/uploads/2019/11/PLATNOSCI_CYFROWE_2019.pdf?fbclid=IwAR1ol9GL6K85vybNy5iwjoctd4k7YPFuT1rki_OpLjTwSqw1DFpGNkBoXBk [access: 2 XII 2019].

[4] *Directive (EU) 2015/849 of the European Parliament and of the Council of 25 May 2015 on the prevention of the use of the financial system for money laundering or terrorist financing, amending Regulation (EU) No 648/2012 of the European Parliament and of the Council and repealing Directive of the European Parliament and of the Council 2005/60/EC and Commission Directive 2006/70/EC* (Official Journal, EU L 141 of 5 June 2015, p. 73).

[5] Also known as Groupe d'action financiere (GAFI) – International Special Group on the Prevention of Money Laundering founded in 1989. The purpose of its activity is to develop practices

a risk-based approach. It assumes that ML/TF risk varies from country to country. Therefore, countries and their competent authorities (CA) and participants in legal transactions must identify risk and manage it on the basis of AMLD4 standards, i.e. take appropriate and adequate legal measures. On May 30, 2018, the Fifth AML Directive (AMLD5) was adopted, with the date of implementation by the Member States of the EU until January 10, 2020.[6] The European Money Laundering and Terrorist Financing Risk Assessment[7] identifies several dozen products and services potentially exposed to ML/TF risk, including: private banking, crowdfunding[8] platforms, virtual currencies, property values with cash-like properties: gold, diamonds.

Pursuant to ML/TF regulations, specific legal obligations have not been imposed on every entity. AML/CTF legislation only applies to obligated institutions which, on the basis of the Polish Anti-Money Laundering Act,[9] include among others (relevant to the subject matter of this study):

- domestic banks, branches of foreign banks, branches of credit institutions, financial institutions based in the territory of the Republic of Poland;
- cooperative savings and credit unions and the National Cooperative Savings and Credit Union;
- national payment institutions, national electronic money institutions, branches of the EU payment institutions, branches of the EU and foreign electronic money institutions, small payment institutions, payment service offices and billing agents;
- investment companies, custodian banks;
- foreign legal entities conducting brokerage activities on the territory of the Republic of Poland;
- companies operating a regulated market;
- investment funds, alternative investment companies, investment fund companies, managers of alternative investment companies;
- insurance companies;
- The National Depository for Securities;

to combat money laundering. The organization publishes recommendations on this topic, http://www.fatf-gafi.org/about/ [access: 2 XII 2019].

[6] *Directive (EU) 2018/843 of the EP and Council of 30 May 2018 amending Directive (EU) 2015/849 on preventing the use of the financial system for the washing or financing of terrorism and amending Directives 2009/138/EC and 2013/36/EU* (Official Journal of the EU L 156 of 19 June 2018, p. 43).

[7] *Report from the Commission to the European Parliament and the Council on the assessment of the risk of money laundering and terrorist financing affecting the internal market and relating to cross-border activities*, https://ec.europa.eu/info/sites/info/files/supranational_risk_assessment_of_the_money_laundering_and_terrorist_financing_risks_affecting_the_union.pdf [access: 4 XII 2019]

[8] The 'crowdfunding' mechanism assumes that the project promoter will pay people who contribute money to the project in a pre-determined form (editor's note).

[9] *Act of 1 March 2018 on Counteracting Money Laundering and the Financing of Terrorism* (Journal of Laws of 2019, item 1115, as amended).

- entrepreneurs engaged in currency exchange;
- entities conducting economic activity consisting in the provision of services in the field of:
  - exchange of virtual currencies for means of payment,
  - exchanges between virtual currencies,
  - brokering the exchange referred to above,
  - keeping accounts;
- entrepreneurs who are not other obligated institutions, providing services consisting in:
  - the creation of a legal person or organizational unit without legal personality,
  - performing the function of a member of the management board or enabling another person to perform this function, or a similar one, in a legal person or an organizational unit without legal personality,
  - providing a registered office, business address or correspondence address and other related services to a legal person or an organizational unit without legal personality,
  - acting or enabling another person to act as a trustee of a trust which was established by legal action,
  - acting or enabling another person to act as exercising rights from shares for the benefit of an entity other than a company listed on a regulated market that is subject to disclosure requirements in accordance with the EU law or equivalent international standards;
- foundations, to the extent that they accept or make payments in cash of a value equal to or exceeding the equivalent of EUR 10,000;
- associations with legal personality to the extent that they accept or make payments in cash with a value equal to or exceeding the equivalent of EUR 10,000;
- entrepreneurs to the extent that they accept or make payments for goods in cash with a value equal to or exceeding the equivalent of EUR 10,000;
- loan institutions.

General risks related to the financial services sector

The joint opinion of the European Supervisory Authorities[10] on the risk of money laundering and terrorist financing affecting the financial sector of the European Union divides the risk into: common for all sectors of financial services and relevant (specific)

[10] European Supervisory Authorities (ESA) consists of: European Securities & Markets Authority (ESMA) – European supervision of stock exchanges and securities, European Insurance & Pensions Authority (EIOPA) – European insurance and pension supervision and European Banking Authority (EBA) – European banking supervision.

only for specific sectors[11] Based on the above document, the following types of risk common to all financial sectors in the European Union can be distinguished:[12]

- risk arising from the UK's withdrawal from the EU (Brexit risk),
- risk related to the development of new technologies,
- risk related to virtual currencies,
- risk related to legislative divergence of EU countries and divergent supervisory practices,
- risk related to internal control weakness
- de-risking risk,[13]
- terrorist financing risk.

Risk arising from the UK's withdrawal from the EU[14]

Brexit carries the challenge of uncertainty as to whether the supervisory authorities of EU Member States will be able to cope with the proper and effective supervision of financial institutions after their relocation from Great Britain to the territories of EU Member States. In the absence of an international agreement, which will regulate, among others legal relations between the United Kingdom and the European Union, this country will no longer be, in legal terms, treated as an EU Member State.

This risk is particularly important because the United Kingdom has been a fintech company basin[15] for many years. The FinTech sector[16] in the UK generates over 6.6 billion pounds of profit. There are over 1.6 thousand such companies operating

[11] *Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector [access: 2 XII 2019].

[12] Ibidem, p. 1.

[13] 'De-risking' means a limitation or cessation by obligated institutions of conducting activities generating obligations under AMLD4, which in practice means a refusal to provide services to entities from areas of increased risk ML and TF.

[14] On 27 March 2017, the United Kingdom expressed its intention to withdraw from the EU. After that, the UK, in the absence of relevant agreements, will be treated as the so-called third country, which means that the EU legal regulations will not apply to it, which in turn will have a direct impact on the financial sector. This country will be treated in the same way as third country entities based in the United Kingdom. This practically means not applying the single passport principle, the single licence principle and the possibility of providing regulated services after obtaining authorization in one member state across the EU.

[15] https://biznes.wprost.pl/technologie/fintech/10013258/brexit-czy-wielka-brytania-straci-pozycje-lidera-fintech.html [access: 2 XII 2019]. 'Fintechs' – financial companies operating only in the network (editor's note).

[16] 'FinTech' is understood as the use of technological solutions in financial innovations, resulting in the creation of new business models. See the *Financial Stability Implications from FinTech. Supervisory and Regulatory Issues that Merit Authorities' Attention*, https://www.fsb.org/wp-content/uploads/R270617.pdf, p. 33 [access: 2 XII 2019].

there,[17] among others such technology companies as Revolut, TransferWise, Monzo, Starling Bank, Oak North and Funding Circle are present over there. In the so-called regulatory sandbox[18] itself there are about 300 fintechs.[19]

Until recently, the European Banking Authority (EBA)[20] had its headquarters in London, but due to the uncertain status of the United Kingdom as an EU member, the headquarters was moved to Paris (as a result of the initiation of the Brexit procedure).[21]

The UK's withdrawal from the EU creates many situations classified as ML/TF risk. These include the following:[22]

- relocation of entities from the UK to other Member States and the need for these entities to adapt to the new regulatory reality[23] and compliance[24] procedures (regulatory migration),
- the need to estimate many new entities, their business models, ownership structure, organization of internal control and their monitoring by new supervisory authorities,
- exercising effective supervision of new entities,
- continuing operations by relocated entities in the UK, which have only formal headquarters in the EU Member States without any structures (so-called shell companies),
- adjustment of financial institutions to the AML/CTF procedure, because after Brexit, the UK will become a third country within the meaning of AMLD4.

---

[17] https://www.money.pl/gospodarka/great-fintech-czyli-jak-to-sie-robi-w-wielkiej-brytanii-6440365075797633a.html [access: 2 XII 2019].

[18] It is a measure commonly used by supervisory authorities to enable technology companies to test new financial products and services without having to apply for and obtain complicated, time-consuming and cost-intensive licenses from these authorities, https://www.cashless.pl/cashlesspedia/piaskownica-regulacyjna [access: 2 XII 2019]; https://www.knf.gov.pl/en/MARKET/Fintech/Regulatory_Sandbox [access: 2 XII 2019].

[19] See report *UK FinTech. State of the Nation*, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/801277/UK-fintech-state-of-the-nation.pdf [access: 2 XII 2019].

[20] The EU agency regulating and supervising banking across all EU countries. The EBA was established on 1 January 2011 on the basis of *Regulation (EU) No 1093/2010 of the European Parliament and of the Council of 24 November 2010 on the establishment of the European Supervisory Authority (European Banking Authority), amendment of Decision No. 716/2009 / EC and repealing Commission Decision 2009/78 / EC* (Official Journal of the EU L 331 of 15 XII 2010, p. 12).

[21] https://www.consilium.europa.eu/en/policies/relocation-london-agencies-brexit/ [access: 2 XII 2019].

[22] *Joint Opinion of the European Supervisory Authorities*…, p. 10 [access: 2 XII 2019].

[23] AMLD4 provides for certain minimum common standards, and EU Member States have the option of raising those standards when transposing AMLD.

[24] 'Compliance' is understood as ensuring compliance of the entity's activities with legal provisions and their monitoring, https://www.rewi.europa-uni.de/pl/lehrstuhl/pr/poloerecht/projekte/Compliance/index.html [access: 2 XII 2019].

In the event of the UK's withdrawal from the EU without a ratified agreement or in the absence of agreement between the UK and the EU supervisory authorities, equivalent to such an agreement, the EU supervisory authorities will be able to exchange information on ML/TF countermeasures to a limited extent. If Brexit is based on a contract, the exchange of information (which is sensitive for electronic payments, as they often have cross-border elements) will depend on the conditions adopted. In this case, the so-called Memorandum of Understanding (MoU)[25] between European Supervisory Authorities and the Financial Conduct Authority (FCA).[26]

Risk related to the development of new technologies[27]

This type of risk is associated with the new areas of FinTech and RegTech.[28] Examples of fintech solutions are secure mobile applications[29] for banks and online services (loans) or online factoring, in which the entire procedure and assessment of the customer's credit (payment) ability is carried out electronically and remotely, and entities offering these services use, among other things, databases of economic information offices, social networking sites such as Facebook, LinkedIn or Instagram.

The most important fintech entities that have their headquarters in Poland are: PayU, Blue Media, Polish Payment Standard – Polish Payment Standard (BLIK), Currency One, Finanteq, VoicePIN, ZenCard. Examples of foreign fintech entities are Revolut[30] and N26.[31]

Examples of fintech solutions in the payment segment are the BLIK payment system[32] and payment systems on mobile devices:[33] Google Pay, Apple Pay, Samsung Pay, as well as contactless payments, unrelated or related to the above systems.

---

[25] The memorandum sets out the rules for the future and wishes to accept specific obligations, https://pressto.amu.edu.pl/index.php/cl/article/viewFile/6437/6458 [access: 2 XII 2019].

[26] Equivalent to the Polish Financial Supervision Authority in Great Britain, https://www.fca.org.uk [access: 2 XII 2019].

[27] *Joint Opinion of the European Supervisory Authorities*…, p. 12 [access: 2 XII 2019].

[28] 'RegTech' is the use of new technologies to support regulatory processes and their application – definition developed by Institute of International Finance, see https://www.iif.com/Innovation/Regtech [access: 2 XII 2019]. See also *Financial Stability Implications from FinTech*…, p. 34 [access: 2 XII 2019]. In addition to 'FinTech' and 'RegTech', there is a third term – 'InsureTech' – refers to the use of modern technologies in solutions that result in increasing the functionality of the insurance sector.

[29] Payment applications for integration with mobile devices (e.g. telephone, iPad).

[30] https://www.revolut.com/pl-PL [access: 2 XII 2019].

[31] https://n26.com/en-eu [access: 2 XII 2019].

[32] https://blikmobile.pl [access: 2 XII 2019].

[33] These are payments made using a mobile device equipped with an operating system, with a multimedia interface using radio technology, wireless telecommunications networks (GSM, GPRS, UMTS, Wi-Fi, NFC, RFiD, Bluetooth), https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf [access: 4 X 2017].

RegTech tools enable entities to collect and analyze data faster, more cheaply and more easily.[34] This is particularly important from the AML/TF point of view (increasing the transparency of financial operations). An example might be the automatic verification of the list of politically exposed persons, (PEP), i.e. according to AMLD4, among others: presidents, prime ministers, deputies, ministers and their families. One of the RegTech's solutions is a dedicated application programming interface (API)[35] designed for a specific financial institution. This action results from meeting the needs of a given institution or providing its economic data from many sources and integrating them so that this financial institution, e.g. a bank, receives all the required information in one system.[36]

The development of technology opens new opportunities for FinTech and RegTech providers but carries the risks associated with ML/TF. Based on the already mentioned joint opinion of the European Supervisory Authorities, the following risks arising from the use of FinTech can be identified:[37]

- providing services in the form of unregulated financial products that do not fall within the scope of the AML/CTF legislation,
- the quality of information collected during the customer due diligence process (CDD),
- misunderstanding of FinTech suppliers regarding AML/CTF requirements and other regulations,
- compliance culture[38] differences between supervised entities,
- the emergence of new technologies at the stage of remote establishing relationships with customers (so-called onboarding), without maintaining security measures in the field of combating cybercrime and identity theft,
- over-reliance by financial institutions (e.g. banks) on outsourcing[39] to fintechs, without paying due attention to their control mechanisms (a common phenomenon in Poland).

When introducing new assistive technologies for RegTech, there may be risks associated with[40]

- uncritical reliance of companies on technological solutions that can lead to limiting people's involvement in transaction monitoring;

---

[34] http://fintechpoland.com/pl/projects/raport-regtech-znaczenie-innowacji-regulacyjnych-dla-sektora-finansowego-i-panstwa/ [access: 2 XII 2019]; https://medium.com/blog-transparent-data/co-to-jest-regtech-i-jak-ma-się-do-fintech-f27bab5a3a55 [access: 2 XII 2019].

[35] Application programming interface; set of rules on how computer programs communicate with each other.

[36] For example, Transparent Data system, https://transparentdata.pl [access: 2 XII 2019].

[37] *Joint Opinion of the European Supervisory Authorities*…, p. 12 [access: 2 XII 2019].

[38] Ensuring compliance with legal regulations, standards or recommendations (editor's note).

[39] Abbreviation of English words: 'outside-resource-using'. 'Outsourcing' consists in the transfer of tasks, functions, projects and processes to be carried out by an external company (editor's note).

[40] *Joint Opinion of the European Supervisory Authorities*…, p. 13 [access: 2 XII 2019].

- no legal regulations regarding RegTech;
- misunderstanding of entities in the areas of new technologies in the field of CDD, which makes entities vulnerable to ML/TF threats;
- over-reliance on entities to whom the possibility of using certain processes has been delegated (the principle of clean hands), without proper insight into their activities and procedures, which in consequence may lead to:
  – difficulties in assessing customer data,
  – doubts ,regarding the reliability of data (records) caused by unsafe practices of their acquisition and storage by RegTech suppliers;
- lack of transparency when transferring responsibility between RegTech suppliers, especially when processes have been transferred to them under an outsourcing agreement and these entities are not obligated institutions under AMLD4.

These threatening situations have been described in the Opinion of the European Supervisory Authorities (ESA) on the use of innovative solutions related to CDD.[41]

Financial transactions have been fully digitized, which various service providers must take into account, especially as these changes significantly increase ML/TF risk. The analysis of the customer profile is fundamental from the point of view of AML's obligations in the area of customer identification and verification. The following types of innovative solutions can be distinguished when assessing the client:[42]

- non-face-to-face verification solutions based on traditional identity documents (passport, driving license) using mobile devices (e.g. smartphone),
- verification solutions based on central repositories of identification documents (created as joint ventures for many companies or outsourced to an external partner),
- solutions based on artificial intelligence (AI) processing a significant amount of information from various sources in different languages. Owing to these systems, it is possible to analyze e.g. transaction history, GPS location, social networking sites, online publications, registers of real beneficiaries, politically exposed persons or their family members. The systems also allow remote detection of false identification documents based on document features (watermarks, photographs, lines sensitive to UV rays, document layout).

Risk related to virtual currencies

Milton Friedman noted that: (...) *the Internet will become one of the main forces reducing the role of governments. The only thing that we lack, but which will certainly be developed soon, is real e-cash a method by which funds can be transferred via*

[41] See *Opinion on the use of innovative solutions by credit and financial institutions in the customer due diligence process*, https://esas-joint-committee.europa.eu/Publications/Opinions/Opinion%20on%20the%20use%20of%20innovative%20solutions%20by%20credit%20and%20financial%20institutions%20(JC-2017-81).pdf [access: 2 XII 2019].

[42] Ibidem, p. 5.

the Internet between entities A and B, while both entity A does not know B and entity B does not know A[43].

The following currency trading models are distinguished in financial systems:[44]

- centralized: there is one entity responsible for the issue and control of trading in a particular currency. Transactions are carried out only through the entity that keeps a record of all transactions,
- decentralized: the central entity delegates to its subordinate structures part of the competences and tasks to be performed,
- dispersed: no hierarchy. No entity remains superior to another entity. There is also no central entity. Each trading participant has the option of contacting with the others. He may also be a currency issuer, may participate in trading control and supervision and have a record of all transactions in the system (which is appropriate for trading virtual currencies).

The payment system consists of a specific group of institutions and procedures used to ensure the efficient circulation of money in a given geographical area.[45] Within this payment system, four levels of participants' activity should be distinguished:

1) first level – entities being parties to executed payment transactions,
2) level two – direct entities handling transaction processing between level one participants; they are payment service providers, e.g. banks and payment institutions,
3) level three – entities participating in the clearing of transactions between level two participants (e.g. the National Clearing House in Poland),
4) level four – entities storing the funds of payment service providers or securities (e.g. the National Bank of Poland and the National Depository for Securities).

Within the payment system, the following systems are distinguished:[46]

- high-value payment system;
- retail payment system, which consists of:
  - card payment subsystem,
  - mobile payment subsystem,
  - the instant payment subsystem;
- securities settlement system.

Virtual currencies (VC) are not regulated financial products in the EU, which exposes customers to risks that are often unpredictable and their catalog is open.[47]

---

[43] Quotation for A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne zastosowanie kryptowaluty*, Warszawa 2018, p. 7.

[44] Ibidem, p.19.

[45] Ibidem, p. 79.

[46] Ibidem, p. 80.

[47] See *EBA Opinion on 'virtual currencies'*, https://eba.europa.eu/sites/default/documents/files/documents/10180/657547/81409b94-4222-45d7-ba3b-7deb5863ab57/EBA-Op-2014-08%20

Due to the lack of regulation at the EU level, national supervisory authorities should provide protection in this area. The European Banking Authority has been publishing reports indicating the risks associated with virtual currencies for years.[48]

Virtual currencies are generally divided into:[49]

- tokens accepted mainly by members of virtual communities that are issued and controlled by its creators, e.g. computer game authors (tokens: Facebook Credits, Amazon Coins, which are centralized virtual currencies); in this case, the issuer is the institution controlling the supply sphere (issue) and authorizes and settles transactions,
- cryptocurrencies.

The European Central Bank defines cryptocurrencies as: (...) *digitally presented value that has not been issued by the central bank, credit institution or electronic money institution, which under certain circumstances can be used as an alternative to money*.[50]

The most well-known example of virtual currency is Bitcoin. Its creator is considered a person (or persons) with a pseudonym Satoshi Nakamoto. Bitcoin was intended to allow for direct and anonymous transactions in e-commerce.[51] This system was to be independent of traditional financial institutions, and financial operations were to be completely separated from global financial systems and central clearing systems.

David Chum is seen as "the father of digital money" and "the father of anonymity on the Internet".[52] He presented a centralized system of anonymous payments increasing the security and privacy of users in relation to other systems existing at that time. In 1982, he published the paper *Blind signatures for untraceable payments*, in which he described the violation of privacy by existing settlement systems.[53] Chum's assumptions were based on the need to limit the financial intermediary's knowledge of time, value and subject of payment, as well as limit the possibility of analyzing

Opinion%20on%20Virtual%20Currencies.pdf?retry=1 [access: 2 XII 2019].

[48] http://www.eba.europa.eu/-/eba-warns-consumers-on-virtual-currencies, http://www.eba.europa.eu/documents/10180/657547/EBA-Op-2014-08+Opinion+on+Virtual+Currencies.pdf; https://www.eba.europa.eu/documents/10180/1547217/EBA+Opinion+on+the+Commission%E2%80%99s+proposal+to+bring+virtual+currency+entities+into+the+scope+of+4AMLD; https://www.eba.europa.eu/documents/10180/2139750/Joint+ESAs+Warning+on+Virtual+Currencies.pdf [access: 2 XII 2019].

[49] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, p. 15.

[50] Ibidem, p 25.

[51] Ibidem, pp.34–37. Bitcoin assumptions are presented in *Bitcoin: A Peer-to-Peer Electronic Cash System*, by an anonymous author with a pseudonym Satoshi Nakamoto. However, it is believed that under this pseudonym there are technological corporations: SAmsung, TOSHiba, NAKAmichi, MOTOrola.

[52] Ibidem, p 30.

[53] Ibidem.

too much metadata (Big Data[54]). For a financial intermediary, data on the location of a person, their lifestyle (e.g. paid travel, hotels, restaurant bills, small expenses, food, medicine, press, support of political and religious institutions) are unnecessary from the point of view of payment. D. Chum developed the so-called blind signature (digital signature, a new type of cryptography). This solution led to the so-called asymmetrical anonymity in which the payer was unknown and the person accepting the payment could be identified, if necessary. The disadvantage of this solution was susceptibility to so-called 'double-spending', i.e., in some cases, the possibility of spending the same funds twice.[55]

In the development of cryptocurrencies, it is also not possible to overlook the so-called 'cypherfunk' movement[56]. Privacy is the foundation of a modern and digital society. It was not believed that it would be ensured by governments, but only through encryption tools and a decentralised communication system. Under the influence of this movement, one of its members presented in 1998 a draft of the anonymous digital currency b-money. The basis for a well-functioning digital society was the existence of an efficient medium of exchange (money) and effective ways of enforcing contracts. The most important element of the movement was the design of rules for making payment transactions without the participation of intermediaries. It was assumed that all transactions would be recorded in the register, and each of its participants had a copy of it. As a result, such a register is impossible to falsify.[57] These concepts led to the creation of bitcoin cryptocurrency in 2008, which was launched in 2009.

Virtual currencies and electronic money[58]

Virtual currencies are often misidentified with the so-called electronic money.[59] The difference between virtual currencies and electronic money outside the regulatory

---

[54] The use of advanced techniques to analyze large resources of diversified data that may not be structured and may come from various sources, https://www.ibm.com/analytics/hadoop/big-data-analytics [access: 2 XII 2019].

[55] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 30–31.

[56] 'Cypherpunk' – an activist promoting the widespread use of strong cryptography as a path to social and political change. They originally formed an informal group communicating through mailing lists for a goal of achieving privacy and security through the active use of cryptography, https://pl.wikipedia.org/wiki/Cypherpunk [access: February 17 2010] – (editor's note).

[57] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 32–33.

[58] In a letter to the banks of 10 July 2015, the Polish Financial Supervision Authority made a legal analysis of the issue of electronic money, see *Position on issuing prepaid cards of 10 July 2015*, https://www.knf.gov.pl/knf/pl/komponenty/img/stanowisko_ws_wydawania_kart_przedplaconych_42192.pdf [access: 2 XII 2019].

[59] Within the meaning of the *Act of 19 August 2011 on payment services* (i.e.: Journal of Laws of 2019, item 659, as amended) and *Directive 2009/110 / EC of the European Parliament and of the Council of 16 September 2009 on taking and operation of electronic money institutions and*

sphere is that virtual currency is an artificial unit of account, while the unit of electronic money is expressed in an entity with legal tender status. Virtual currencies, on the other hand, do not have to be associated with traditional money and its fiat currency (FC).

The distinguishing factor of cryptocurrencies in terms of technology is open source code and open source.[60] The use of a distributed transaction system and the structure being based on cryptography are in favour of classifying an instrument for cryptocurrencies. Classification of a given instrument for cryptocurrency is supported by the use of a distributed transaction system and. There must also be a global, public and distributed database, including transactions using cryptocurrency.

The basis of bitcoin was open source software, which is publicly available source code, so that everyone could analyze and improve it on an ongoing basis. Bitcoin also enabled the processing of direct transactions between Internet users, using a peer-to-peer (also: person-to-person), P2P[61] communication protocol, which meant no central server (transaction information repository) and no need to use a transaction intermediary.[62] There is therefore no mediation of the so-called trusted third party.

Bitcoin transactions are saved in blocks, which then combine into a blockchain, i.e. the record of approved transactions.[63] These entries make up the public ledger (database) stored by all bitcoin users' computers. The innovation of this system consists in a blockchain operating within a public distributed register of bitcoin transactions, in which it is impossible to withdraw the transaction, which is beneficial for the payment merchants (e.g. a store accepting payment in a cryptocurrency), but can be risky for the payer.[64]

There is no central unit or supervisory authorities in the bitcoin system. The user structure of this bitcoin system consists of two levels: the first level includes users – merchants, and the second level includes entities supporting transaction processing, such as payment intermediaries and cryptocurrency trading platforms.

All cryptocurrency trading platforms are on the list of public warnings issued by the Polish Financial Supervision Authority.[65] Until they were embraced by AMLD4,

prudential supervision of their activities, amending Directives 2005/60/EC and 2006/48/EC and repealing Directive 2000/46/ EC (Official Journal of the EU L 267 of 10 October 2009, p. 7).

[60] Products that allow the use of their source code https://pl.wikipedia.org/wiki/Otwarte_oprogramowanie [access: 2 XII 2019].

[61] It means the equivalence of network participants, i.e. any computer connected to the network can send and receive data on the network, which allows files to be downloaded and made available to computers connected to the network, https://poradnikprzedsiebiorcy.pl/-peer-to-peer-definicja-historia-powstania-i-wplyw-na-rozwoj-internetu-cz-1 [access: 2 XII 2019].

[62] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, p. 35.

[63] https://blockgeeks.com/guides/what-is-blockchain-technology/ [access: 2 XII 2019]; https://pl.wikipedia.org/wiki/Blockchain [access: 2 XII 2019].

[64] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 51–53.

[65] The list is available at the link https://www.knf.gov.pl/dla_konsumenta/ostrzezenia_publiczne [access: 2 XII 2019].

they did not have to use any AML/CTF measures (including customer identification and verification), which often led to a situation in which funds from the so-called unauthorized payment transactions, due to the misappropriation of access data to the bank account, were transferred to these platforms by instant payment systems and then invested in bitcoins. Due to such a procedure, it is in principle impossible to identify the perpetrators and bring them to criminal liability, and the proceedings were discontinued at the stage of preparatory proceedings in the case.

Bitcoin – transaction processing and legal dimension

One of the biggest problems of a bitcoin system is throughput. It is estimated at the level of one transaction per second or a maximum of seven transactions per second. For comparison, the average number of transactions per second in the PayPal service is 100, Visie – 2000 while the maximum performance of this system is 56,000 transactions per second. Processing one bitcoin transaction takes from several minutes to an hour. The objection against this system is its high energy consumption. The functioning of the system requires the constant supply of energy to equipment, and the demand for energy increases with the development of the network. Estimates indicate that one transaction in the Bitcoin system absorbs the average daily electricity demand of one and a half households in the US, and the daily costs of energy consumed by this system reach $ 15 million. The bitcoin system is also characterized by pseudo-anonymity, which should be associated with the public access to the record of executed transactions. This allows you to track and analyze transactions marked with a specific computer IP address. An important drawback is the cryptographic protocol. It has not been broken yet, but it is theoretically possible. This can occur when someone gains more than 50 percent of the system's computing power. This can lead to a change in the current blockchain[66] consensus and repeatedly issue the same value units.[67]

Cryptographic assets (rights) are defined[68] as values based on cryptography and distributed ledger technology (DLT), one example of which is blockchain. DTL, on the other hand, is a distributed database with registers that can be replicated. They are shared and synchronized within the consensus of geographically dispersed companies and individuals.[69]

Blockchain technology (understood as one of the types of Distributed Ledger Technology, DLT) is primarily used to transfer bitcoins between individuals using private (used to control the ownership of bitcoin units) and public keys. DLT is used to record bitcoin unit transfers. When a transaction is generated, it is distributed

[66] See wider: https://www.bbva.com/en/difference-dlt-blockchain/, https://101blockchains.com/blockchain-vs-distributed-ledger-technology/ [access: 2 XII 2019].

[67] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 123–127.

[68] See *EBA reports on crypto-assets*, https://eba.europa.eu/eba-reports-on-crypto-assets [access: 2 XII 2019].

[69] https://pl.wikipedia.org/wiki/Technologia_rozproszonego_rejestru [access: 2 XII 2019].

throughout the DLT network, which, using a private key, verifies that the seller owns the bitcoin units. DLT enables storing, updating and verifying information in a decentralized manner.[70]

Trading virtual currencies is exposed to the risk of money laundering and terrorist financing, which can be remedied by considering entities conducting such economic activity as obligated institutions.[71] This applies to the provision of services in the field of:

- exchange of virtual currencies for means of payment,
- exchanges between virtual currencies,
- intermediation in the exchanges referred to above,
- keeping accounts in an electronic form as a set of identification data, providing authorized persons with the option of using virtual currency units, including exchanging transactions.

According to the AMLD5 Directive, custodian wallet providers[72] are recognized as obligated institutions. A legal definition of virtual currencies has also been introduced here, defining them as digital determinants of values that are not issued or guaranteed by a central bank or public authority and do not have to be associated with a legally binding currency, and have no legal status of currency or money, but are accepted by natural or legal persons as a means of exchange and can be transferred, stored or sold electronically. In Poland, the term virtual currencies is understood as a digital representation of values that are not:[73]

- legal means of payment issued by Narodowy Bank Polski (NBP), foreign central banks or other public administration bodies,
- international accounting units established by an international organization and accepted by individual countries belonging to or cooperating with that organization,
- electronic money as defined in The Payment Services Act,[74]
- financial instruments, as defined in the Act on Trading in Financial Instruments,[75]
- bills of exchange or checks that are exchangeable in business transactions for legal means of payment and accepted as a means of exchange.

Virtual currencies are classified as so-called property values,[76] which also include property rights, other movable property or real estate, means of payment, financial

[70] A. Piotrowska, *Bitcoin. Płatnicze i inwestycyjne*…, pp. 51–53.

[71] Article 2 section 1 point 12 of the Act on counteracting money laundering and terrorist financing.

[72] Article 3 point 19 AMLD5 refers to entities providing services consisting in the storage of private credentials on behalf of their clients for the purposes of possessing, storing and transferring virtual currencies.

[73] Article 2 section 1 point 26 of the Act on counteracting money laundering and terrorist financing.

[74] *The Act of 19 August 2011 on Payment Services* (i.e.: Journal of Laws of 2019, item 659, as amended).

[75] *The Act of 29 July 2005 on Trading in Financial Instruments* (i.e.: Journal of Laws of 2018, item 2286, as amended).

[76] Article 2 section 2 point 27 of the Act on counteracting money laundering and terrorist financing.

instruments within the meaning of the Act on Trading in Financial Instruments, other securities and foreign exchange values.

The European Banking Authority and the European Securities and Markets Authority (ESMA[77]) have published a report on the application of EU law to crypto-assets.[78] Based on the above report, the following threats related to virtual currencies can be listed:

- lack of knowledge and understanding of the functioning of VC companies and their products,
- the growing number of online transactions accompanied by a negligible identification of the customer.

In 2018, FATF adopted a recommendation (Recommendation 15[79]) aimed at including the terms "virtual assets" and "virtual assets service providers" in the definition. As a consequence, EU AML/CTF legislation currently applies to these assets and entities. Crypto-assets mean:

- assets based on cryptography and DLT or similar technologies,
- assets that are not used and guaranteed by a bank or public authorities,
- assets that can be exchanged and used for investment or facilitating access to goods and services.

It is assumed that virtual currencies may meet the legal criteria for electronic money and be subject to all regulatory requirements for electronic money where:

- are stored electronically,
- have a monetary value,
- represent specific claims against a virtual currency publisher,
- are issued in exchange for funds received,
- are issued for the purpose of making payments,
- are accepted by other entities, which are not only publishers.

Virtual currencies are defined by the EBA as:[80]

- having a digital representation of value, which does not exclude the possibility of a physical equivalent,
- not issued by a central bank or other public authority,
- not related to traditional currency,
- acceptable by legal and natural persons as a means of payment,
- those that can be transferred, stored or disposed of electronically.

---

[77] https://www.esma.europa.eu/about-esma/esma-in-short/whos-who [access: 2 XII 2019].

[78] See *Advice: initial coin offerings and crypto-assets*, ESMA50-157-1391, January 9 2019, https://www.esma.europa.eu/sites/default/files/library/esma50-157-1391_crypto_advice.pdf [access: 2 XII 2019].

[79] http://www.fatf-gafi.org/publications/fatfrecommendations/documents/regulation-virtual-assets-interpretive-note.html [access: 2 XII 2019].

[80] See *EBA opinion on 'virtual*…, p. 11 [access: 2 XII 2019].

The EBA opinion identifies approximately 70 specific risks associated with virtual currencies, including:[81]

- risks to users,
- risks to other market participants,
- risks to financial integrity,
- risks to payment systems in fiat currencies,
- risks to regulators.

Risk related to the legislative divergence of EU countries and divergent supervisory practices

This risk is due to the principle of minimum harmonization[82] included in EU directives. It is also increased by the different implementation[83] of AMLD directives into the legal orders of the Member States.

Differences in the consistent application of anti-money laundering legislation further exacerbate divergent practices of supervisory authorities in the Member States regarding the same issues. The discrepancy in these practices may result from:

- another risk-based approach,
- a different understanding of ML/TF risk by supervisory authorities,
- the various measures involved in ML/TF supervision in individual Member States.

Threats resulting from discrepancies in anti-money laundering legislation mean that some entities obtain permits in countries more liberally approaching this phenomenon, i.e. services will be provided by these entities in other EU Member States.

In some countries, AML regulations have been formulated in such a way that supervisory authorities cannot act until they find evidence of criminal activity. Due to the applicable single passport principle, such action by supervisory authorities is a particular threat because once an entity obtains permits, it may operate on other markets.

Under the previous AML directives, there was no outright articulated obligation of cooperation between financial information authorities of individual countries in the xchange of information. For this reason, there was a risk that these bodies had only a partial view of the ML/TF situation. Otherwise it was presented in AMLD5. These provisions will also be complemented by guidelines on cooperation and multilateral agreements on the exchange of information.

[81] Ibidem, p. 5.

[82] 'Minimal harmonization' means that the EU legislator sets a common and minimum standard of regulation for a given area, https://www.eversheds-sutherland.com/documents/global/poland/articles_pdf/pl/2011-12 01_eps_prawo_konsumenckie_ue_dyrekywy_oparte_na_harmonizacji_minimalnej_akunkiel.pdf, p. 46 [access: 2 XII 2019].

[83] Introduction of the EU directive into the national legal order.

Risk arising from divergent supervisory practices[84]

Moneyval Committee[85] and FATF have long questioned some AML/CTF practices of some countries regarding their adequacy. The European Banking Authority has made allegations against one of the supervisors of breaches of EU law[86] in relation to the failure to comply with AML requirements.

A different approach of supervisory authorities to supervised entities results from:

- differences in risk levels,
- uncritical adoption of the approach of the authorities of other Member States in specific sectors to the estimated risk,
- differences in the training of ML/FT personnel.

Risk related to internal control weakness[87]

This risk results from the poor implementation of the means of identification and verification of the customer using the banking system. One of the main assumptions of AMLD4 was the introduction by obligated institutions of internal control systems tailored to the risk to which the entity is exposed in connection with its activities (the so-called risked based approach).

Although supervisory authorities take the view that supervised entities have put in place appropriate internal control systems, particularly as regards transaction recording, customer identification and verification, and reporting of suspicious transactions, the data received by the European Supervisory Authiorites (ESA) lead to the conclusion that the functioning of these policies in practice is inefficient.[88]

Another drawback is the insufficient resources of supervised institutions in the field of AML/CFT. Supervisory authorities identify the most common violations of AML/CFT legal requirements consisting of:

- insufficient control caused by incorrect identification and verification of the client, including in the scope of actual beneficiaries,
- inadequate internal control, AML/CFT policies and procedures, and client risk assessment.

---

[84] *Joint Opinion of the European Supervisory Authorities*…, p. 17 [access: 2 XII 2019].

[85] A committee operating at the Council of Europe to evaluate anti-money laundering and anti-terrorist financing measures, https://www.kic.gov.pl/pl/documents/764034/1002265/20120911_MONEYVAL_inf.pdf [access: 2 XII 2019].

[86] The recommendation concerned the Maltese Financial Intelligence Unit, https://www.eba.europa.eu/-/eba-issues-recommendation-to-the-maltese-financial-intelligence-analysis-unit-in-relation-to-its-supervision-of-pilatus-bank [access: 2 XII 2019].

[87] *Joint Opinion of the European Supervisory Authorities*…, p. 20 [access: 2 XII 2019].

[88] Ibidem.

Risk arising from de-risking[89]

The phenomenon of de-risking is caused by the wrong approach of entities to ML/TF risk management, consisting in refusing to enter into business relationships with clients assessed as posing a risk from the perspective of AML/CTF policies of obligated institutions. This approach leads to the "push" of these entities into the spheres where they remain beyond any control in the field of ML/TF. This, in turn, causes the financial sector to be exposed to ML/TF risk. Lack of access of excluded entities to the financial system leads to their transactions outside the AML/CFT control systems. They go down to informal payment channels to meet their needs (mainly through cash transactions, which makes it impossible to track transactions).[90]

The European Supervisory Authorities take the view that the risked-based approach does not require obligated institutions to terminate contracts or terminate a business relationship only because of a higher risk of money laundering and terrorist financing. This approach, rather than preventing the above mentioned issues, would increase the risk.

Risk of financing terrorism[91]

Supervisory authorities report that the biggest problem related to the risk of financing terrorism is the weakness of the control system in relation to transaction monitoring. People financing terrorism may not necessarily want to hide their identity, they can also use funds from legal sources (e.g. crowdfunding). For this reason, customer identification and verification goes to the downstream plan, giving way to proper transaction monitoring.[92]

The fight against terrorist financing is hampered by the lack of access to relevant information, often held by law enforcement authorities, that has helped identify the threat at an early stage. That is why it is so important for law enforcement authorities to cooperate with supervisory authorities in this respect, because each of these entities has a view of the same situation from a different perspective.

Specific risks related to the financial services sector

Sector specific risk will be presented jointly for credit,[93] payment and electronic money institutions as the institutions most vulnerable to ML/TF threats. The following basic problems can be highlighted in this area:

---

[89] Ibidem, p. 25.

[90] Ibidem.

[91] Ibidem, p. 24.

[92] Ibidem.

[93] Article 4 section 1 point 17 of *the Act of 29 August 1997 – Banking Law* (i.e.: Journal of Laws of 2019, item 2357).

- sector specific risk;
- quality of controls and the most frequent infringements in the financial sector, including:
  - incorrect level of customer identification and verification by financial institutions, risk related to customer business models,
  - monitoring of ongoing cooperation, including transaction monitoring,
  - overall sector risk profile,

Symptoms indicating an increased ML/TF risk include the following customer behavior:

- making economically incomprehensible decisions, lack of interest in more favorable financial conditions of the product,
- withdrawing large amounts from ATMs,
- frequent transactions of similar value,
- lack of orientation in product features,
- his or her behavior or the presence of an accompanying person indicating that the client is controlled and does not make any decisions alone,
- refusal to perform activities related to his or her identification and verification,
- resignation from the transaction if the institution shows interest in the customer,
- a proposal to grant a financial advantage to the person carrying out the identification in exchange for failure to carry out the act or to carry it out in an inappropriate manner,
- using documents that are doubtful as to their authenticity.

Credit institutions and banks[94]

Credit institutions[95] (CIs) and banksare used by ML/TF risk customers as institutions for entering the financial system.[96] This was particularly evident when opening bank accounts based on a verification transfer.[97] The Polish Financial Supervision Authority has considered that the conclusion of a bank account agreement using a verification transfer from another payment account as a means of confirming the customer's identity is acceptable if it is not possible to conclude the next payment account agreement

[94] *Joint Opinion of the European Supervisory Authorities*…, p. 30 et seq. [access: 2 XII 2019].

[95] Article 4 section 1 point 17 of the Banking Act.

[96] D. Chodziński, *Pranie pieniędzy jako jedna z form działania zorganizowanych grup przestepczych*, Legionowo 2012, p. 19, http://www.csp.edu.pl/download/6/16760/Pranie-pieniedzyjakojednazformdzialaniazorganizowanychgrupprzestepczychDChodzinsk.pdf [access: 4 XII 2019].

[97] See Guideline 6 to the *KNF Recommendation of November 2015 regarding the security of payment transactions carried out on the Internet by banks, national payment institutions, national electronic money institutions and cooperative savings and credit unions,* https://zarabiajnabankach.pl/wp-content/uploads/2016/07/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf, p. 16 [access: 2 XII 2019].

with another payment service provider, using the transfer from the account opened to confirm the identity with this provider.

Cash transactions are also a factor causing the development of the ML/TF threat, especially since the majority of credit institutions are retail institutions, i.e. consumer and mass institutions. At the same time, institutions are exposed because of cross-border transactions, especially where the Member State is seen as a financial center.

When analyzing the financial transactions carried out by these institutions, an annual increase in violations of anti-money laundering regulations described as "serious breaches" can be observed:

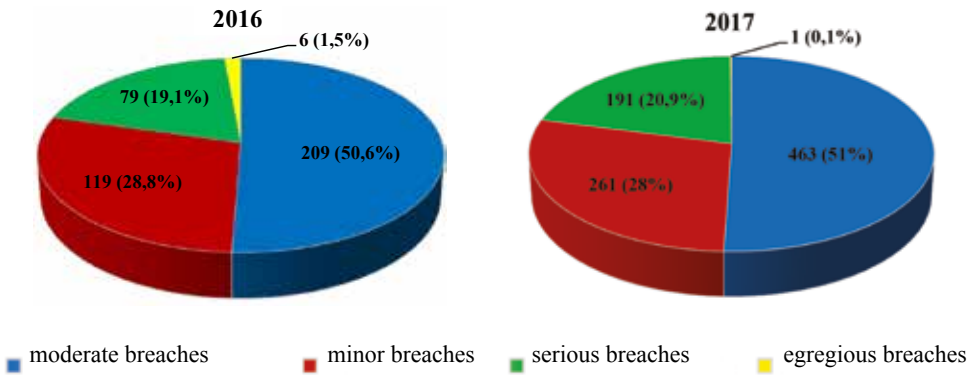


Chart 1. Violations of anti-money laundering regulations.

Source: *Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, p. 34 [access: 2 XII 2019].

Electronic money issuers, EMI[98]

The level of risk associated with issuing electronic money depends primarily on: access methods to e-money products (e.g. remote on-boarding customers[99]), features of e-money products, the extent to which EMI use other entities to distribute and remit e-money on their behalf.

The more restrictions are placed on the use of the e-money product, the less susceptibility to ML/TF. The restrictions used include, among others, payment limits, no ATM transactions, e-money acceptance possible in a limited network of merchants,[100] no person-to-person transactions and no cross-border transactions. At the same time, the above mentioned restrictions and e-money legal definitions mean

[98] *Joint Opinion of the European Supervisory Authorities*…, p. 46.

[99] Remote conclusion of contracts with the customer.

[100] Within the meaning of art. 2 point 1b of the Act on payment services.

that the use of e-money is restricted.[101] The most common violations in the EMI sector include insufficient monitoring of policies and procedures, low ML/TF awareness, as well as the lack of transaction monitoring and lack of supervision of publishers over the e-money distribution network, which is important due to the EMI sector's dependence on technology. In the EMI sector, there is an increase in "material breaches" and a significant increase in "moderate breaches", as shown in Chart 2:

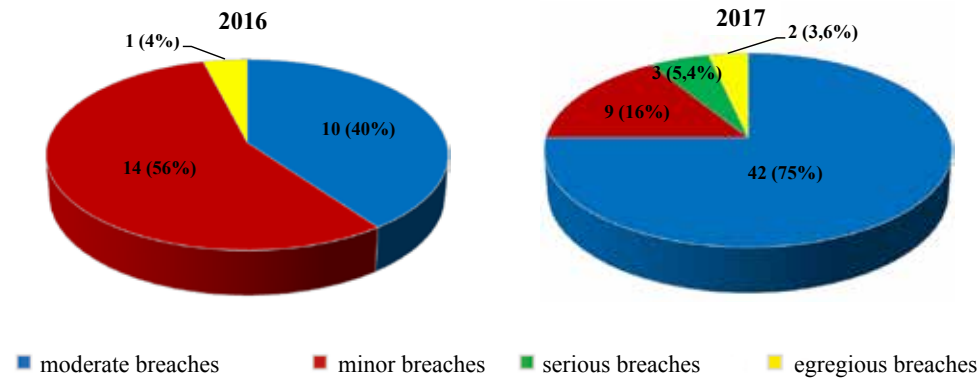


Chart 2. Violations of regulations related to the use of electronic money.

Source: *Joint Opinion of the European Supervisory Authorities of 4 October 2019 on the risks of money laundering and terrorist financing affecting the European Union's financial sector*, https://eba.europa.eu/esas-highlight-money-laundering-and-terrorist-financing-risks-in-the-eu-financial-sector, p. 50 [access: 2 XII 2019].

Payment institutions, PI[102]

The risk of money laundering and terrorist financing in the payment institutions sector[103] is mainly associated with the type of services provided and the type of client. The greatest risk is associated with remittances,[104] especially with cash settlements.

The increased level of ML/TF restrictions introduced, associated with this sector, has led to de-risking practices directed by banks to money transfer service providers operating in regions with a higher ML/ TF risk. Remittances are particularly important in the case of services directed to clients who do not have access to regulated financial

[101] Until 2019, the KNF granted only one permission to issue electronic money. This permission was received by Company Billon Solutions, https://businessinsider.com.pl/finanse/billon-solutions-licencja-e-money/xjb6be1, https://billongroup.com/pl/ [access: 2 XII 2019].

[102] Within the meaning of art. 2 point 11 of the Payment Services Act.

[103] *Joint Opinion of the European Supervisory Authorities*…, p. 52.

[104] Within the meaning of art. 3 section 3 of the Payment Services Act.

services or have limited access to them. The use of the hawala system[105] for ML/TF purposes by low-value money transfers[106] is observed.

The most common infringements in the payment institutions sector

Supervisory authorities check to what extent the policy of payment institutions is adequate to the provisions regarding customer identification and verification, transaction register and suspicious transactions reporting. However, there are problems in the effectiveness of the practices used. There is also concern about the low awareness of participants in the payment institutions sector regarding ML/TF threats resulting from wrong assessment of the client risk and his business activities, including from the need to process transactions quickly, which is related to this sector.

Summary

The analysis of the above legal regulations and the positions of individual supervisory authorities leads to the conclusion that due to the geometric increase in the number of electronic payments and their digitization at the time of issuing these provisions or their implementation into the national legal system, they are not adequate to reality. This entails increased vulnerability to the risk of money laundering and terrorist financing.

The number of regulations both in the European Union and in Poland and the degree of their complexity allows us to conclude that whenever we deal with innovative changes in regulations, Americans invent it, the Chinese copy it, and Europeans bring it into practice. This is clearly demonstrated by the fact that despite the possibility of issuing electronic money for many years, the first authorization in this respect was granted in Poland only in 2019.

The challenges faced by the entire electronic payments market, as well as supervisory authorities, are adaptation to the challenges and implications associated with the development of FinTech and RegTech, tracking trends and challenges in the area of virtual currencies, supporting the exchange of information and cooperation between financial institutions and supervisory authorities, as well as counteracting de-risking practices.

[105] Understood as an informal transfer of funds without the involvement of authorized entities (such as banks), http://www.nowastrategia.org.pl/system-hawala-i-finansowanie-terroryzmu/ [access: 2 XII 2019].

[106] See *National Money Laundering and Terrorist Financing Risk Assessment*, https://www.gov.pl/web/finanse/krajowa-ocena-ryzyka-prania-pieniedzy-oraz-finansowania-terroryzmu, p. 125 [access: 2 XII 2019].

Abstract

Research shows that the most popular payment instrument is a payment card, then a bank account with Internet access and then a PayPal account. The progress and increase in the digitization of electronic payments means that when legislation is issued in these areas, they are no longer adequate to the changing reality. This makes them vulnerable to the risks associated with criminal activities, including terrorist activities. Challenges for the entire electronic payments market and supervisory authorities in the coming years will focus on adaptation to new digital challenges, implications related to the development of FinTech and RegTech, tracking trends and challenges in the area of virtual currencies, supporting information exchange and cooperation between financial institutions and supervisory authorities and counteracting de-risking practices.

Keywords: FinTech, RegTech, anti-money laundering, counteracting terrorist financing, AML, CTF, EBA, KNF.

Leszek Wiszniewski

The role and significance of intelligence analysis in ensuring national security

In the 21st century people are forced to receive ever greater amounts of more or less useful information. One of the main factors influencing this phenomenon is technology developing at a staggering rate. People using the internet, including social media (e.g. Facebook, Twitter, YouTube), are the addressee of 34 gigabytes of data, which according to the scientists from the University of California in San Diego translates into 100,000 words daily (twice as much as at the beginning of 1980's)[1]. This results in the necessity to process information quickly and to rank it according to its significance. The politicians in our country holding managerial positions face similar problems. Information overload often impedes making the decision on which human health and life may depend. Therefore, due to the dynamically changing environment of national security as well as multitude of challenges and threats arising from this process, the significance of data analysis will be increasing. Of particular importance are materials drawn up on the basis of data coming from covert sources, which enable the geopolitical situation assessment (e.g. in case of hybrid activities carried out by an opponent, including disinformation) and taking pre-emptive action (e.g. preventing terrorist attacks by arresting people involved in their preparation or preventive use of security measures in case of vague signals of potential threats). The role of secret services (foreign intelligence and counterintelligence) and uniformed services will also be enhanced. The legislator gave them the competence to gather information by intelligence operational activity as well as to draw up on its basis adequately prepared analytical products for decision-makers.

In the first part of the work the problem of data analysis will be discussed from a theoretical standpoint, including definition issues and analytical cycle with particular emphasis on the ways of collecting information and different kinds of analysis. In the second part, legal conditions regarding selected Polish institutions responsible for ensuring security and preparing analyses within their scope of competence will be presented.

---

[1] *The American Diet: 34 Gigabytes a Day*, https://bits.blogs.nytimes.com/2009/12/09/the-american-diet-34-gigabytes-a-day/?_r=0 [access: 3 IX 2019].

Definition issues

At the beginning of the deliberations on data analysis we should refer to scientific literature in order to properly understand the terms used in this study. According to the definitions found in the *Polish Scientific Publisher Dictionary of the Polish Language* (Polish name: *Słownik Języka Polskiego PWN*) analysis is 'mental retrieving of characteristics or components of the examined phenomenon or subject'[2], whereas information is 'notifying of something, communicating something; message, instruction'[3]. In academic materials a phrase appears that 'information' is (…) *a collection of facts, events, features etc. of defined objects (things, processes, systems) contained in the message (communication), and expressed in such a way (form) that the recipient can respond to the situation that has arisen and undertake mental or physical action*[4]. In the specialist military and security literature one can read that (…) *data analysis in the area of national security consists in giving sense to this information, so (1) it includes correct inference about the consequences of the content of information and (2) it maximizes the usefulness of the information in making decisions by the recipient by formulating recommendations of specific action*[5]. Understanding the concept of information security remains an essential question. In the publications on the subject it is used in two contexts. The first of them refers more to information processing threat which is confirmed by Piotr Potejko (*information security is a set of activities, methods, procedures, undertaken by authorized authorities in order to ensure the integrity of the gathered, stored and processed information resources by securing them against adverse, unauthorized disclosure, modification or destruction[6])* and Krzysztof Liedel *(information security is very often understood as protection of information against adverse – accidental or aware – disclosure, modification, destruction or preventing its processing*[7]). Slightly different understanding of the term is suggested by Leszek Kwiatkowski, who claims that (…) *what is meant by information security of the subject (man or organization) is the possibility of obtaining information of high quality as well protecting the possessed information against loss*[8]. This view is shared by Krzysztof Liderman *(information security signifies justified trust in the quality and availability of the obtained and*

---

2 L. Drabik, E. Sobol, *Słownik języka polskiego*, Warszawa 2005, p. 14.

3 Ibidem, p. 277

4 P. Sienkiewicz, *10 wykładów*, Warszawa 2005, p. 62.

5 J. Konieczny, *Analiza informacji w dziedzinie bezpieczeństwa państwa*, Warszawa 2014, p. 256.

6 P. Potejko, *Bezpieczeństwo informacyjne*, w: K.A. Wojtaszczyk, A. Materska-Sosnowska (ed.), B*ezpieczeństwo państwa*, Warszawa 2009, p. 194.

7 K. Liedel, *Bezpieczeństwo informacyjne w dobie terrorystycznych i innych zagrożeń bezpieczeństwa narodowego*, Toruń 2008, p. 19.

8 L.F Korzeniowski, *Podstawy nauk o bezpieczeństwie*, Warszawa 2012, p. 147.

used information[9]) and Józef Janczak together with Andrzej Nowak who claim that (…) *when there is talk of information security it always refers to the subject which is threatened by lack of information or the possibility of losing information resources*[10]. The National Security Bureau experts made an attempt to clarify the term information security of the state. They presented the information security of the state in *The doctrines of information security in the Republic of Poland* (Polish name: *Doktryny bezpieczeństwa informacyjnego RP*) of 2015 as:

> (…) cross-sectoral area of security whose content refers to informational environment (including cyberspace) of the state; a process which aims to ensure secure functioning of the state in the informational space by controlling its own, internal infosphere as well as effective safeguarding national interests in the external (foreign) infosphere. It is achieved by conducting the following tasks: providing adequate protection of the possessed information resources and protection against hostile disinformation and propaganda activities (in the defensive sense), while simultaneously maintaining the capacity to conduct offensive activities in this area against potential opponents (countries or other entities). These tasks are specified in the (operational or preparatory) strategy (doctrine) of information security, while an adequate information security system is maintained and developed in order to execute them[11].

For the needs of this work it is worth adopting a broader definition – suggested by L. Korzeniowski or K. Linderman – of the term 'information security', which refers to the capacity of obtaining information allowing decision-makers to ensure national security.

The subchapter devoted to the definition issues is where it is worth explaining what propaganda (disinformation) and informational noise are, which have recently become a debate subject in the Polish public space. Disinformation is a message incompatible with the reality which may become (...) *an element of information fight between competing entities*[12] (e.g. states or companies). Propaganda and disinformation were more broadly defined in the project The doctrines of information security in the Republic of Poland: (…) *spreading manipulated or fabricated information (or a combination of both) in order to make the recipient behave in a specific way beneficial to the one who disinforms or in order to distract the attention from the actually*

[9] K. Liderman, *Bezpieczeństwo informacyjne*, Warsaw 2012, p. 22.

[10] J. Janczak, A. Nowak, *Bezpieczeństwo informacyjne. Wybrane problemy*, Warszawa 2013, p. 18.

[11] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP*, https://www.bbn.gov.pl/ftp/dok/01/Projekt_Doktryny_Bezpieczenstwa_Informacyjnego_RP.pdf [access: 3 IX 2017].

[12] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa 2012, p. 36.

existing events[13]. Whereas linguists define the term informational noise as 'an excess of information hampering the extraction of true and essential information'[14].

Intelligence cycle

Data analysis is only one of a few stages of a broader process which aims to support the authorities of a given state in decision-making, allowing them to ensure broadly understood security of the citizens. In the publications on the subject this process is traditionally referred to as intelligence cycle, which usually consists of – depending on the taxonomy adopted by particular scientists – four to six stages. For the purpose of this publication four phases of this cycle have been adopted which include:

1) **defining the information demand** by state organs which are authorized to do so under applicable law and commissioning tasks to the subordinated institutions (e.g. security and public order services, intelligence and counter-intelligence agencies). This stage is closely correlated to the current global events and occurrences (e.g. armed conflicts, terrorism) which may have negative influence on the national security. It is on their basis that the government lays down the guidelines for the activities of the services. In this context it is necessary for the decision-makers to be able to prioritize threats;
2) **collecting information by services according to the authorities' needs**;
3) **analysing the gathered data**[15];
4) **passing the final analytical products (in accordance with competences) to the recipients**. Tomasz Aleksandrowicz notices that this stage – in case when there is no reaction of the authorities to the received document – concludes the intelligence cycle, and if another commission appears then we deal with so-called open intelligence cycle[16].

[13] *Projekt Doktryny Bezpieczeństwa Informacyjnego RP…*

[14] http://sjp.pwn.pl/sjp/;3067966 [acces: 13 V 2017].

[15] The problem of collecting data and its processing will be presented in the further part of the publication.

[16] T.R. Aleksandrowicz, *Analiza informacji w administracji i biznesie,* Warszawa 1999, pp. 55–56.

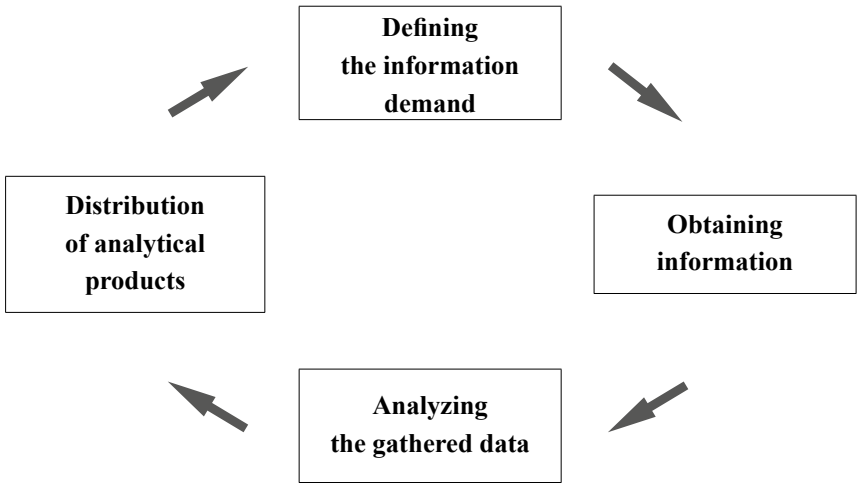


Figure. Intelligence cycle.

Source: Self-study based on K. Liedel, P. Piasecka, T. R. Aleksandrowicz, *Analiza informacji. Teoria i praktyka*, Warszawa, pp. 82–87.

It is worth presenting a few examples of disturbing the information cycle. Experts distinguish mistakes made both by decision-makers and analysts. The recipients of the final products may:

- formulate their needs in an unclear way which may result from the lack of ability to use the possessed forces and resources, including secret services;
- not use the knowledge and conclusions presented in the documents[17]. In this context it is worth pointing to the problem described in the social psychology by prof. Irving Janis i.e. groupthink syndrome (GTS). It is defined as (…) *an irrational pattern of thinking and behaving in a group, which imposes an artificial consensus and suppresses any dissenting voices*[18]. It means that decision-makers (politicians or military commanders) as members of a bigger group may yield to it and – being afraid of exclusion – they may willingly limit their intellectual scope for adequate situation assessment. Some of the GTS examples – mentioned by I. Jenkins in the article *Groupthink*, published in 1971 – are wrong decisions made by the Americans, including lack of proper preparation for the Japanese attack on Pearl Harbor, the failed Bay of Pigs invasion and the decision to increase American involvement in the Vietnam War[19].

[17] J. Konieczny, *Analiza informacji w dziedzinie*…, p. 248.

[18] K. Albrecht, *Inteligencja praktyczna. Sztuka i nauka zdrowego rozsądku*, Gliwice 2009, p. 217.

[19] I. Janis, *Groupthink*, "Psychology Today" 1971, no. 6, pp. 43–46, 74–76.

Mistakes may also appear at the stage of preparing analytical material for the final recipient. Among the most frequent of them are[20]:

- the conviction that the amount of material necessary to create the analytical product for the external receiver is sufficient and lack of interest to use the incoming information which affects the assessment of the threat (this behavior may result from an analyst's laziness, who already has his draft document prepared and accepted and new data radically changes the adopted assumptions, which entails further work on the same document);
- lack of proper verification of the information supplied by the source. False news may distort the picture of reality which may lead to politicians making wrong decisions;
- writing according to the expectations of the addressees or supervisors (e.g. people responsible for processing data fearing for their career may present in the analyses the assessments and theses compatible with the way the management of their institution see the world);
- delay in material transfer (lack of information at the appropriate time hinders making the right decision).

Methods of collecting information

A data analysis is preceded by the process of obtaining this information. In the publications on the subject a great number of methods of gathering information on national security are mentioned. Currently, one can point to at least a few of them. Among the most popular ones one should point to:

- **OSINT** (Open Source Intelligence) called also *white intelligence* in Polish – collecting information from overt sources i.e. traditional and electronic media, social media (e.g. Facebook), official state registers, public administration documents made available to the public, lectures, science conferences and materials which can be accessed without special permits or skills. In the recent years OSINT has become an invaluable source of knowledge as a result of the progressive phenomenon of digitalisation, ever greater internet access and human willingness to share a broad spectrum of private information using social media.
- **HUMINT** (Human Intelligence) is obtaining knowledge from so-called personal sources of information. HUMINT should be understood as classic intelligence activities. Mostly, state institutions (e.g. secret services) authorized to conduct intelligence operational activity attempt to come into possession of materials from people having information of essential importance for internal or external security of the state, its constitutional order, the position of the state

[20] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji*…, pp. 112–115.

on the international stage as well as its military and economic potential. Secret service officers use a broad spectrum of tools to initiate a contact and later to recruit. In the publications on the subject it is pointed to different kinds of motivation of the people who agree to cooperate with security institutions. The most popular theory makes reference to the acronym **MICE** (i.e. Money, Ideology, Coercion, Ego). According to its assumptions people pass information to the services due to, e.g. money received in return, opinions held by this person, fear of being discredited;

- **SIGINT** (Signals Intelligence)[21] which includes: **COMINT** (*Communication Intelligence* – communication information which comes from phone calls, conversations held on radio and other means of communication), **ELINT** (*Electronic Intelligence* – data coming from analysing electromagnetic signals, not used in telecommunication) and **TELLINT** (*Telemetry Intelligence* – technical and intelligence information coming from the gathered and processed light signals or foreign telemetry). In conclusion, SIGINT involves obtaining information by means of radars, phone tapping, directional microphones, and – possibly first of all – the control of the information flow on the internet. Currently, when one takes into account many users' low awareness of ensuring security of their action in the cyberspace, the materials originated in such a way become incredibly precious not only for hackers or criminal groups but also for state services which in a covert way and under the applicable law should obtain any knowledge of interest to them. At the same time, because of a large amount of information sent via telecommunication networks, gathering and analysing it requires specialist skills or computer software which support the processing of the gathered materials.
- **IMINT** (Imagery Intelligence) which is designated in the literature as **PHOTINT** (Photo Intelligence)[22] – obtaining knowledge, e.g. from photographs taken by satellites equipped with high-quality cameras or by officers during surveillance of people or installations. Information obtained in this way allows… to indicate or confirm undesired environmental changes (e.g. movement of enemy troops, new constructions developed for military use);
- **MASINT** (Measurement and Signatures Intelligence) – scientific and technical intelligence received by quality and quantity data analysis (metric, angular, spatial, wavelength, time relationships, modulation, hydromagnetic) coming from specialized technical sensors[23].

[21] Own translation based on: *Global National Security and Intelligence Agencies Handbook*, Washington 2015, p. 279.

[22] Ibidem.

[23] K. Liedel, P. Piasecka, T.R. Aleksandrowicz, *Analiza informacji…*, p. 59.

Types of analysis and analytical techniques

Another stage of the intelligence cycle is the analysis of the knowledge gathered according to the request of the politicians holding managerial positions in the state. One can point to at least two main **types of analysis** constituting support in the decision-making process. These are:

- **strategic analysis** – understood as comprehensive diagnosis of the past and present events, which enables us to prepare a forecast of security threats in the wide sense of the term as well as conclusions and recommendations. They enable the recipients of such material to make a decision bringing long-term effects;
- **signal analysis** – prepared on the basis of the services' current work. Usually it takes the form of one or two paragraph long so-called information cube. In the material consisting of one paragraph only (its form resembles press release) one can find answers to the most basic questions (who? what? where? when?). In case of analyses of two paragraphs short conclusions and possible recommendations are included additionally.

Analytical techniques used in the course of preparing documents essential to the national security are a separate issue. The more interesting of them are:

- **high impact and low probability analyses.** Their authors describe events which may imply serious consequences for the national security but the probability of their occurrence is not large. Important elements of such a study are: diagnosis how an undesired situation may occur and indicators (so-called red flags) warning against approaching danger;
- **future occurrence scenario analyses.** On the basis of the gathered information, own experience and knowledge of typical cases analysts prepare the event forecast in the short, medium and long term. Usually, this kind of analysis consists of three possible versions (scenarios); an optimistic one (the most beneficial for the state), a pessimistic one (negative) and the most probable one;
- **"red hat" analyses.** Their aim is to recreate opponent's pattern of thinking (people, terrorist organizations) and to predict – including all variables – their possible decisions in the future (including potential decisions, e. g. undermining the national security).

Collecting and processing information by selected state institutions

In the Polish security system numerous state institutions function which prepare analytical products for decision makers. The scope of the information which is necessary to prepare analyses passed to and processed by particular entities is varied

and results from their statutory competence. Civilian secret services gather different kinds of information than military ones and law enforcement organs gather still others.

Polish counterintelligence and intelligence – acting under, and within the limits of the law – are responsible respectively for (…) *acquiring, analysing, processing and forwarding to appropriate authorities information which may be vital to the protection of internal security of the state and its constitutional order*[24] (Internal Security Agency, Polish acronym: ABW) and for (…) *acquiring, analysing, processing and forwarding to appropriate organs the information that may be vital to the security and international position of the Republic of Poland and its economic and defensive potential*[25] (Intelligence Agency, Polish acronym: AW). At the same time, the Heads of the ABW and AW are obliged to pass, without delay, to the President of the Republic of Poland and to the Prime Minister the information which may be vital to the security and international position of the Republic of Poland. Furthermore, unless the Prime Minister decides otherwise the Heads of the ABW and AW pass the information to constitutional ministers in accordance with their competence[26].

At the stage of gathering information officers use the powers defined in chapter 4 of the *Internal Security Agency and Foreign Intelligence Agency Act of 24 May 2002*. Among these powers, there are:

- intelligence control (including obtaining and recording the contents of telephone conversations by applying technical measures, also transmitted via telecommunication networks as well as the vision and sound of people from rooms, means of transport or space other than public)[27];
- covert cooperation with persons not being secret service officers[28];
- assistance of organs of government administration which are obliged to pass to ABW or AW information vital to the external security and international position of the Republic of Poland[29].

Processing the gathered information takes place in the specialized organizational units of particular services. There is no possibility to determine their detailed scope of competence on the basis of open sources of information, since these issues are regulated by regulations on classified information. A change to the organizational structure of the Internal Security Agency testifies to the growing significance of data analysis. In November 2018 *Ordinance no. 163 of the Prime Minister of 26 September 2018 on granting the Statute of the Internal Security Agency*[30] came into force. In ccordance

[24] *Act of 24 May 2002 on the Internal Security Agency and the Intelligence Agency* (i.e. Journal of Laws of 2016, item 1897, as amended), art 5.

[25] Ibidem, art. 6.

[26] Ibidem, art. 18.

[27] Ibidem, art. 27.

[28] Ibidem, art. 36.

[29] Ibidem, art. 41.

[30] M.P. of 2018, item 927.

with its provisions a new Department of Information, Analysis and Prognosis was separated from, as one can presume, Registry and Analysis Bureau (called also Bureau E). Currently, most probably its officers are responsible for preparing analytical products in the Internal Security Agency[31]. Moreover, one can conclude that – drawing on the interview with Gen. Adam Rapacki conducted by Krzysztof Liedel – terrorist threat analysis may be, to some extent, performed by the Counterterrorism Centre which was set up pursuant to the *Ordinance no. 102 of the Prime Minister of 17 September 2008 amending the Ordinance on granting the Statute of the Internal Security Agency* (act. repealed – note ed.). Gen. Rapacki indicated that (…) *apart from processing information of operational character the Centre prepares analyses on particular issues in order to render the knowledge distributed form the Centre uniform for all entities*[32]. In case of the Intelligence Agency even such deliberations were impossible until recently, since the statute of this institution did not reveal which organizational unit was responsible for data analysis (almost all of them bearing name: bureau)[33]. In this respect a change also took place in 2018. Pursuant to the *Ordinance no. 106 of the Prime Minister of 3 July 2018 amending the Ordinance on granting the Statute of the Intelligence Agency*[34] a new unit was created – the Department of Information, which – just like in the case of ABW – presumably prepares analytical work for the authorities of the RP[35].

Another scope of information is obtained and processed by military secret services. The Military Counterintelligence Service (Polish acronym: SKW) is obliged to (…) *acquire, gather, analyse, process and transfer information meaningful for the national defence, security or combat capacity of the Armed Forces of RP or other organizational units of the Ministry of National Defence*[36]. Whereas, the Military Intelligence Service (Polish acronym: SWW) acquires, gathers, analyses, processes and transfers to competent authorities information meaningful for the defence potential of the Republic of Poland, security and combat capacity of the Armed Forces of RP as well as the conditions of fulfilment of tasks outside the country by the Armed Forces of RP. This service also identifies and analyses threats which may affect the defence potential, appearing e.g. in conflict regions[37]. The Heads of SKW and SWW pass the gathered and processed information – after notifying the Minister of National

[31] Ibidem, § 3

[32] K. Liedel, *Zwalczanie terroryzmu międzynarodowego w polskiej polityce bezpieczeństwa,* Warszawa 2010, p. 132.

[33] *Announcement of the Prime Minister of 14 September 2016 on the publication of a uniform text of Ordinance of the Prime Minister on granting the Statute of the Foreign Intelligence Agency* (i.e. M.P. of 2016, item 936), § 3.

[34] M.P. of 2018, item 660.

[35] Ibidem, § 1.

[36] *Act of 9 June 2006 on the Military Counterintelligence Service and the Military Intelligence Service* (i.e. Journal of Laws of 2016, item 2138, as amended).

[37] Ibidem, art. 6.

Defence – without delay to the President of RP and the Chairman of the Council of Ministers. Moreover, if the information relates to the scope of activity of a competent minister they pass the information to this minister, unless the Chairman of the Council of Ministers decides otherwise[38].

At the stage of gathering information the SKW and SWW officers have the power to conduct activities defined in Chapter 3 of the *Military Counterintelligence Service and Military Intelligence Service Act of 9 June 2006*. In numerous cases they are in line with the ones prescribed for ABW and AW (e.g. intelligence control or covert cooperation with persons not being secret service officers). At the same time, it is difficult to determine which organizational units inside SKW and SWW are accountable for data analysis since their structure remains secret. (the legislator using terms like: department, board, bureau[39]).

The Central Anti-Corruption Bureau (Polish acronym: CBA), created in 2006 (…) *as a secret service to combat corruption in public and economic life, particularly in public and local government institutions as well as to fight against activities detrimental to the state's economic interests*[40], was obliged (…) *to conduct analytical activities concerning phenomena falling within the CBA's competence as well as presenting information within this scope to the Chairman of the Council of Ministers, the President of the Republic of Poland, the Sejm and the Senate*[41].

At the stage of gathering information CBA officers use the powers defined in chapter 3 of the *Act of 9 June 2006 on the Central Anti-Corruption Bureau*. In case of CBA they are also often in line with the ones prescribed for ABW, AW, SKW or SWW (e.g. intelligence control, covert cooperation with persons not being secret service officers). At the same time, presumably the Analysis Department is responsible for processing and analysing information acquired as a result of intelligence operational activities[42].

The Police and the Border Guard (Polish acronym: SG) which are supervised by the Minister of Interior and Administration, while conducting their statutory tasks also acquire intelligence information. Therefore, the Police processes data related to (…) *protection of public safety and order, including ensuring peace in public places and in public means of transport, road traffic and on waters allocated for common use*[43]. Whereas the Border Guard (…) *gathers and processes information concerning*

---

[38] Ibidem, art. 19.

[39] *Ordinance of the Minister of National Defence of 21 April 2017 on granting the Statute of the Military Counterintelligence Service (M.P. of 2017, item 431) and Ordinance of the Minister of National Defence of 13 June 2018 amending the Ordinance on granting the Statute of the Military Intelligence Service* (M.P. of 2018, item 694).

[40] *Act of 9 June 2006 on the Central Anti-Corruption Bureau* (Journal of Laws of 2016, item 1310, as amended), art. 1.

[41] Ibidem, art. 2.

[42] *Ordinance no. 72 of the Prime Minister of 6 October 2010 on granting the Statute of the Central Anti-Corruption Bureau* (M.P. of 2010 no. 76, item 953), § 3.

[43] Act of 6 April 1990 on the Police (Journal of Laws of 2016, item 1782, as amended), § 1.

the protection of the national border, border traffic control, preventing and counteracting illegal migration[44]. The process of data analysis and its transfer to decision makers occurs in the organizational units of particular services inside, respectively, the General Police Headquarters (Polish acronym: KGP) and the General Border Guard Headquarters (Polish acronym: KG SG). Inside KGP there exists, e.g.:

- The Cabinet of the Police Commander in Chief (Polish name: Gabinet Komendanta Głównego Policji), its tasks being (…) *coordinating the preparation of materials for the meetings of parliamentary committees and sub-committees and the participation of the Police Commander in Chief and his deputies in such meetings, preparing analyses on the operation of the Police in case of spontaneously arising needs of the KGP management*[45];
- The Chief Police Staff (Polish name: Główny Sztab Policji), its task being (…) *managing updated information on the state of security and order (...), including gathering and analysing data on current events and threats on the territory of the country as well as undertaking measures to prevent and eliminate them*[46].

Whereas, in the KG SG there exists:

- The Board for Foreigners (Polish name: Zarząd do spraw Cudzoziemców), its tasks being (…) *preparing cyclical and periodic analyses and materials, in particular on foreigners returning from the territory of RP*[47];
- The Analysis and Information Bureau (Polish name: Biuro Analityczno-Informacyjne) which is responsible for, inter alia, (…) *providing the Border Guard Commander in Chief and his deputies with assistance in the decision making process, in particular by preparing and supplying information and analyses of strategic importance for the operation of the Border Guard*[48].

It is enough to mention the scope of competence of only a few institutions to show haw many entities deal with data analysis. The materials obtained by these entities and their area of competence – despite varied tasks – often overlap. Therefore, the legislator in 2007 made an attempt to streamline the national security system with regard to data flow between its particular components. *The Act of 26 April 2007 on Crisis Management*[49] established the Government Centre for Security (Polish

[44] *Act of 12 October 1990 on the Border Guard* (Journal of Laws of 2016, item 1643, as amended), § 1.

[45] http://www.policja.pl/pol/kgp/gabinet-komendanta-glo/ [access: 3 IX 2019].

[46] http://www.policja.pl/pol/kgp/glowny-sztab-policji [access: 3 IX 2019].

[47] http://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/zarzad-do-spraw-cudzozi/1909,Zarzad-do-Spraw-Cudzoziemcow-Komendy-Glownej-Strazy-Granicznej.html [access: 3 IX 2019].

[48] https://strazgraniczna.pl/pl/straz-graniczna/struktura-sg/komenda-glowna-sg/komorki-organizacyjne-k/biuro-analityczno-sytua/7895,Biuro-Analityczno-Sytuacyjne.html [access: 9 XII 2019].

[49] I. e. Journal of Laws o 2019, item 1398, as amended.

acronym: RCB) – a structure which coordinates the information flow and serves as a National Centre for Crisis Management. The primary tasks of RCB are: (...) *analysis and assessment of possible occurrence and development of threats, collection of information on threats and conduction of analysis of collected materials, development of conclusions and recommendations on preventing and counteracting the threats*[50]. The emergence of a separate organizational unit in the structure of RCB testifies to the role and significance of information in this institution, i.e. the Analysis and Response Bureau, which in turn includes e.g. the Operational-Analytical Centre. The tasks of this centre are: *monitoring and analysing the situation and level of the national security as well as the occurrence of threats in this respect; compiling accounts, reports, assessments: – of the activities conducted by the Centre in crisis situations – of the tasks entrusted by the Council of Ministers or the Chairman of the Council of Ministers, of the activities in crisis situations conducted by public administration organs competent in the matters of crisis management*[51].

Conclusions

The author of this work is aware that the subject has not been exhausted. His intention was merely to signal some interesting aspects of analytical work and current system solutions in the field of creating analytical products for the authorities of RP, supporting the decision making process in the area of national security. One can reach certain conclusions based on the consideration so far and bearing in mind that a full presentation of the problem would require a multi-page elaboration:

1. With regard to a large amount of information appearing daily (potentially vital to the life, health and property of Polish citizens, constitutional order or international position of RP) the role and significance of data analysis will increase. Therefore, the labour market will seek specialists who are able to prioritize threats and describe synthetically undesired phenomena.
2. Another challenge, resulting from increasing amounts of data, is creating new tools and ongoing improving the existing ones, including computer software assisting analysts in efficient processing and organizing the collected knowledge.
3. In Poland numerous entities are responsible for preparing analyses on potential threats to the national security. Frequently, these entities have similar competence and therefore unnecessary duplication of efforts in the area of identifying, gathering and processing information may take place. For this reason, constant and enhanced cooperation between them seems essential, including exchange of information to achieve synergy effect.

[50] *Act of 26 April 2007 on Crisis Management* (i.e. Journal of Laws of 2017, item 209), art. 11.

[51] http:// https://rcb.gov.pl/centrum-operacyjno-analityczne-2/ [access: 3 IX 2019].

4. It is worth starting a discussion on reforming the security system, including creating one, central body or transforming the existing one (e.g. the Government Centre for Security), which would deal with analysing information passed from secret services and offices. Subsequently, its task would be preparing one comprehensive material on a daily basis, whose recipients would be the most important persons in the state. This conclusion seems justified if one takes into account the postulates expressed by the former Head of The Military Counterintelligence Service Andrzej Kowalski (in 2013 he indicated the necessity of establishing the Centre of Strategic Analyses at the Minister Coordinator of Secret Services[52]), the authors of *White Book on National Security of the Republic of Poland*[53] (Polish name: *Biała Księga Bezieczeństwa Narodowego*) or other experts dealing with the question of security (e.g. Casimir Pulaski Foundation[54]).

Abstract

The article presents the issue of data analysis and its role in the process of ensuring national security. In the first part, the theoretical aspects of processing messages essential from the point of view of decision makers were highlighted, including definition issues, means of collecting information as well as types of data analysis. Moreover, in the further part of the publication the emphasis was put on the multiplicity of bodies responsible for providing analyses to politicians holding managerial positions in the country. In the conclusions, it was postulated to enhance cooperation as far as data flow between particular components of the national security system is concerned and establishing a new institution responsible for coordination and preparing joint analytical products, e.g. for the President of RP and the Chairman of the Council of Ministers.

Keywords: analysis, data, national security, intelligence services, decision making process.

[52] *Plan zmian w służbach opracowywany od kilku lat*, http://niezalezna.pl/73124-plan-zmian-w-sluzbach-opracowywany-od-kilku-lat-znamy-szczegoly-wideo [dostęp: 13 V 2017].

[53] The authors of the document signalled the necessity to build '(…) a unit (bureau, centre, department etc.) responsible for conducting strategic syntheses of information supplied by secret services and developing integrated assessments according to the needs of managing national security. Its task would be collecting information from all services responsible for particular areas of security and subsequently analysing and assessing the information for the needs of the supreme state management institutions'. CF *Biała Księga Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej*, Warszawa 2013, p. 210.

[54] G. Małecki, *Reforma służb specjalnych z perspektywy 15 lat*, https://pulaski.pl/wp-content/uploads/2015/02/Raport_reforma_sluzb__FKP.pdf [dostęp: 13 V 2017].

O autorach

Monika G. Bartoszewicz – doktor, Uniwersytet Masaryka (Brno, Republika Czeska).

Robert Borkowski – doktor habilitowany, profesor nadzwyczajny Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego. Członek rady naukowej Centrum Badań nad Terroryzmem.

Paweł Gacek – doktor nauk prawnych, funkcjonariusz Komendy Miejskiej Policji w Krakowie.

Dariusz Gradzi – adwokat, kancelaria adwokacka AKGK Adwokaci Kostański Gradzi Kuczara s.c.

Krzysztof Horosiewicz – doktor, Uniwersytet Humanistyczno-Przyrodniczy im. Jana Długosza w Częstochowie.

Krzysztof Izak – emerytowany funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.

Bartosz Jagodziński – pracownik Dolnośląskiego Urzędu Celno-Skarbowego we Wrocławiu.

Maciej A. Kędzierski – doktor nauk prawnych, radca prawny, emerytowany funkcjonariusz Policji.

Paweł Łabuz – doktor, Wyższa Szkoła Ekonomii, Prawa i Nauk Medycznych im. prof. Edwarda Lipińskiego w Kielcach.

Kamil Nowak – doktor, Agencja Bezpieczeństwa Wewnętrznego.

Tomasz Safjański – doktor, członek rady naukowej Centrum Profilaktyki Społecznej w Milanówku.

Leszek Wiszniewski – Agencja Bezpieczeństwa Wewnętrznego.

About authors

Monika G. Bartoszewicz – PhD, Masaryk University (Brno, Czech Republic).

Robert Borkowski – PhD with post-doctoral degree, associated profesor at Andrzej Frycz Modrzewski Krakow University. Member of the academic council at the Terrorism Research Center.

Paweł Gacek – PhD in legal science, officer of the Local Police Department in Cracow.

Dariusz Gradzi – attorney, AKGK Adwokaci Kostański Gradzi Kuczara law firm.

Krzysztof Horosiewicz – PhD, Jan Długosz University in Częstochowa.

Krzysztof Izak – retired officer of the Internal Security Agency.

Bartosz Jagodziński – employee of the Lower Silesia Tax and Customs Office in Wrocław.

Maciej A. Kędzierski – PhD in legal science, attorney-at-law, retired Police officer.

Paweł Łabuz – PhD, Professor Edward Lipiński School of Economics, Law and Medical Sciences in Kielce.

Kamil Nowak – PhD, Internal Security Agency.

Tomasz Safjański – PhD, member of the academic council at the Social Prevention Centre in Milanówek.

Leszek Wiszniewski – Internal Security Agency.

Informacje dla autorów
czasopisma „Przegląd Bezpieczeństwa Wewnętrznego”
i serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego

I. Zasady przyjmowania prac.

1. Redakcja „Przeglądu Bezpieczeństwa Wewnętrznego” przyjmuje tylko materiały oryginalne (wcześniej niepublikowane).
2. Materiały należy przesyłać na adres redakcji: redakcja.pbw@abw.gov.pl.
3. Materiały kierowane do druku w czasopiśmie „Przegląd Bezpieczeństwa Wewnętrznego” i w ramach serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego podlegają ocenie merytorycznej członków Redakcji i co najmniej dwóch recenzentów zewnętrznych.
4. Recenzje zewnętrzne mają formę pisemną i kończą się jednoznacznym wnioskiem o dopuszczeniu artykułu do publikacji (bez zmian lub po wprowadzeniu przez autora zmian sugerowanych przez recenzentów) lub jego odrzuceniu.
5. W przypadku dwóch recenzji sprzecznych Redakcja przesyła artykuł do kolejnego recenzenta. Po analizie wszystkich recenzji Redakcja podejmuje decyzję o zamieszczeniu lub niezamieszczaniu artykułu.
6. Do publikacji są kwalifikowane artykuły, które uzyskały pozytywną opinię końcową.
7. Po zakwalifikowaniu artykułu do publikacji autor lub autorzy podpisują umowę o przeniesieniu na wydawcę autorskich praw majątkowych.
8. Autorzy artykułów zakwalifikowanych do druku otrzymują honoraria w wysokości 30 zł brutto za jedną stronę tekstu, sformatowanego zgodnie z *Informacjami dla autorów czasopisma „Przegląd Bezpieczeństwa Wewnętrznego” i serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego*, znajdującymi się w każdym drukowanym numerze „Przeglądu…” oraz na oficjalnej stronie internetowej Agencji w zakładce „PBW”.
9. W przypadku utworu stworzonego przez kilka osób każda z nich jest zobowiązana 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.
10. Autorzy są zobowiązani do wypełnienia formularzy zgody na publikację materiałów przez Redakcję „Przeglądu Bezpieczeństwa Wewnętrznego” (*Formularz zgody autora na publikację artykułu w czasopiśmie „Przegląd Bezpieczeństwa Wewnętrznego* oraz *Formularz zgody autora na publikację tekstu w ramach*

serii Biblioteka Przeglądu Bezpieczeństwa Wewnętrznego są dostępne na stronie Agencji Bezpieczeństwa Wewnętrznego) i przesłania ich na adres Redakcji PBW podany w pkt I ppkt 2.

II. Zasady przesyłania tekstów.

1. Wszystkie teksty należy przesyłać w postaci zapisu elektronicznego (Word, Open Office).
2. Do artykułu należy dołączyć:
   a) bibliografię załącznikową,
   b) abstrakty w języku polskim i angielskim 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).

III. Normalizacja tekstu.

1. Marginesy: 2,5 cm z każdej strony.
2. Czcionka tekstu głównego: Times New Roman 12 pkt; interlinia 1,0.
3. Czcionka przypisów: Times New Roman 10 pkt; interlinia 1,0.
4. Objętość artykułu zgłaszanego do publikacji (wraz z bibliografią, abstraktami i słowami kluczowymi) nie może przekraczać 15 stron wydruku komputerowego w formacie A4, sprawozdania z konferencji – 3 stron, recenzji – 10 stron.
5. Tekst powinien być wyjustowany.
6. Tytuł, podtytuł i śródtytuły: Times New Roman, bold
7. Rysunki i fotografie należy lokalizować w tekście głównym za pomocą podpisów.
8. 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.
9. Należy podać źródła wszystkich materiałów ilustracyjnych (zdjęć, rysunków, wykresów, schematów, tabel itp.).
10. Na końcu podpisu pod materiałem ilustracyjnym należy stawiać kropkę.

11. Nie należy stosować tzw. twardych spacji.
12. Ortografię i interpunkcję tekstu należy uwspółcześniać.
13. Wszelkie wyróżnienia w oryginalnym tekście dokumentu, dokonane przez jego twórcę, powinny być wyróżnione wytłuszczoną czcionką.
14. Nawiasy ukośne /…/ powinny być zamieniane na nawiasy półokrągłe (…).
15. Uzupełnienia i komentarze odautorskie itp. należy podawać w nawiasach kwadratowych, drukiem prostym.
16. Opuszczenia w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie półokrągłym.

IV. Cytaty i wyróżniki.

1. Cytaty o długości do pięciu wersów należy zapisywać kursywą, dłuższe należy wyróżniać przez wcięcie (1,0 cm z lewej i prawej strony, licząc od granic tekstu głównego) oraz odstęp dwóch wersów nad i pod przytoczeniem, druk prosty, czcionka o jeden stopień mniejsza niż w tekście głównym.
2. Listy przytaczane w całości należy wyróżniać przez odstęp 2 wersów nad i pod przytoczeniem (nie należy stosować wcięcia ani kursywy).
3. Cytaty obcojęzyczne powinny być przetłumaczone w przypisie (tłumaczy autor tekstu).
4. Wtrącone zwroty obcojęzyczne piszemy kursywą (np. à *rebours*, *sui generis*).
5. Tytuły dzieł sztuki (plastycznych, muzycznych, dramatycznych, filmowych), książek, artykułów, obrazów, konkursów, prac naukowych, nazw ustaw oraz innych aktów prawnych należy zapisywać kursywą, nazwy czasopism – w cudzysłowie. Zgodnie z uchwałą RJP z 2008 r. wszystkie wyrazy w tytułach czasopism, poza spójnikami i przyimkami występującymi wewnątrz tych tytułów, zapisuje się wielkimi literami).
6. W cudzysłowie należy zapisywać także: pseudonimy (np. kpr. „Smukły"), kryptonimy oraz nazwy instytucji występujące na końcu nazwy wielowyrazowej, często będącej rozwinięciem skrótowca (np. operacja „Market Garden", Związek Młodzieży Polskiej „Zet"); w nazwach jawnych organizacji politycznych nie stosuje się cudzysłowu (np. Polska Partia Socjalistyczna).
7. Cytaty ze źródeł i literatury przedmiotu należy wyróżniać kursywą bez cudzysłowu.
8. Nazwy wystaw, konferencji i sesji naukowych należy zapisywać pismem prostym w cudzysłowie.
9. Cudzysłów należy zapisywać za pomocą znaku drukarskiego „" – a nie innych podobnych znaków (‘’, „”).
10. Jeśli w obrębie jednego cudzysłowu występuje drugi cudzysłów, do jego wyodrębnienia należy stosować znak «».
11. Jeżeli w tekście zapisanym kursywą występuje element wyróżniany

kursywą (np. tytuł dzieła), należy go wyróżniać drukiem prostym (np. *Uwielbiała czytać książki, szczególnie często wracała do* Zbrodni i kary *oraz* Biesów).

12. Wyróżnienia odautorskie należy zapisywać rozstrzelonym drukiem (1,5 pkt), np. w y r ó ż n i e n i a o d a u t o r s k i e.
13. 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. 3 lipca 1969 r.).
14. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp., jeśli są wymieniane w tekście po raz pierwszy.
15. Obce nazwy organizacji oraz skróty od nich utworzone należy zapisywać pismem prostym.

V. Znaki interpunkcyjne i obce.

1. W zestawieniach (np. Austro-Węgry, Stronnictwo Demokratytczno-Narodowe, polsko-niemiecki) i w nazwiskach złożonych z dwóch członów (np. Jankowska-Cieślak) należy stosować dywiz; myślnika bez spacji należy używać w przypadku połączeń doraźnych, które odpowiadają nie jednemu obiektowi rzeczywistości pozajęzykowej, ale dwóm – najczęściej łączy się w ten sposób liczby (np. t. 1–2, w latach 2015–2020).
2. Obce nazwy miejsc i osób, podobnie jak inne słowa obce, należy zapisywać z użyciem liter i znaków obcych alfabetów (np. Národni divadlo, Tomáš Masaryk), chyba że stosuje się przyjętą w uzusie w przypadku niektórych słynnych postaci konwencję spolszczoną (np. Tomasz Masaryk, William Szekspir).

VI. Przypisy.

1. Znak przypisu należy umieszczać zawsze po słowie, nawiasie zamykającym lub po zamknięciu cudzysłowu, a przed znakiem interpunkcyjnym.
2. Przypisy należy rozpoczynać wielką literą, a kończyć kropką. Małą literą należy rozpoczynać jedynie przypisy dotyczące adresów stron internetowych (np. [1] https://www.abw.gov.pl/pl,[2] www.bip.abw.gov.pl).
3. Przypisy należy umieszczać na dole stron.
4. Przypisy we wstępie (posłowiu) oraz w tabelach mają numerację oddzielną od przypisów w źródłach.
5. W przypadku autorów podpisujących się dwojgiem imion należy podawać inicjały obu imion bez spacji między nimi (np. J.K. Bielecki).
6. Zawsze należy podawać podtytuł publikacji.

7. W przypisach konsekwentnie należy stosować następujące oznaczenia: tenże/taż, tamże, tłum., wstęp, posł., (red.), oprac., i in., t., cz., z., nr, [bmw] – brak miejsca wydania, [bdw] – brak daty wydania, [bmdw] – brak miejsca i daty wydania, zob., por., zob. szerzej: (z dwukropkiem), cyt. za: (z dwukropkiem), i nast.
8. Tomy, części, numery i zeszyty oraz numer wydania należy zapisywać cyframi arabskimi (np. t. 2, cz. 3, nr 4, z. 5, wyd. 2).
9. Miesiące należy zapisywać cyframi rzymskimi bez kropek rozdzielających dzień, miesiąc i rok (w tekście głównym nazwę miesiąca należy zapisywać słownie).
10. W przypisach należy podawać najpierw inicjał imienia oraz nazwisko autora (redaktora); w bibliografii załącznikowej (alfabetycznej) natomiast – nazwisko, a potem: inicjał imienia w przypadku głównego autora (głównych autorów publikacji) oraz dalej inicjały i nazwiska w przypadku kolejnych osób.

    PRZYKŁADY:

    Kowalski L., *Warszawa tamtych lat*, wstęp A. Nowak, Warszawa 2015, ABC Wydawnictwo Historyczne).

11. Należy skracać opis w przypisie (bibliografii) przez upraszczanie często skomplikowanych formuł dotyczących redakcji – do oznaczeń: oprac., red.
12. Gdy autorów (redaktorów, tłumaczy) jest więcej niż trzech, należy podać inicjał (inicjały) imienia i nazwisko alfabetycznie pierwszego z nich, dodając do niego skrót: i in. (i inni).
13. Strony należy zapisywać następująco: s. 2; s. 2, 7; s. 3–5 (myślnik, nie dywiz).
14. Jeśli w przypisach pojawił się więcej niż jeden tekst tego samego autora, to przy kolejnym przywołaniu konkretnego dzieła tego autora tytuł należy skracać do czytelnej postaci, dodając wielokropek i rezygnując z podawania ponownie miejsca i roku wydania.

    PRZYKŁAD:

    L. Wasilewski, *Ze wspomnień*…, s. 224–225).

15. Gdy podaje się przypis łączny dla kilku tomów lub części jakiejś publikacji, numery tomów należy zapisywać z myślnikiem, nie z dywizem. To samo dotyczy lat publikacji.

    PRZYKŁAD:

    K. Grodziska, *Polskie groby na cmentarzach Londynu*, t. 1–2, Kraków 1995–2001.

16. W przypadku dwóch lub trzech miejsc wydania (miejscowości), należy je zapisywać z myślnikami (np. Wrocław–Kraków), jeżeli jest ich więcej – należy podać tylko pierwsze z nich.
17. Jeśli imię zaczyna się dwuznakiem (np. Sz, Cz), należy zapisać tylko pierwsza literę; wyjątkiem jest Ch.

    PRZYKŁAD:

    C. Miłosz, *Druga przestrzeń*, Kraków 2002, Znak.
    Ch. Dickens, *Wielkie nadzieje*, tłum. K. Beylin, Warszawa 1999.

18. Cytaty w przypisach należy zapisywać pismem prostym w cudzysłowie.

VII. Struktura przypisów.

1. Przypis archiwalny:
   pełna nazwa archiwum (gdy pojawia się po raz pierwszy) i w nawiasie formułka „dalej:" oraz proponowany skrót tej nazwy do stosowania za każdym kolejnym razem, 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:

   Archiwum Instytutu Pamięci Narodowej, Oddziałowe Biuro Udostępniania i Archiwizacji Dokumentów w Krakowie (dalej: AIPN, OBUiAD w Krakowie), IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57.

   APK, UWSl. (skrót, gdy wcześniej pojawiła się pełna nazwa miejsca przechowywania źródła), sygn. 736, sprawozdanie z działalności Policji Województwa Śląskiego za 1928 r., 5 I 1929 r., k. 57.

2. Książka polska:
   inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), numer tomu, inicjał imienia i nazwisko autora wstępu, inicjał imienia i nazwisko autora posłowia, inicjał imienia i nazwisko autora opracowania, miejsce i rok wydania, strony.

   PRZYKŁAD:

   B. Prus, *Lalka*, t. 1, oprac. J. Bachórz, Wrocław 1998, s. 100–200.

3. Książka tłumaczona:
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), numer tomu, inicjał imienia i nazwisko tłumacza, inicjał imienia i nazwisko autora wstępu, inicjał imienia i nazwisko autora posłowia, inicjał imienia i nazwisko autora opracowania, miejsce i rok wydania, strony.

   PRZYKŁAD:

   Ch. Taylor, *Źródła podmiotowości. Narodziny tożsamości nowoczesnej*, tłum. M. Gruszczyński i in., wstęp A. Bielik-Robson, oprac. T. Gadacz, Warszawa 2001, s. 15–20.

4. Książka zagraniczna:
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), numer tomu, inicjał imienia i nazwisko tłumacza, inicjał imienia i nazwisko autora wstępu, inicjał imienia i nazwisko autora posłowia, inicjał imienia i nazwisko autora opracowania, miejsce i rok wydania, strony. Stosujemy zapis bibliograficzny polski, w tym obcobrzmiące nazwy miejsc wydania.

   PRZYKŁAD:

   P. Hadot, *The Veil of Isis. An Essay on the History of the Idea of Nature*, tłum. M. Chase, Cambridge–Massachussets–London 2006, s. 40–50.

5. Publikacja w pracy zbiorowej:
inicjał imienia i nazwisko autora, *tytuł publikacji zamieszczonej w pracy zbiorowej* (kursywą), w: inicjał imienia i nazwisko autora, *tytuł pracy* (kursywą), numer tomu, inicjał imienia i nazwisko redaktora, miejsce i rok wydania, strony.

   PRZYKŁAD:

   W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, s. 36.

6. Dzieło wielotomowe:
inicjał imienia i nazwisko autora, *tytuł* (kursywą). *Podtytuł* (kursywą), miejsce i rok wydania (np. 2007, jeśli wszystkie tomy zostały wydane w tym samym roku, lub 2000–2001, jeśli tomy zostały wydane w różnym czasie), 2 t. (dwa tomy; cyfry arabskie).

   PRZYKŁAD:

   B. Prus, *Lalka*, Warszawa 1985, 4 t.

7. Praca zbiorowa (dotyczy także antologii i opracowań):
tytuł. Podtytuł pracy zbiorowej (kursywą), inicjał imienia (lub pełne imię) i nazwisko redaktora (red.), miejsce i rok wydania.

   PRZYKŁAD:

   Historia Łodzi. Ze wspomnień mieszkańców, A. Kowalski (red.), Łódź 2001.

8. Artykuł w książce:
inicjał imienia i nazwisko autora, *tytuł* (kursywą), inicjał imienia i nazwisko tłumacza (jeśli części są tłumaczone przez różne osoby), w: *tytuł zbioru* (kursywą), numer tomu, część, inicjał imienia i nazwisko tłumacza całości, inicjał imienia i nazwisko redaktora (lub redaktorów), miejsce i rok wydania, strony.

   PRZYKŁADY:

   W. Szkłowski, *Sztuka jako chwyt*, tłum. R. Łużny, w: *Teoria badań literackich za granicą*, t. 2, cz. 3, S. Skwarczyńska (red.), Kraków 1984, s. 20–30.

   H. Trevor-Roper, *Góralskie tradycje Szkocji*, w: *Tradycja wynaleziona*, tłum. M. Godyń, F. Godyń, E. Hobsbawm, T. Ranger (red.), Kraków 2008, s. 40.

9. Artykuł w zbiorze tego samego autora:
inicjał imienia i nazwisko autora, *tytuł* (kursywą), w: tenże/taż, *tytuł zbioru* (kursywą), numer tomu, inicjał imienia i nazwisko redaktora (redaktorów), inicjał imienia i nazwisko tłumacza, miejsce i rok wydania, strony.

   PRZYKŁAD:

   M. Janion, *Apokalipsa bez zbawienia. Tematy jeanpaulowskie*, w: taż, *Żyjąc, tracimy życie. Niepokojące tematy egzystencji*, Warszawa 2001, s. 15–20.

10. Artykuł w czasopiśmie:
inicjał imienia i nazwisko autora, *tytuł* (kursywą), inicjał imienia i nazwisko tłumacza, „Tytuł Czasopisma" rok (wszystkie człony tytułów czasopism, poza spójnikami i przyimkami występującymi wewnątrz tych tytułów, należy zapisywać wielkimi literami), numer w danym roku, zeszyt, numer, część (w opisie należy stosować cyfry arabskie), strony.

PRZYKŁAD:

W. Nowak, *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 13.

11. Artykuł w dzienniku:
inicjał imienia i nazwisko autora artykułu, *tytuł. Podtytuł artykułu w dzienniku*, „Tytuł Dziennika" i dalej data dzienna (nazwę miesiąca należy zapisywać słownie).

PRZYKŁAD:

Kowalski, *Energia wiatrowa. Nowe możliwości*, „Rzeczpospolita" z 2 marca 2020 r.

12. Tekst w czasopiśmie zagranicznym:
zapis jak w pkt 10; zawsze należy podawać rok ukazania się i numer czasopisma tylko w tym roku.

PRZYKŁAD:

C.M. Bowra, *Orpheus and Eurydice*, „Classical Quarterly" 1952, nr 3–4.

13. Wydawnictwa internetowe:
adresy internetowe należy zapisywać małymi literami (bez podkreśleń i hiperłączy), po przecinku w nawiasie kwadratowym należy podać informację odacie dostępu (w dacie miesiąc zapisuje się cyfrą rzymską).

PRZYKŁAD:

http://www.pbw.gov/abw/cat.html [dostęp: 1 XII 2011].

14. Artykuły lub dokumenty zamieszczone na stronach internetowych:
tytuł artykułu (*dokumentu*) – kursywą, adres internetowy, w nawiasie kwadratowym – informacja o dacie dostępu.

PRZYKŁAD:

EU NAVFOR Somalia – mission, http://www.eunavfor.eu/about-us/mission/ [dostęp: 20 VII 2014].

15. Nie należy stosować skrótów: op. cit., lok., cit.

VIII. Zapis nazwisk.

1. W tekście głównym nazwiska należy zapisywać następująco: za pierwszym razem pełne imię i nazwisko, później samo nazwisko (chyba że powtórzenie pełnego imienia jest uzasadnione względami stylistycznymi); poza adresami bibliograficznymi w przypisach i bibliografii nie należy stosować zapisu z inicjałem.

   PRZYKŁAD:

   Gabriel Narutowicz (lub Narutowicz; nie: G. Narutowicz) został prezydentem w 1922 r.

2. Jeśli dwie postaci noszą to samo nazwisko, w przypadku gdy nie jest oczywiste, o której z nich mowa, należy powtórzyć imię lub nazwać tę osobę za pomocą omówienia.

IX. Skróty.

1. W tekście głównym należy stosować ogólnie przyjęte skróty: np., itp., m.in. (bez spacji), rkps, mps, t., z. itd.), a także z reguły: r. (rok) i w. (wiek).
2. Należy przemyśleć zasadność wprowadzania skrótów nazw instytucji lub organizacji (zwłaszcza gdy będą stosowane rzadko), a szczególnie w przypadku wydawania źródła; wprowadzanie skrótu jest interwencją w język zapisu.
3. Należy wprowadzać jeden skrót dla jednej nazwy.
4. Skróty należy stosować konsekwentnie – jeśli skrót został wprowadzony, odtąd zastępuje w tekście daną nazwę za każdym razem, gdy się ona pojawia.
5. W skrótach nie należy stosować dywizów.

   PRZYKŁAD:

   Polska Partia Socjalno-Demokratyczna Galicji i Śląska = PPSD (nie: PPS-D).

X. Bibliografia załącznikowa

1. Przy sporządzaniu bibliografii załącznikowej kolejne pozycje należy szeregować w porządku alfabetycznym. Opis każdej pozycji należy rozpocząć od nazwiska autora, po nim należy podać inicjał imienia, postawić kropkę, przecinek, a następnie według schematu przypisu – tytuł zapisany kursywą itd. (w przypadku artykułu w czasopiśmie lub w pracy zbiorowej należy podać zakres stron).

PRZYKŁADY:

Kowalski W., *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2,

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, s. 542.

2. Akty prawne należy oddzielać od innych źródeł.
3. Akty prawne należy szeregować według hierarchii przyjętej dla tego typu dokumentów, tj. w porządku:

   A. Konstytucja
   B. Ratyfikowane umowy międzynarodowe.
   C. Rozporządzenia, dyrektywy i decyzje UE.
   D. Ustawy i rozporządzenia z mocą ustawy.
   E. Rozporządzenia.
   F. Akty prawa miejscowego.

Redakcja nie zwraca autorom nadesłanych prac, a także zastrzega sobie prawo do ich skracania, opracowania redakcyjnego, w tym adiustacji tekstów, oraz zmiany tytułów i śródtytułów.

Redakcja zastrzega sobie możliwość odmowy przyjęcia artykułu bez podania przyczyn.

Redakcja zwraca uwagę, że *ghostwriting** i *guest authorship*** są przejawami 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.

Redakcja informuje, że wszystkie artykuły zakwalifikowane do publikacji są weryfikowane z wykorzystaniem programu antyplagiatowego.

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.