Nr 8 (5) 2013

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

CENTRALNY OŚRODEK SZKOLENIA
im. gen. dyw. Stefana Roweckiego „GROTA”

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 8 (5) 2013

INTERNAL SECURITY REVIEW

WARSAW 8 (5) 2013

ISSN 2080-1335

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

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

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

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

Numer zamknięto i oddano do druku w maju 2013 r.

Skład i druk
Agencja Bezpieczeństwa Wewnętrznego
00-993 Warszawa, ul. Rakowiecka 2A
tel. (+48) 22 58 57 657

Spis treści

CONTENTS

Pamięci Krzysztofa Kozłowskiego – pierwszego szefa Urzędu Ochrony Państwa

śp. KRZYSZTOF KOZŁOWSKI
18 sierpnia 1931– 26 marca 2013

Doktor filozofii, dziennikarz. Podsekretarz stanu, a następnie minister spraw wewnętrznych w rządzie Tadeusza Mazowieckiego. Pierwszy szef Urzędu Ochrony Państwa. Senator RP I, II, III i IV kadencji. Przewodniczący Rady Konsultacyjnej przy Centralnym Ośrodku Szkolenia ABW w Emowie. Współfundator, założyciel oraz pierwszy przewodniczący Rady Fundacji Pomocy Rodzinom Funkcjonariuszy i Pracowników UOP i ABW.

Krzysztof Kozłowski urodził się w Przybysławicach. Jego rodzicami byli Tomasz Kozłowski i Jadwiga z domu Postępska. W latach 1950–1956 studiował filozofię na Katolickim Uniwersytecie Lubelskim. Obronił doktorat z filozofii, był wykładowcą nauk politycznych na KUL. Od 1956 r. związał się ze środowiskiem „Tygodnika Powszechnego" (w latach 1965–2007 pełnił funkcję zastępcy redaktora naczelnego). W latach 80. był doradcą Komisji Robotniczej Hutników w Nowej Hucie oraz ekspertem NSZZ „Solidarność". W 1989 r. uczestniczył w obradach Okrągłego Stołu jako członek zespołu ds. reform politycznych oraz podzespołu ds. środków masowego przekazu. W rządzie Tadeusza Mazowieckiego pełnił funkcje: wiceministra spraw wewnętrznych, szefa Urzędu Ochrony Państwa oraz ministra spraw wewnętrznych. W latach 1989–2001 sprawował mandat senatora RP I kadencji z ramienia Komitetu Obywatelskiego „Solidarność", II i III kadencji z listy Unii Demokratycznej oraz IV kadencji z listy Unii Wolności. W 2001 r. zrezygnował z działalności politycznej. Od 2008 r. był przewodniczącym Rady Konsultacyjnej przy Centralnym Ośrodku Szkolenia ABW w Emowie. W 2010 r. zaangażował się w powołanie Fundacji Pomocy Rodzinom Funkcjonariuszy i Pracowników UOP i ABW. Był pierwszym Przewodniczącym Rady Fundacji.

W 2011 r. został odznaczony Krzyżem Wielkim Orderu Odrodzenia Polski oraz Odznaką Honorową imienia gen. dyw. Stefana Roweckiego „Grota".

Krzysztof Kozłowski został pochowany 5 kwietnia 2013 r. na Cmentarzu Salwatorskim w Krakowie.

* * *

Wpływ Krzysztofa Kozłowskiego trwał dłużej niż czas jego urzędowania. Był też głębszy, bo dokonywał się własnym przykładem, czym powinny być służby specjalne w państwie demokratycznym, kompetentne, lecz poddane cywilnej kontroli. Doktor filozofii i intelektualista z Wiślnej i KUL-u polubił tę pracę i wykonujących ją ludzi. Szanował ich. W funkcjonariuszu podnosił człowieka. I za to sam był szanowany.
(fragment mowy pożegnalnej wygłoszonej przez Tadeusza Mazowieckiego)

Krzysztof Kozłowski

Rewolucja po polsku[1]

6 kwietnia – to święto Agencji Bezpieczeństwa Wewnętrznego. Dlaczego 6 kwietnia? Bo wtedy – 20 lat temu – nastąpiło uchwalenie pakietu tzw. ustaw policyjnych. Dlaczego ten dzień jest i powinien być świętem? Bo była rewolucja, ale najważniejsze było to, że uchwalono ustawy. W tradycji polskiej jest zakorzenione to, że wywołujemy rewolucję przy pomocy ustaw. Tak było z Konstytucją 3 Maja i oby tak było w przyszłości. Jeżeli myślę o rewolucji, to chyba nie przesadzam.

Jeżeli w ciągu kilku miesięcy zmienił się ustrój polityczny, gospodarczy, społeczny i sytuacja międzynarodowa naszego kraju, jeżeli zmieniły się jego parametry, to tego rodzaju zmiany, tak szybkie i gwałtowne, nazywamy rewolucją (nawet jeśli nie było ofiar ani żadnej wybitej szyby). Wywołanie tego typu rewolucji jest godne polecenia.

20 lat temu z kalendarza sejmowego wynikało, że właśnie 6 kwietnia miał być uchwalony pakiet ustaw. Daty zawsze są rzeczą umowną, natomiast ważne są procesy. Rewolucja też jest pewnym procesem, nawet, gdy trwa miesiące, a nie lata. Taką umowną datą jest też przecież 11 listopada. 11 listopada 1918 roku nikt nie zdawał sobie sprawy, że jest to wielki dzień. Po prostu była zła komunikacja między ludźmi. Ten dzień jako rocznica odzyskania niepodległości został wyznaczony dużo później. Chcemy mieć takie dni, ważne i określone. 6 kwietnia jest dobrym dniem do obchodzenia święta ABW, bo rzeczywiście przyjęcie ustaw policyjnych w przypadku służb specjalnych miało kolosalne znaczenie.

Jak należy przeprowadzać rewolucję? Po polsku, a więc nie w sposób barbarzyński. Rewolucję należy robić spokojnie, ale stanowczo, i nie oglądać się na tych, którzy próbują przyspieszać, ani na tych, którzy panikują. Przeprowadzenie rewolucji wymaga odwagi. Ci, którzy 20 lat temu podjęli się ją przeprowadzić, wykazali odwagę. Jeżeli mówię, że nie należy panikować, to dlatego że przeciwnik, przeciwko któremu rewolucja jest skierowana, zwykle okazuje się zbyt pewny siebie i to go gubi. W sierpniu 1989 roku, w momencie, kiedy Tadeusz Mazowiecki został wyznaczony na premiera (ale nowy rząd się jeszcze nie ukonstytuował), na odprawie kierowniczej resortu spraw wewnętrznych ówcześni wiceministrowie na polecenie szefa tego resortu przekonywali, że nic się nie dzieje. *To jest zagranie taktyczne. No, tak wypada teraz grać, ale dopóki resorty siłowe są w naszych rękach, socjalizm w Polsce jest niezagrożony*, twierdzili. W grudniu tegoż roku podczas jednej z konferencji szefowie resortu mówili: *Tak, zmiany są konieczne. Zmieniliśmy nazwy departamentów, rozwiązaliśmy ZOMO i teraz będą ustawy, ale to my będziemy te ustawy redagować, bo one są w naszych rękach. Towarzysze, nie bójcie się, nikomu nic złego się nie stanie, a szefem nowej struktury, która zastąpi Służbę Bezpieczeństwa będzie* – podkreślano – *płk Karpacz* (ostatni szef Służby Bezpieczeństwa). Takie były nastroje w grudniu.

W kwietniu 1990 r. przy pomocy także ludzi z resortu powstały wspomniane ustawy. Z ogromną wdzięcznością i szacunkiem wspominam Panią doc. płk Orłowską,

[1] Tekst pochodzi z wydania specjalnego „Przeglądu Bezpieczeństwa Wewnętrznego", pt. *20-lecie UOP/ABW*, Warszawa 2010, COS ABW, s. 13–15.

która włożyła ogromny wkład w ich stworzenie. Ale były one pisane i redagowane przez osoby, które wkrótce potem objęły stanowiska wiceministrów, tj. Jana Widackiego i Jerzego Zimowskiego. Zimowski był szefem podkomisji sejmowej, która je opracowywała, a Widacki głównym ekspertem od strony prawnej. Zadufanie poprzedników zemściło się na nich. Nastąpiło pęknięcie i rozsypywanie się czegoś, co wydawało się niewzruszalnym monolitem. Gdy w marcu 1990 roku przyszedłem, nie posiadając żadnej władzy, jako podsekretarz stanu do MSW (cóż, podsekretarz stanu o niczym tak naprawdę nie decyduje), tych trzydziestu kilku generałów, z którymi się zetknąłem, reprezentowało pogląd, że nie mają sobie nic do zarzucenia i nie zamierzają ani ustąpić, ani odejść, tylko wiernie służyć dalej. Ustawy, powołujące do życia między innymi Urząd Ochrony Państwa, zmieniły ich nastawienie. Gmach MSW przy ulicy Rakowieckiej zaczął pękać. Jeden po drugim spływały setki, a potem tysiące raportów o odejście ze służby. W maju 1990 r. spłynął ich ogrom, doprowadzając do tego, że cały proces weryfikacji dotyczył poruczników, kapitanów, majorów i tylko w niewielu przypadkach podpułkowników czy pułkowników. Cała kadra wyższych oficerów – tych trzydziestu kilku generałów, około 4 tysięcy podpułkowników i pułkowników – odeszła ze służby, zanim doszło do weryfikacji.

Ustawy uchwalone 6 kwietnia weszły w życie 10 maja 1990 r. Jak zaczynaliśmy? Premier Mazowiecki wręczył dwie nominacje. Urzędem Ochrony Państwa miał pokierować piszący te słowa i jego zastępca, Andrzej Milczanowski. Do organizacji tej instytucji zaangażowana była poza tym garstka młodych entuzjastów. Nie było automatycznego przejścia z poprzednich służb do UOP. Istniała możliwość zatrudnienia w nowych strukturach tylko tych, którzy pozytywnie przeszli weryfikacje. UOP mógł ich zatrudnić, bądź nie. Oczywiście, negatywnie zweryfikowani zostali z litery prawa poza resortem. Tak więc było nas dwóch, a podlegała nam formalnie nieokreślona ilość – bo odchodzili codziennie – byłych funkcjonariuszy byłej Służby Bezpieczeństwa. Od 10 maja struktura Służby Bezpieczeństwa już nie istniała, natomiast funkcjonariusze, którzy zdawali broń oraz dokumentację, podlegali mi jeszcze indywidualnie. Wówczas zaczęliśmy tworzyć coś, co dzisiaj przybrało formy służb specjalnych, z ABW na czele.

Czego należy się wystrzegać, przeprowadzając rewolucję po polsku? Przede wszystkim odwetu, takiej ludzkiej zwyczajnej zemsty. Bo odwet i zemsta nie tyle godzi w tych, na których chcemy się zemścić, ile w nas. Po prostu nas zżera. Nie należy wyżywać się na ludziach, chyba że są przestępcami. Ale to jest już inna sprawa i inna procedura. Przestępcy powinni być po prostu sądzeni. Rewolucja w strukturach służb to przede wszystkim stawianie nowych celów, podejmowanie nowych metod działania, wdrożenie innego sposobu reagowania. Ludziom, którzy nie są przestępcami, nawet jeśli wychowano ich i ukształtowano w innej rzeczywistości politycznej, należało – jestem o tym głęboko przekonany – dać szansę. Pokazać, że mają jedyną w życiu szansę wykonywania swojego zawodu w sposób uczciwy i profesjonalny. Jeśli będą służyć niepodległej, demokratycznej Rzeczpospolitej – Rzeczpospolita będzie im wdzięczna. Stąd do żywego dotykają mnie zawsze, szczególnie podejmowane po latach, wszelkie próby bezsensownego odwetu i karania ludzi za to, że służyli Trzeciej Rzeczpospolitej (…). Jest rzeczą istotną, aby pamiętać, że wszystko jest oparte na ludziach i że pomiatanie ludźmi jest najgorszą rzeczą, jaka może się komukolwiek przydarzyć.

Jak zatem przeprowadzić rewolucję, a potem rządzić? Zawsze uważałem, że na to jest dość prosta recepta. Każdy szef powinien dbać o to, żeby jego najbliżsi współpracownicy byli lepsi od niego. Wówczas będzie mógł spokojnie patrzeć w przyszłość. Trzeba dobierać ludzi możliwie najlepszych, nie bać się tego. Trzeba mieć komfort

posiadania pracowników, którzy w wielu sprawach i znają się, i radzą sobie lepiej niż my. I przede wszystkim, należy wyrywać służby – i to chyba na wstępnym etapie nam się udało, bo później, jak wiadomo, było rożnie – z objęć polityki i ideologii. Służby specjalne nie mogą służyć żadnej ideologii czy partii politycznej. Służby powinny służyć Państwu i tylko Państwu. Szef nie może być człowiekiem polityki. Powinien być piorunochronem, osłaniać służby swoją osobą przed naporem politycznych zawieruch i awantur. Apolityczność służb to w konsekwencji ich ciągłość, stabilność. Rewolucje są czasami w historii niezbędne. Taką rewolucję 20 lat temu musieliśmy przeprowadzić. Ale najgorsze, co służbom może się przydarzyć, to rewolucja permanentna. Rewolucja, która nieprzerwanie burzy coś, co inni zbudowali, niszcząc przez to ciągłość i spokój niezbędny w pracy funkcjonariuszy. Oby polskie służby specjalne nigdy z podobnymi problemami nie musiały się już mierzyć.

Kraków, 2010

I
ARTYKUŁY I ROZPRAWY

Marcin Gołaszewski

Przełom w procesie walidacji i wyrażaniu wartości diagnostycznej testów wykorzystywanych w badaniach poligraficznych

Proces normalizacji badań poligraficznych

W ciągu ostatnich kilku lat dla poligraferów zarówno w Polsce, jak i na świecie szczególnego znaczenia nabrały takie pojęcia, jak normalizacja i standardy. „Standard" to typowy i przeciętny model czegoś[1]; wspólnie ustalone kryterium, które określa najbardziej pożądane cechy jakiegoś zjawiska. „Norma" natomiast, zgodnie z *Ustawą z dnia 12 września 2002 r. o normalizacji*[2], to *dokument przyjęty na zasadzie konsensu i zatwierdzony przez upoważnioną jednostkę organizacyjną, ustalający – do powszechnego i wielokrotnego stosowania – zasady, wytyczne lub charakterystyki odnoszące się do różnych rodzajów działalności lub ich wyników i zmierzający do uzyskania optymalnego stopnia uporządkowania w określonym zakresie*. Do celów normalizacji należy zaliczyć m.in.: zapewnienie jakości i niezawodności wyrobów, procesów i usług, a także ułatwianie porozumiewania się przez określanie terminów, definicji, oznaczeń i symboli do powszechnego stosowania. Z kolei wśród zasad normalizacji znajdują się: jawność i powszechna dostępność do standardów, uwzględnianie interesu publicznego, dobrowolność uczestnictwa w procesie opracowywania i stosowania norm, zapewnienie możliwości uczestnictwa wszystkich zainteresowanych w procesie opracowywania norm, porozumienie jako podstawa procesu uzgadniania treści norm, jednolitość i spójność postanowień norm, wykorzystywanie sprawdzonych osiągnięć nauki i techniki.

Standardy badań poligraficznych obejmują takie zagadnienia, jak:

- kto może być badany, w jakich okolicznościach i przez kogo,
- rodzaje i sposoby przeprowadzania badań (w tym przygotowanie, wywiad przedtestowy, techniki badawcze i analiza danych),
- sporządzanie dokumentacji i formułowanie opinii,
- kontrola jakości,
- etyka profesjonalna.

Zasady, wytyczne i charakterystyki odnoszące się do powyższych standardów badań poligraficznych wyznaczane są przez:

- normy prawne (w Polsce są to w zasadzie tylko przesłanki przeprowadzania badań poligraficznych oraz wymóg uzyskania zgody badanego; trudno też uznać za standard zarządzenia szefów polskich służb z uwagi na niejednolitość postanowień. Dla porównania w USA jest prowadzony program kontroli jakości, a także istnieją wymogi licencyjne obowiązujące w wielu stanach),
- normy organizacyjne (postanowienia organizacji profesjonalnych, np. American Polygraph Association – APA, Stowarzyszenia Poligraferów Polskich – SPP oraz

[1] *Słownik Języka Polskiego PWN*, [online], http://sjp.pwn.pl/slownik/2576133/standard [dostęp: 21 IX 2012].

[2] *Ustawa z dnia 12 września 2002 r. o normalizacji* (Dz.U. Nr 169, poz. 1386).

organizacji normalizacyjnych, np. American Society for Testing and Materials – ASTM International[3]),
- praktykę i utarte zwyczaje (np. przyjęto zasadę, że nie bada się kobiet ciężarnych, choć formalnie nie jest to nigdzie uregulowane).

Po co nam standardy?

W większości obszarów praktyki badań w Polsce panuje zupełna swoboda. Oznacza to ryzyko rosnących nadużyć i niekompetencji, w skrajnym przypadku utratę wiarygodności środowiska badających i samej metody. Podobna sytuacja, czyli problemy związane ze słabą standaryzacją i brakiem odpowiednich regulacji dotyczących obszaru praktyki badań poligraficznych, miała miejsce w latach 80. i 90. XX wieku w USA. W połączeniu ze zjawiskiem cięcia kosztów związanych z prowadzeniem badań i ostrą konkurencją na rynku usług oferowanych przez poligraferów (czego w Polsce jeszcze się nie obserwuje), doprowadziło to do patologii – nierzetelnych badań wykonywanych na ilość kosztem jakości. Społeczeństwo amerykańskie zaczęło się więc bronić przed badaniami psychofizjologicznymi. Kongres Stanów Zjednoczonych wprowadził pewne restrykcje odnoszące się do tego typu badań. Należy zwrócić uwagę przede wszystkim na dwa akty prawne. Pierwszy z nich został przyjęty w 1990 r. pod nazwą *Americans with Disabilities Act* (ADA). Na podstawie tego dokumentu wykluczono możliwość zadawania pytań dotyczących historii zdrowotnej, a zatem również w kwestii spożywania alkoholu i zażywania leków. Z kolei w 1998 r. Kongres uchwalił *Employee Polygraph Protection Act* (EPPA), ograniczający stosowanie badań poligraficznych wobec pracowników. Wyjątki ustanowiono na rzecz organów rządowych i bezpieczeństwa publicznego, a także w przemyśle farmaceutycznym i jądrowym.

Z doświadczeń amerykańskich płynie wniosek dla Polski, że należy uczyć się na cudzych błędach. Obecnie w różnych zawodach i specjalnościach popularność zyskuje idea deregulacji, jednak w sferze badań poligraficznych zarysowuje się przeciwna potrzeba – wprowadzenia dodatkowych regulacji i wdrożenia standardów.

Polska droga ku jednolitym wysokim standardom jakości badań psychofizjologicznych opartym na solidnych podstawach naukowych

W Polsce proces dochodzenia specjalistów z zakresu badań poligraficznych do wspólnych standardów odbywał się, jak dotąd, głównie poprzez wymianę doświadczeń na seminariach naukowych. Jednym z pierwszych było ogólnopolskie sympozjum naukowe zatytułowane „Badania wariograficzne na użytek prawa", które zorganizowano w 1976 r. w Toruniu. W kolejnych latach brakowało dynamiki w rozwoju tej dziedziny. Ożywienie nastąpiło dopiero na początku XXI wieku. Cykl seminariów poligraficznych organizują każdego roku na zmianę Policja i Żandarmeria Wojskowa. W czerwcu 2010 r. w Emowie odbyło się natomiast z inicjatywy Agencji Bezpieczeństwa Wewnętrznego pierwsze w Polsce Międzynarodowe Sympozjum Poligraferów. Stanowiło ono swoisty

[3] Międzynarodowy charakter ASTM podkreślono, dodając w 2001 r. do nazwy człon *International*. Podobny pomysł był przedmiotem dyskusji podczas 45. dorocznego sympozjum APA w Myrtle Beach w 2010 r. Przeważyło jednak konserwatywne podejście, tj. argument dotyczący rozpoznawalności dotychczasowej marki, na której wiarygodność pracowano przez wiele lat.

impuls w kierunku poważnych prac nad normalizacją badań poligraficznych w naszym kraju.

Inną płaszczyznę prac nad jednolitymi standardami stanowi działalność utworzonego w 1994 r. Stowarzyszenia Poligraferów Polskich. Po okresie kilkuletniego przestoju stowarzyszenie zostało reaktywowane w 2012 r., a na nowego przewodniczącego został wybrany prof. dr hab. Jan Widacki. W kwietniu 2012 r. Zarząd SPP przedstawił ministrowi spraw wewnętrznych Jackowi Cichockiemu memorandum zatytułowane: *Możliwości pełniejszego wykorzystania badań poligraficznych w polskich służbach policyjnych i specjalnych*. Zwrócono w nim uwagę na zróżnicowany poziom przygotowania ekspertów zatrudnionych w instytucjach państwowych i – co za tym idzie – potrzebę systematycznego doskonalenia zawodowego z umożliwieniem kontaktów z doświadczonymi instruktorami z krajów wiodących pod względem zaawansowania badań poligraficznych (USA, Izrael). Wyrażono ubolewanie, że wielu funkcjonariuszy śledczych i przedstawicieli wymiaru sprawiedliwości nie jest świadomych tego, w jaki sposób należy stosować poligraf w śledztwach i dlatego nie wykorzystują wszystkich możliwości, jakimi dysponują. Dla tych grup również niezbędne są odpowiednie szkolenia.

W dokumencie wskazano ponadto, w jakich obszarach, poza obecną praktyką, poligraf mógłby być użyteczny. Mianowicie – badania psychofizjologiczne, szerzej niż dotychczas, można byłoby przeprowadzać w ramach kontroli operacyjnych źródeł informacji oraz w sprawach kadrowych (nie tylko w odniesieniu do kandydatów do służb[4], ale także przy awansach na newralgiczne stanowiska, dostępie do najważniejszych tajemnic i okresowej kontroli funkcjonariuszy). Jeżeli chodzi o nowe obszary zastosowania badań psychofizjologicznych[5], to zaproponowano przeprowadzanie badań przy kontroli nad świadkiem koronnym, a także badanie osób ubiegających się o poświadczenie bezpieczeństwa, azyl lub przyznanie statusu uchodźcy. Część z tych propozycji wymagałaby wydania odpowiednich instrukcji, zarządzeń, a nawet nowelizacji ustaw.

Zwrócono też uwagę na problem prywatnie świadczonych usług w zakresie wykonywania badań poligraficznych. Wyrażono uzasadnione obawy, że osoby bez odpowiednich kwalifikacji są powoływane w charakterze biegłych. W odpowiedzi na to SPP zadeklarowało gotowość przedstawienia zainteresowanym organom listy rekomendowanych osób, których kompetencje nie budzą żadnych wątpliwości.

Dla środowiska polskich poligraferów zarysowują się jednak korzystne perspektywy. Rozwój badań poligraficznych w Polsce z uznaniem dostrzega APA – międzynarodowa organizacja o niepodważalnej pozycji. Jej kierownictwo prognozuje, że Polska mogłaby nawet odgrywać w tej dziedzinie wiodącą rolę w Europie. APA jest gotowe zorganizować w naszym kraju poważne seminarium naukowe, podobne do tego, które odbyło się dla obszaru Azji i Pacyfiku na początku 2012 r. w Singapurze. Oprócz tego w ciągu kilku najbliższych lat przewiduje się ustanowienie w Polsce akredytowanej przez APA placówki szkoleniowej o zasięgu europejskim.

---

[4] Zaskakujące, że takich badań nie przechodzą obecnie kandydaci do służby w Biurze Ochrony Rządu.

[5] Coraz głośniej mówi się również o możliwości wykorzystania badań poligraficznych w ramach nadzoru i terapii osób skazanych za przestępstwa na tle seksualnym. Zaawansowane programy tego typu są prowadzone w Stanach Zjednoczonych i Wielkiej Brytanii.

Normy o znaczeniu międzynarodowym. Nowe podwyższone standardy APA z 2012 r.

Normy badań poligraficznych do powszechnego stosowania odnajdujemy w standardach (obligatoryjnych zarządzeniach) i wytycznych (rekomendacjach) American Polygraph Association oraz w standardach ASTM International. Pierwsza z tych organizacji została założona w 1966 r. i skupia ponad trzy tysiące poligraferów. Druga zaś jest organizacją normalizacyjną, która istnieje od 1898 r. Obie mają w swoich nazwach przymiotnik „American", lecz w istocie są to organizacje międzynarodowe zrzeszające przedstawicieli z całego świata.

W dniu 1 stycznia 2012 r. weszły w życie nowe **standardy praktyki APA**, które wprowadziły m.in.:

- obligatoryjne zastosowanie czujnika ruchu,
- generalny wymóg korzystania jedynie z tych technik, które zostały poddane walidacji (a więc są potwierdzone naukowo),
- określone kryteria dopuszczalności technik w poszczególnych rodzajach badań: dowodowych, konfrontacyjnych, wykrywczych (dochodzeniowych) i przesiewowych,
- w standardach potwierdzono też obowiązek przeprowadzenia kalibracji poligrafu (inaczej mówiąc testu funkcjonalności tego urządzenia) przynajmniej raz na 6 miesięcy.

Warto sprecyzować, że *validus* w jęz. łacińskim oznacza: silny, mocny, skuteczny[6]. „Walidacja" metody pomiarowej – według normy PN-EN ISO/IEC 17025:2005[7] – jest potwierdzeniem przez zbadanie i przedstawienie obiektywnego dowodu, że zostały spełnione wymagania dotyczące zamierzonego zastosowania. Innymi słowy chodzi zatem o stwierdzenie, że test mierzy to, do czego został zaprojektowany, proces analizy według danej metody przebiega w sposób rzetelny, daje wiarygodne wyniki oraz jest niezawodny, zapewnia spójność, czyli odpowiedni poziom zgodności między badającymi (w przypadku badań poligraficznych – chodzi przede wszystkim o odpowiedź na pytanie, jak dokładny będzie poligraf, gdy losowo wybrana osoba przeprowadzająca badanie zastosuje ten sam test wobec również losowo wybranego przeciętnego badanego z dowolnego zakątka Ziemi). Dokładność (poprawność i precyzję) metod pomiarowych i wyników pomiarów określa Polska Norma PN-ISO 5725-2:2002[8].

Jak słusznie zauważyła Pamela Shaw (Przewodnicząca APA w latach 2011–2012), *Wymóg korzystania z potwierdzonych naukowo metod badawczych nie jest, oczywiście, niczym nowym. Inne dziedziny – jak medycyna czy psychologia – doszły w końcu do tych samych wniosków, aczkolwiek wiele lat po tym, jak te dziedziny zostały ustanowione. Okazało się to dla nich wspaniałą rzeczą. Wyobraźcie sobie, jeśli możecie, jak wyglądałyby dziedziny medycyny i psychologii, gdyby nie istniały wymogi stosowania potwierdzonych naukowo metod. Walidacja służy licznym istotnym funkcjom, a w szczególności ochronie obywateli przez nadużyciami, brakiem kompetencji i szarlatańst*wem[9].

---

[6] W. Kopaliński, *Słownik wyrazów obcych i zwrotów obcojęzycznych,* Warszawa 2001, De Agostini, s. 532.

[7] *Ogólne wymagania dotyczące kompetencji laboratoriów badawczych i wzorcujących*, Polski Komitet Normalizacyjny, Warszawa 2005.

[8] *Dokładność (poprawność i precyzja) metod pomiarowych i wyników pomiarów*, Polski Komitet Normalizacyjny, Warszawa 2002.

[9] „Polygraph" 2011, nr 4, s. 194.

Należy pamiętać, że technika to nie tylko sekwencja pytań testowych, ale też zbiór zasad dotyczących sposobu prowadzenia wywiadu przedtestowego, formułowania i omawiania pytań testowych, prezentacji bodźców (pytań) w czasie testu oraz metody analizy danych testowych. Zgodnie z wytycznymi APA, aby uznać daną technikę badawczą za potwierdzoną naukowo, musi ona charakteryzować się następującymi cechami:

- format testu powinien być zgodny z naukowymi zasadami dotyczącymi selekcji celów, formułowania pytań i prezentacji bodźców podczas testu,
- musi uwzględniać potwierdzony naukowo model analizy danych testowych,
- badania dotyczące nowej techniki powinny być przynajmniej dwukrotnie opublikowane w „Polygraph", ewentualnie innych niezależnych czasopismach naukowych, publikacjach rządowych lub wydanych tekstach akademickich.

W omawianych wytycznych sprecyzowano ponadto **kryteria,** jakie powinna spełniać technika dopuszczona do określonych typów badań. Są one nastepujące:

- w **badaniach dowodowych** (dla organów procesowych): przyjmuje się ≥90 proc. dokładności (trafności) i ≤20 proc. wyników nierozstrzygniętych,
- w **badaniach konfrontacyjnych** (dwóch ekspertów bada dwóch lub więcej badanych przedstawiających sprzeczne wersje zdarzenia w taki sposób, że jedna z osób z całą pewnością kłamie): ≥86 proc. dokładności i ≤20 proc. wyników nierozstrzygniętych,
- w **badaniach wykrywczych** (dochodzeniowo-śledczych): ≥80 proc. dokładności (trafności) i ≤20 proc. wyników nierozstrzygniętych,
- w **badaniach przesiewowych** (sprawdzeniowych): potwierdzony w badaniach naukowych poziom dokładności jest znacznie wyższy niż statystyczna szansa wraz z podejściem „sukcesywnego pokonywania przeszkód" wymagającym przeprowadzenia dodatkowych uznanych i bardziej precyzyjnych testów, jeśli test przesiewowy nie jest korzystnie rozwiązany (tzn. pozostają wątpliwości odnośnie do prawdomówności badanego).

Nowe standardy praktyki ustanowione przez APA obowiązują od 1 stycznia 2012 r. członków tej organizacji pod rygorem sankcji (o ile prawo w danym państwie czy stanie nie stanowi inaczej). Inna uznana organizacja – AAPP (Amerykańskie Stowarzyszenie Poligraferów Policyjnych) – zamierza wprowadzić te same standardy w niedługim czasie. Przewiduje się ponadto, że kolejne (stanowe i krajowe) stowarzyszenia poligraferów również to uczynią. Podobnie w Agencji Bezpieczeństwa Wewnętrznego standardy te są obecnie stosowane.

Podwyższone standardy, które niedawno weszły w życie, zostały opracowane już w 2007 r. jako odpowiedź na raport opiniotwórczej amerykańskiej organizacji naukowo-badawczej National Research Council (NRC) z 2003 r.[10] We wnioskach z tego raportu znalazły się zarówno negatywne, jak i pozytywne uwagi. Przeważały jednak te pierwsze:

- naukowe podstawy badań poligraficznych są dalekie od tego, czego oczekuje się od testu, który ma istotny wpływ na podejmowanie decyzji dotyczących bezpieczeństwa narodowego,
- dużą liczbę opracowań dotyczących poligrafu można określić jako czysto teoretyczną,
- istnieją ważne ograniczenia w kwestii diagnostycznej trafności testów, nawet przy postępie w technikach pomiaru i oceny,

[10] *The polygraph and lie detection*, National Research Council, Washington 2003, The National Academies Press.

- istnieją powody do obaw, że podczas badania możliwe jest skuteczne zastosowanie środków zakłócających.

W raporcie NRC zawarto też spostrzeżenia, które dawały powody do umiarkowanego optymizmu na przyszłość. Przyznano bowiem, że *mimo, iż nauka wskazuje na ograniczenia w zakresie potencjalnej trafności testów poligraficznych, jest możliwe, aby osiągnęły na tyle wystarczającą dokładność, by były użyteczne w praktyce*. W metaanalizie wykonanej przez NRC wskaźnik dokładności dla testów w konkretnej sprawie wahał się między 0,81 a 0,91 dla średnich 26 wartości z 52 zbiorów danych branych pod uwagę[11], czyli – mimo ogólnej krytyki – potwierdzono wysoką skuteczność tego rodzaju badań. Takie wyniki otrzymano w 2003 r. Obecnie stan wiedzy na temat badań poligraficznych jest znacznie większy.

Metaanaliza technik badań poligraficznych przeprowadzona przez APA

Zasadnicze pytanie brzmi: które ze znanych dotychczas technik spełniają nowe podwyższone standardy (kryteria walidacyjne) APA z 2012 r.? Odpowiedź przyniosła tzw. **metaanaliza** – uważana za samodzielny rodzaj badania naukowego, który polega na wtórnym odkrywaniu wiedzy poprzez systematyczny przegląd informacji na dany temat zawartych w publikacjach lub źródłach pierwotnych, połączenie tych danych, ich analizę statystyczną, uogólnienie wyników i wnioskowanie.

Metaanaliza przeprowadzona przez Komitet APA ad-hoc ds. potwierdzonych technik objęła: 37 opracowań naukowych (w których omówiono 52 eksperymenty i analizy), 289 osób oceniających testy, 12 665 ocenionych rezultatów spośród 4283 zweryfikowanych badań (6597 wyników z 2300 zweryfikowanych badań ze stwierdzeniem wprowadzania w błąd i 6068 wyników z 1983 zweryfikowanych badań ze stwierdzeniem prawdomówności). Wykluczono te opracowania, które nie dostarczały statystycznych danych będących przedmiotem zainteresowania metaanalizy, a także takie, w których procedury testowania nie zgadzały się z publikowanymi możliwymi do zidentyfikowania opisami technik lub metodami analizy danych testowych. W rezultacie metaanalizy określono:

- **średnią dokładność wszystkich typów badań** poligraficznych na poziomie 87,1 proc. przy średniej ilości wyników nierozstrzygniętych (INC – ang. *inconclusive*) – 12,7 proc.,
- **średnią dokładność badań jednowątkowych** z wykorzystaniem uznanych technik wynoszącą 92,1 proc., przy wynikach INC – 8,8 proc.,
- **średnią dokładność badań przesiewowych** z wykorzystaniem uznanych technik – 85 proc., przy wynikach INC – 12,5 proc.
- **listę technik dopuszczonych do różnych typów badań poligraficznych** (obowiązuje od 1 stycznia 2012 r.).

[11] Zob. tamże, s. 148.

Tabela 1. Lista technik dopuszczonych do badań poligraficznych zgodnie ze standardem APA 2012 r.

Techniki dowodowe (na potrzeby badań dla organów procesowych)/ **/metoda analizy danych**	**Techniki badań wielopodmiotowych** (głównie konfrontacyjnych)[1]/ **/metoda analizy danych**	**Techniki wykrywcze** (pozostałe badania)/ **/metoda analizy danych**
US Federal You-Phase / ESS[2] ■ średnia dokładność: 90,4% ■ nierozstrzygnięte (INC): 19,2% ■ czułość na kłamstwo (*sensitivity*[3]): 84,5% ■ specyficzność (*specificity*[4]): 75,7%	**USAF MGQT**[5] **/ ESS** ■ średnia dokładność: 87,5% ■ nierozstrzygnięte (INC): 17% ■ czułość: 72,9% ■ specyficzność: 70%	**USAF MGQT / skala 7-pozycyjna** ■ średnia dokładność: 81,7% ■ nierozstrzygnięte (INC): 19,7% ■ czułość: 78,3% ■ specyficzność: 53,8%
ZCT (Federal, Utah) / ESS ■ dokładność: 92,1% ■ INC: 9,8% ■ czułość: 81,7% ■ specyficzność: 84,6%	**Federal You-Phase / skala 7-pozycyjna** ■ dokładność: 88,3% ■ INC: 16,8% ■ czułość: 84,5% ■ specyficzność: 75,7%	**CIT (GKT) / system Lykkena** ■ dokładność: 82,3% ■ INC: 0,1% ■ czułość: 81,5% ■ specyficzność: 83,2%
Utah ZCT (różne wersje ogółem) **/ Utah** ■ dokładność: 93% ■ INC: 10,7% ■ czułość: 85,3% ■ specyficzność: 80,9%	**Federal ZCT / skala 7-pozycyjna** ■ dokładność: 86% ■ INC: 17,1% ■ czułość: 85,8% ■ specyficzność: 58,1%	**DLST (TES) / skala 7-pozycyjna** ■ dokładność: 84,4% ■ INC: 8,8% ■ czułość: 74,8% ■ specyficzność: 79,2%
Utah ZCT DLC / Utah ■ dokładność: 90,2% ■ INC: 7,3% ■ czułość: 81,5% ■ specyficzność: 85,7%	**Federal ZCT / skala 7-pozycyjna dowodowa**[6] ■ dokładność: 88% ■ INC: 8,5% ■ czułość: 80,4% ■ specyficzność: 80,9%	**DLST (TES) / ESS** ■ dokładność: 85,8% ■ INC: 9% ■ czułość: 80,9% ■ specyficzność: 75,1%

[1] W dosłownym tłumaczeniu z jęz. ang. *paired testing* (badania sparowane, testy dobrane w pary) – gdzie dwóch badających egzaminuje dwie osoby przedstawiające sprzeczne wersje zdarzenia w taki sposób, że jedna z osób z całą pewnością kłamie.

[2] Ang. *Empirical Scoring System* – empiryczny system oceniania. Jest to poparty dowodami naukowymi model numerycznej analizy danych tekstowych.

[3] Ang. *sensitivity* (czułość, wrażliwość) – odsetek prawidłowych wyników pozytywnych; nastawienie na wykrycie wprowadzania w błąd; zdolność do wyodrębnienia kwestii budzących wątpliwości, stanowiących zagrożenie (istotnych) dla badanego; minimalizacja fałszywych wyników negatywnych (błędnie zaliczających reakcje badanego na pytania relewantne jako typowe dla populacji osób szczerych).

[4] Ang. *specificity* (specyficzność, skonkretyzowanie) – odsetek prawidłowych wyników negatywnych; nastawienie na weryfikację prawdomówności, zdiagnozowanie problemu; zdolność do wykluczenia związku badanego z danym czynem; minimalizacja fałszywych wyników pozytywnych (błędnie zaliczających reakcje badanego na pytania relewantne jako typowe dla populacji osób nieszczerych).

[5] Uśrednione dane dla obu wersji AFMGQT (1 i 2). Zbliżone strukturalnie do tej techniki są **LEPET** oraz **Utah MGQT**, dlatego uznaje się je za dopuszczalne, o ile będą zastosowane te same metody analizy danych testowych jak przy AFMGQT.

[6] W skali „7-pozycyjnej dowodowej" próg decyzyjny dla opinii NDI jest nieco obniżony niż w tradycyjnej i wynosi +4. Dla opinii DI pozostaje bez zmian (-6).

Utah ZCT PLC / Utah ■ dokładność: 93,1% ■ INC: 7,7% ■ czułość: 86,7% ■ specyficzność: 83,3% **Utah ZCT RCMP** (v.1) **/ Utah** ■ dokładność: 93,9% ■ INC: 18,5% ■ czułość: 83,3% ■ specyficzność 70% ***IZCT / HSS** ■ dokładność: 99,4% ■ INC: 3,3% ■ czułość: 97,7% ■ specyficzność: 94,6% ***MQTZCT / Matte** ■ dokładność: 99,4% ■ INC: 2,9% ■ czułość: 96,7% ■ specyficzność: 96,3%	**Backster You-Phase / /Backster** ■ dokładność: 86,2% ■ INC: 19,6% ■ czułość: 83,6% ■ specyficzność: 55,6%	

Źródło: Opracowanie własne na podstawie: *American Polygraph Association, Meta-Analytic Survey of Criterion Accuracy of Validated Techniques,* „Polygraph" 2011, nr 4.

Jak rozumieć powyższą tabelę? W pierwszej kolumnie umieszczono techniki spełniające kryteria ≥90 proc. dokładności (trafności) i ≤20 proc. wyników nierozstrzygniętych. W drugiej kolumnie znalazły się techniki o przynajmniej 86 proc. dokładności i dające nie więcej niż 20 proc. wyników nierozstrzygniętych. W trzeciej natomiast znalazły się techniki o co najmniej 80 proc. dokładności i dające najwyżej 20 proc. wyników nierozstrzygniętych. Techniki z pierwszej kolumny mogą być stosowane również w badaniach wyszczególnionych w kolumnie drugiej, a do badań określonych w ostatniej kolumnie można wykorzystywać techniki wymienione we wszystkich kolumnach. Patrząc od lewej do prawej kryteria dopuszczalności (dokładność) ulegają bowiem obniżeniu.

Przy dwóch technikach – IZCT i MQTZCT – naniesiono w tabeli odnośniki (*). Techniki te zostały wpisane na listę, ale zaznaczono, że dane statystyczne znacznie odbiegają od pozostałych danych dotyczących technik badań poligraficznych i stanowią tzw. wartości oddalone. Należy zatem podchodzić do nich z dużą ostrożnością. Tym bardziej, że są to tzw. techniki autorskie, które nie zostały zweryfikowane przez niezależnych badaczy. APA zwróciła ponadto uwagę na pewne uchybienia w procesie walidacji tych technik.

Na liście nie znalazły się natomiast te techniki, dla których nie można było odnaleźć dwóch opublikowanych opracowań naukowych potwierdzających ich niezawodność i rzetelność lub jeśli stwierdzona dokładność albo wskaźnik wyników nierozstrzygniętych wykraczały poza graniczne wymogi APA dla badań dowodowych, konfrontacyjnych i wykrywczych. Wśród tych technik można wymienić m.in.: US Army MGQT, test Reida, POT-B, technikę Marcy'ego oraz R/I[12].

[12] Korzystanie z dwóch ostatnich technik jest warunkowo dozwolone do końca 2012 r. Jest to dodatkowy czas na przeprowadzenie walidacji. Nic jednak nie wskazuje na to, aby wysiłki zwolenników tych technik się powiodły.

Wszystkie inne techniki, które nie znajdują się na liście, powinny być opatrzone adnotacją „eksperymentalne". Takie techniki, jak np. R/I, POT-B lub SAT mogą być wykorzystywane pomocniczo, o ile nie będą traktowane jako podstawa do wydania opinii na temat prawdomówności badanego. Zbiór dopuszczalnych technik jest otwarty. Może on zostać poszerzony o nowe techniki, jeśli spełnią one kryteria walidacyjne i dotyczące minimalnych poziomów dokładności oraz maksymalnych poziomów wyników nierozstrzygniętych.

Może się zdarzyć, że niektórzy poligraferzy od dawna stosują pewną technikę z przekonaniem, że jest ona skuteczna. Dlatego ich zaniepokojenie może wzbudzić fakt, że wybrana przez nich technika nie została poparta dostatecznymi dowodami naukowymi i nie znalazła się na wspomnianej liście. W takim przypadku powinni oni dostosować się do wytycznych APA, ponieważ jest to największa organizacja skupiająca poligraferów z różnych obszarów geograficznych na świecie i wywiera ogromny wpływ na metodykę i rozwój badań psychofizjologicznych. Szczególnie w ostatnich latach czyni wysiłki, aby ekspertyzy z zakresu badań poligraficznych nosiły cechy dowodów naukowych i tak były odbierane przez potencjalnych zleceniodawców, osoby poddawane badaniom i całe środowisko nauk sądowych.

Dowodowe wykorzystanie ekspertyzy z zakresu badań poligraficznych (uwarunkowania prawne w USA i w Polsce)

W Stanach Zjednoczonych w 1920 r. miał miejsce precedens, w którym obrońca Jamesa Frye'a oskarżonego o zabójstwo złożył wniosek o poddanie go badaniom poligraficznym. Sąd sformułował wtedy koncepcję *general acceptance* oznaczającą, że dopuszczalność dowodu naukowego ma wtedy miejsce, gdy uzyska się powszechną akceptację specjalistów z danej dziedziny co do odpowiednio wysokiej wartości danego rodzaju ekspertyzy. Większość z nich uznała, że badania poligraficzne dopiero się rozwijają i w związku z tym są mało wiarygodne.

W 1989 r. Federalny Sąd Apelacyjny z 11. Okręgu stwierdził w sprawie Stany Zjednoczone vs. Piccinonna, iż (…) *per se wykluczenie dowodu z poligrafu nie jest już zagwarantowane*[13].

Natomiast w 1993 r. Sąd Najwyższy USA w sprawie Daubert vs. Merrell Dow Pharmaceuticals, Inc. uznał iż, reguła Frye'a jest zbyt restrykcyjna. Określił wówczas następujące warunki dopuszczalności dowodu naukowego, nazwane później regułą Dauberta:

- możliwość weryfikacji przedstawionej teorii,
- ustalony poziom błędu dla danej techniki,
- zrecenzowanie i opublikowanie badań dotyczących danej techniki,
- znany poziom akceptacji techniki w środowisku naukowym,
- ustanowienie standardów określających prawidłowe i akceptowalne stosowanie danej techniki.

Choć w Polsce reguła Dauberta formalnie nie obowiązuje, to sformułowane powyżej warunki zostały przytoczone jako swoisty punkt odniesienia, do którego powinni dążyć polscy poligraferzy. Kluczowe znaczenie w procesowym wykorzystaniu dowodów z badania poligraficznego mają art. 192a, 193 i 199a kodeksu postępowania

[13] M. Handler, Ch.R. Honts, D.J. Krapohl, R. Nelson, S. Griffin, *Integration of pre-employment polygraph screening into the police selection process*, „Polygraph" 2009, nr 4, s. 242.

karnego[14]. Artykuł 193 jest ogólnym przepisem odnoszącym się do biegłych i stanowi, że: *Jeżeli stwierdzenie okoliczności mających istotne znaczenie dla rozstrzygnięcia sprawy wymaga wiadomości specjalnych, zasięga się opinii biegłego albo biegłych*. Natomiast art. 192a przewiduje, iż *W celu ograniczenia kręgu osób podejrzanych lub ustalenia wartości dowodowej ujawnionych śladów można pobrać odciski daktyloskopijne, wymaz ze śluzówki policzków, włosy, ślinę, próby pisma, zapach, wykonać fotografię osoby lub dokonać utrwalenia głosu*. (…) *Za zgodą osoby badanej biegły może również zastosować środki techniczne mające na celu kontrolę nieświadomych reakcji organizmu tej osoby.* Adresatem tego przepisu jest organ prowadzący postępowanie przygotowawcze w danej sprawie. Z kolei art. 199a jest uzupełnieniem regulacji zawartej w art. 192a § 2 i brzmi następująco: *Stosowanie w czasie badania przez biegłego środków technicznych mających na celu kontrolę nieświadomych reakcji organizmu badanej osoby możliwe jest wyłącznie za jej zgodą. Przepisu art. 199 nie stosuje się*. Cóż z tego wynika? Pośrednio uprawnione jest wnioskowanie, że na podstawie tego artykułu badania poligraficzne mogą być prowadzone również w fazie *in personam* postępowania przygotowawczego – wobec podejrzanego, a nawet w postępowaniu sądowym – w stosunku do oskarżonego[15]. Badania te mogą odnosić się także do świadka (art. 192 § 1). Artykuł 199a uchyla ponadto zakaz dowodowy wskazany w art. 199 (czyli niedopuszczalność korzystania z wypowiedzi oskarżonego jako dowodu dotyczącego zarzucanego mu czynu, złożonych wobec biegłego).

Jednak, co trafnie podkreślił prof. dr hab. Tadeusz Tomaszewski, „Problem w największym zakresie dotyczy nie przepisów kodeksowych (choć oczywiście są one źle rozumiane), lecz oceny dowodów. Jak wiadomo, w polskim procesie karnym obowiązuje zasada swobodnej oceny dowodów. W związku z tym zawsze tak było (i teraz też tak jest), że jeżeli przepisy dopuszczały dowód z badań poligraficznych, to tylko w gestii organu procesowego leżała ocena, czy jest to wystarczająco wiarygodna metoda, aby ją zastosować. Sąd decyduje, czy wykorzystać opinię z badania poligraficznego jako jedną z podstaw swego orzeczenia. Brakuje, niestety, odpowiedniego wyszkolenia i wiedzy wśród prawników na temat badań poligraficznych, stąd wielu procesualistów nie rozumie, jakie może być prawidłowe wykorzystanie poligrafu”[16].

Znaczący postęp w precyzji określania wyników testów. Sposób na rozwiązanie części problemów spotykanych dotychczas w praktyce

Do niedawna jedyną techniką, przy której można było wyraźnie wskazać prawdopodobieństwo wystąpienia błędu dla obliczanych wyników był CIT[17] – de facto jest to nieco bardziej rozbudowana technika z seriami testów wiedzy o czynie – GKT[18] lub

[14] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (Dz.U. Nr 89, poz. 555 z późn. zm.).

[15] T. Grzegorczyk, *Kodeks postępowania karnego. Komentarz*, Kraków 2005, Zakamycze, s. 513.

[16] T. Tomaszewski, *O biegłych dla biegłych – wykład dla ekspertów*, w: *Normy prawne i standardy branżowe w zakresie badań poligraficznych w wybranych krajach*, materiały z Międzynarodowego Sympozjum Poligraferów, Centralny Ośrodek Szkolenia ABW, Emów 21–24.06.2010, s. 90.

[17] Z jęz. ang. *Concealed Information Test* – test ukrytych informacji.

[18] Z jęz. ang. *Guilty Knowledge Test* – test wiedzy winnego, w Polsce bardziej znany jako „test wiedzy o czynie”; klasyczny test rozpoznania.

POT-A[19], wykorzystująca system oceniania Lykkena[20]. Jej niewątpliwą wadą jest praktyczne zastosowanie jedynie w kilku procentach weryfikowanych za pomocą poligrafu wersji zdarzeń.

Od 2009 r. dla ekspertów dostępny jest również Empiryczny System Oceniania (ESS), który można zastosować przy większości uznanych technik badawczych. Ma to wręcz rewolucyjne znaczenie. ESS jest bowiem narzędziem, które istotnie zwiększa wartość diagnostyczną (dowodową) ekspertyzy z zakresu badań poligraficznych, ponieważ pozwala na określenie konkretnego znaczenia statystycznego (prawdopodobieństwa błędu) rezultatów testów. Jest to nieskomplikowany, prosty do zastosowania system. Uwzględnia dane normatywne (wartości reprezentatywne, które mogą być wykorzystane jako linia odniesienia, do której będą porównywane następnie uzyskiwane dane) – zarówno dla badań diagnostycznych, jak i przesiewowych – a to oznacza szeroki zakres zastosowania. Znane są też wielkości wrażliwości, specyficzności, błędu fałszywych wyników pozytywnych, błędu fałszywych wyników negatywnych oraz badań nierozstrzygniętych w przypadku badanych prawdomównych i kłamiących.

W wielu przypadkach poligraferzy stwierdzają we wnioskach ze swoich badań, że wyniki testów świadczą o „wysokim prawdopodobieństwie" wprowadzania przez badanego w błąd lub odwrotnie. Na przykład w zarządzeniu Komendanta Głównego Straży Granicznej[21] przedstawiono jedną z możliwych treści opinii po badaniu poligraficznym: *w wyniku analizy poligramów, uzyskanych wyjaśnień, a także zachowania w czasie badania można stwierdzić z dużym prawdopodobieństwem, iż osoba badana ukrywa istotne fakty związane z pytaniami (nr pytania), co stawia ją w niekorzystnym świetle jako kandydata do służby w Straży Granicznej*. Takie wnioskowanie jest jednak obarczone poważnym mankamentem. Pojawia się bowiem pytanie – *z dużym prawdopodobieństwem*, czyli z jakim? Jaką tolerancję błędu przyjęto i jakie jest prawdopodobieństwo błędu (wartość p) dla wyników poszczególnych testów przeprowadzonych w konkretnym badaniu? Oczywiście – mając na uwadze fakt, że średnia wartość diagnostyczna wszystkich testów poligraficznych wynosi około 90 proc., a gdy dochodzi do tego jeszcze doświadczenie badającego, który ma bezpośredni kontakt z badanym – to w zdecydowanej większości przypadków opinia o prawdomówności badanego będzie trafna, a przynajmniej można przyjąć, że prawdopodobieństwo takiej ewentualności będzie wysokie. Warto przeanalizować jednak problem, który obrazuje scena hipotetycznego spektaklu na sali rozpraw[22].

---

[19] Z jęz. ang. *Peak of Tension A* – test szczytowego napięcia typu A, czyli ze znanym rozwiązaniem (kluczem w teście).

[20] W systemie Lykkena bierze się pod uwagę jedynie reakcje elektrodermalne. Jeśli największe pobudzenie fizjologiczne występuje przy kwestii kluczowej, to ocena dla tego testu wynosi 2. Jeśli druga co do wielkości reakcja EDA/GSR występuje przy kwestii kluczowej, ocena wynosi wówczas 1. Wszystkie pozostałe warianty są oceniane na 0. Zakres końcowych wyników może się więc wahać od 0 do podwójnej liczby podtestów CIT. Próg decyzyjny stanowi liczba równa ilości przeprowadzonych serii testu CIT. Specjalna tabela określa dla każdego wyniku testu prawdopodobieństwo rozpoznania przez badanego kluczowych elementów umieszczonych w teście. Na przykład łączna ocena równa 7 przy pięciu seriach pytań będzie oznaczała istnienie prawdopodobieństwa wynoszącego zaledwie 3 proc., że badany nie zna szczegółów danego zdarzenia.

[21] *Zarządzenie nr 4 Komendanta Głównego Straży Granicznej z dnia 11 stycznia 2012 roku*. (Dz. Urz. Komendy Głównej Straży Granicznej, poz. 3, 1 lutego 2012 r.).

[22] Por. R. Nelson, M. Handler, P. Shaw, M. Gougler, B. Blalock, Ch. Russell, B. Cushman, M. Oelrich, *Using the Empirical Scoring System*, „Polygraph" 2011, nr 2.

Akt 1

Organ procesowy do biegłego: „Wydał Pan opinię NDI – nie stwierdzono wprowadzania w błąd. Czy jest Pan całkowicie przekonany, że reakcje zarejestrowane podczas przeprowadzonego przez Pana testu poligraficznego przy pytaniach odnoszących się do rozpatrywanej sprawy wyglądają tak typowo, jak u osoby prawdomównej?"

Biegły: „Tak".

Organ procesowy: „Tak? Powtórzę zatem jeszcze raz. Czy jest Pan absolutnie pewny, że reakcje zarejestrowane na wykresach poligraficznych przy pytaniach relewantnych mogły wystąpić wyłącznie, czyli w 100 proc. przypadków, u osoby prawdomównej?"

Biegły: „Pan dobrze wie, iż nie ma właściwie metody analizy kryminalistycznej, która byłaby w 100 proc. przypadków bezbłędna. Jednakże w tym konkretnym przypadku istnieje bardzo wysokie prawdopodobieństwo, że u badanego[23] wystąpiły takie reakcje, które typowo przypisuje się osobie prawdomównej. Innymi słowy – jest znikome prawdopodobieństwo, że reakcje zarejestrowane u badanego mogłyby być właściwe dla osoby wprowadzającej w błąd".

Organ procesowy: „Potwierdził Pan, że zastosowana metoda nie jest w 100 proc. bezbłędna, ale jednocześnie utrzymuje Pan, że prawdopodobieństwo błędu wydanej przez Pana opinii jest znikome. Proszę wobec tego o przedstawienie poziomu statystycznego znaczenia lub prawdopodobieństwa błędu dla rezultatu ocenianego przez Pana testu".

Biegły: „Przepraszam, czy może Pan powtórzyć pytanie. Nie do końca rozumiem..."

Organ procesowy: „Jaka jest wartość p lub prawdopodobieństwo błędu związane z pańskim numerycznie ocenianym rezultatem testu?"

Biegły: „Yhh... Niestety, nie mogę tego powiedzieć. Nie dysponuję takimi danymi".

Organ procesowy: „W tej sytuacji nie mam więcej pytań, Wysoki Sądzie".

W tej sytuacji sąd zapewne nie skorzysta z opinii biegłego przy wydawaniu swojego orzeczenia.

Przedstawiona scena nie musiała jednak tak wyglądać. Pomocny w rozwiązaniu przedstawionego problemu byłby wspomniany wcześniej system oceniania ESS. Załóżmy w przykładowym wariancie, że przeprowadziliśmy test Federal ZCT[24] w konkretnej sprawie (jedno zagadnienie). Oceniliśmy go zgodnie z systemem ESS i otrzymaliśmy wynik całkowity +12. Reguły decyzyjne ESS dla testów porównania stref zakładają, że przy ocenie całościowej $\geq +2$ wydajemy opinię NDI (ang. *no deception indicated* – nie stwierdzono wprowadzania w błąd). Następnie patrzymy na odpowiednią tabelę prawdopodobieństwa i szukamy wartości +12 w kolumnie z wynikami wskazującymi na prawdomówność badanego.

[23] Oskarżonego lub świadka.

[24] Test porównania stref Rządu Federalnego USA.

Tabela 2. Prawdopodobieństwo błędu dla różnych wyników numerycznej analizy danych testowych zgodnie z systemem ESS w badaniach wszystkimi formatami ZCT z trzema pytaniami relewantnymi.

Badania ZCT (wszystkie formaty z trzema pytaniami relewantnymi)			
Progi decyzyjne - prawdomówność		**Progi decyzyjne – wprowadzanie w błąd**	
Na podstawie dystrybucji całościowych ocen osób wprowadzających w błąd		**Na podstawie dystrybucji całościowych ocen osób prawdomównych**	
Próg decyzyjny	**Wartość p**	**Próg decyzyjny**	**Wartość p**
-1	0,159	1	0,159
0	0,130	0	0,127
1	0,106	-1	0,099
2	0,085	-2	0,077
3	0,067	-3	0,058
4	0,052	-4	0,043
5	0,040	-5	0,032
6	0,030	-6	0,023
7	0,023	-7	0,016
8	0,017	-8*	0,011
9	0,012	-9	0,008
10	0,008	-10	0,005
11	0,006	-11	0,003
12	**0,004**	-12	0,002
13	0,003	-13	0,001
14	0,002	-14	<0,001
15	0,001	-15	<0,001
16	<0,001	-16	<0,001

Źródło: R. Nelson, M. Handler, *Empirical Scoring System: NPC Quick Reference*, Lafayette Instrument 2010.

Zgodnie z danymi statystycznymi zawartymi w tabeli wydanie opinii NDI na podstawie sumy globalnej +12 świadczy o tym, iż znaczenie statystyczne dla tego wyniku testu wynosi 0,004 – czyli istnieje prawdopodobieństwo wynoszące zaledwie 0,4 proc., że osoba badana wprowadzała jednak w błąd podczas testu. Inaczej mówiąc – prawdopodobieństwo, że osoba badana była prawdomówna podczas tego testu wynosi aż 99,6 proc. Gdyby biegły dysponował tymi danymi, scena na sali rozpraw wyglądałaby zupełnie inaczej niż w pierwszym przykładzie.

Akt 2

Organ procesowy: „Jaki jest poziom statystycznego znaczenia lub prawdopodobieństwo błędu dla rezultatu manualnie ocenianego przez Pana testu?"

Biegły: „Na podstawie danych normatywnych i Empirycznego Systemu Oceniania – popartego dowodami naukowymi modelu numerycznej analizy danych testowych przy psychofizjologicznej detekcji wprowadzania w błąd – poziom statystycznego znaczenia lub prawdopodobieństwo błędu (wartość p) dla tego rezultatu testu wynosi 0,004. Innymi słowy – prawdopodobieństwo, że taki wynik testu zaistniał przy osobie wprowadzającej w błąd jest równe 4 na 1000, czyli jak 1 na 250 (0,4 proc.) przypadków."

Organ procesowy: „Nie mam więcej pytań, Wysoki Sądzie".

W ten sposób biegły doskonale poradził sobie z trudnym pytaniem sędziego, prokuratora czy obrońcy i potwierdził wysoką wartość diagnostyczną swojej ekspertyzy.

Zaprezentowany przykład pokazuje, jak precyzyjnie jest w stanie wypowiadać się współcześnie ekspert z zakresu badań poligraficznych. Ma on do dyspozycji szeroki wachlarz uznanych technik i systemów oceny poligramów, dzięki czemu potrafi skutecznie zweryfikować wiele problemów o różnym stopniu złożoności. Warto podkreślić, że opieranie się na podstawach naukowych daje poligraferom pewność oraz zaufanie do rezultatów badań i czyni ich wiarygodnymi w oczach odbiorców sporządzanych opinii. Pozostaje wyrazić nadzieję, że będzie to nasza „polska norma".

Abstrakt

W niniejszym artykule autor opisuje proces normalizacji badań poligraficznych w Polsce i na świecie oraz uzasadnia potrzebę określenia jednolitych standardów przeprowadzania takich badań. Powołuje się przy tym na dotychczasowy dorobek American Polygraph Association, przedstawiając wnioski płynące z najnowszego raportu tej organizacji na temat uznanych technik badawczych. Następnie rozważa problematykę dowodowego wykorzystania ekspertyz z zakresu badań poligraficznych, porównując polskie regulacje do sytuacji w Stanach Zjednoczonych. Na zakończenie autor pokazuje obecne możliwości precyzyjnego określania rezultatów testów poligraficznych na podstawie Empirycznego Systemu Oceniania (ESS).

Abstract

In this article the author describes the standardization of polygraph examinations in Poland and around the world, and justifies the need for uniform standards for conducting such examinations. He refers to the current achievements of the American Polygraph Association and presents the conclusions of the latest report on validated polygraph techniques. The issue of evidentiary usage of polygraph expert opinions in Poland is also considered in comparison to the situation in the United States. Finally, the author shows the current capabilities of formulating precise outcomes of polygraph tests according to Empirical Scoring System (ESS).

Mirosław Sadowski

Dżihad – święta wojna w islamie

(...) *one must go on jihad at least once a year... One may use a catapult against them* [non-Muslims – przyp. aut. art.] *when they are in a fortress, even if among them are women and children. One may set fire on them and/or drown them.*

Al-Ghazali[1]

(...) *celem islamskiego dżihadu jest wyeliminowanie wszystkich systemów niemuzułmańskich i wprowadzenie w ich miejsce rządów opartych na islamie. W tych rewolucyjnych zapędach islam nie zamierza ograniczać się do jednego kraju czy nawet grupy państw. Celem islamu jest rewolucja na skalę światową.*

Sayyid Abul A'la Maududi[2]

Celem artykułu jest wyjaśnienie kontrowersji i nieporozumień narosłych wokół koncepcji dżihadu. Autor przedstawia je w kontekście innych obowiązków nałożonych na muzułmanów, a następnie dokonuje historycznego przeglądu wybranych stanowisk i analizy leksykalnej badanego zagadnienia. Omawiając dżihad z dwóch punktów widzenia: jako agresywną wojnę z niewiernymi z jednej strony i walkę, jaką toczą wyznawcy Allaha z własnymi słabościami, aby stać się lepszymi muzułmanami z drugiej strony, autor stara się wykazać metodologiczną słuszność obu stanowisk. W konkluzji próbuje dowieść, że dżihad rozumiany jako święta wojna z niewiernymi i będący jego konsekwencją dżihadyzm są jednymi z najbardziej niebezpiecznych wyzwań przed jakimi stoi współczesny świat.

Islam, ostatnia z trzech wielkich religii monoteistycznych wyrosłych w semickim kręgu cywilizacyjnym, zarówno w jej średniowiecznym rozumieniu, jak i dzisiaj, wyznacza granice działalności człowieka w jego życiu indywidualnym i wspólnotowym. Ta współcześnie najdynamiczniej rozwijająca się religia i ideologia, wspomagana prawem religijnym – szariatem, wytycza swoim wyznawcom ściśle określone ramy

[1] (...) *każdy musi wziąć udział w dżihadzie przynajmniej raz do roku... Wolno użyć katapulty przeciw nim* [niemuzułmanom – przyp. aut. art.]*, kiedy są w fortecy, nawet jeśli są wśród nich kobiety i dzieci. Wolno ich podpalić i/lub utopić*...Za: M.A. Khan, *Islamic Jihad: A Legacy of Forced Conversion, Imperialismand Slavery*, New York 2009, iUniverse, s. 1. Abu Hamid Muhammad Al-Ghazali (1058–1111) był teologiem, filozofem, mistykiem, prawnikiem i muzułmańskim teoretykiem polityki. W myśl jego koncepcji politycznej szariat jest fundamentem, na którym opiera się funkcjonowanie państwa bożego. W swoich rozważaniach podejmował kwestie jedności władzy duchownej i świeckiej, przekonywał, że rządy w państwie powinny być tak sprawowane, aby wierny muzułmanin mógł jak najlepiej przygotować się do życia przyszłego. Al-Ghazali jest uważany przez muzułmanów za drugi po proroku Mahomecie wielki autorytet islamu.

[2] S.A. Ala Mududi, *Dżihad w islamie,* Bejrut 1980, s. 9, za: N. Darwish, *Okrucieństwo w majestacie prawa. Prześladowanie kobiet w świecie islamu*, Warszawa 2008, Kefass, s. 16. Sayyid Abul A'la Maududi (1903–1977), pakistański dziennikarz, teolog i radykalny filozof polityczny, uważany za jednego z najbardziej wpływowych myślicieli islamskich XX wieku.

i reguły postępowania. Warto wyjaśnić, że szariat to religijne prawo muzułmańskie (prawo islamu), które powstawało między VII a IX wiekiem po Chrystusie. Na źródła tego prawa składają się: Koran, sunna, idżma i kijas[3]. Szariat określa obowiązki wobec Allaha i zasady postępowania pomiędzy ludźmi, zwłaszcza pomiędzy muzułmanami, opierając się na trzech fundamentalnych nierównościach: pomiędzy muzułmaninem a wyznawcą innej religii, pomiędzy mężczyzną a kobietą oraz pomiędzy człowiekiem wolnym a niewolnikiem (dziś to trzecie rozróżnienie straciło na znaczeniu). Z prawnego punktu widzenia szariat uznaje wyższość muzułmanina nad niemuzułmaninem, podobnie wyższość mężczyzny nad kobietą. Kobiety mają niższy status, którego źródeł należy poszukiwać w Koranie: werset 228 sury II głosi: *Mężczyźni mają nad nimi wyższość*[4]. W celu lepszego zobrazowania tej zależności można przytoczyć następujące różnice: tylko mężczyzna – muzułmanin może poślubić niemuzułmankę, muzułmanka nie może poślubić niemuzułmanina. Tylko mężczyzna może mieć cztery żony. Zeznania jednego mężczyzny równoważą zeznania dwóch kobiet. Kobieta dziedziczy połowę tego, co mężczyzna. Kolejną zasadą świadczącą o przewadze islamu nad innymi religiami jest to, że niemuzułmanin nie może dziedziczyć po muzułmaninie.

Również kwestie dotyczące prowadzenia świętej wojny w islamie (dżihadu) są regulowane przez szariat. Przed analizą terminu „dżihad" w artykule zostanie przedstawionych kilka uwag na temat islamu i obowiązków, które ciążą na jego wyznawcach. Nie sposób bowiem dokonać analizy zjawiska „muzułmańskiej świętej wojny" bez odniesienia się do jego religijnych i prawnych korzeni.

Zgodnie z powszechnie przyjętym przekonaniem, islam nie tylko żąda akceptacji pewnych prawd i dogmatów religijnych, lecz określa także zespół wierzeń i przepisów regulujących doczesną organizację wspólnoty wiernych i zachowania indywidualnych wyznawców. Tym samym życie muzułmanina było oparte na zasadach przekazanych przez Mahometa w Koranie, wokół których od narodzin islamu kształtowała się muzułmańska cywilizacja i które organizowały życie prywatne wyznawców Allaha. Warto zauważyć, że w warunkach tradycyjnych religia ta była na Bliskim Wschodzie stylem życia i w sposób niezwykle precyzyjny określała reguły postępowania i zachowanie wiernych. Na przykład gildie kupieckie miały charakter stowarzyszeń religijnych, a zwyczajowy strój był sankcjonowany religijnie. Również nauczanie, sposób nacinania arbuza, pora, zasady odmawiania i kierunek modlitwy, wszystko to miało religijną podstawę i było drobiazgowo regulowane przez szariat. Z uwagi na to, że islam, inaczej niż judaizm czy chrześcijaństwo, nie znał stanu kapłańskiego, spory odsetek ludności miejskiej wykonywał zawody o charakterze religijnym.

W islamie nie ma instytucji Kościoła ani centralnej władzy duchownej odpowiadającej katolickiej instytucji papiestwa. Islam nie zna sakramentów świętych, a tym samym nie potrzebuje duchowieństwa, które byłoby ich szafarzem, chociaż wśród muzułmanów istnieje grupa mężczyzn mających podobną pozycję i autorytet, jak duchowni w innych religiach, a niekiedy nawet znacznie je przewyższającą. Na przykład współcześnie piątkowe modły w meczecie prowadzone są przez imama – mężczyznę wyróżniającego się wiedzą teologiczną.

---

[3] Szerzej por. M. Sadowski, *Powstanie i rozwój islamskiej doktryny prawa* (*VII – IX w.*), „Przegląd Prawa i Administracji" 2003, nr 55, s. 3–31.

[4] Wszystkie cytaty z Koranu autor przytacza za: *Koran,* tłum. J. Bielawski, Warszawa 1986, PIW. W opisie tego i kolejnych cytatów autor podaje najpierw numer sury, tj. rozdziału (cyfra rzymska), a następnie numer ajatu – wersetu (cyfra arabska).

Islam, w odróżnieniu od religii rzymsko-katolickiej, nie ma dogmatów ustalanych i bronionych przez centralną władzę duchowną, ponieważ w islamie władza taka nie istnieje. Pomimo tego w islamie występują pewne prawdy, w które muzułmanie muszą wierzyć i manifestować swoją wiarę w nie na zewnątrz, w przeciwnym razie mogliby zostać uznani za heretyków lub obłudników. Muzułmanin musi wierzyć w jednego Boga, aniołów, księgi objawione, których dopełnieniem jest Koran, wysłanników i proroków – od Adama po Mahometa, a także w dzień Sądu Ostatecznego, po którym każdego człowieka czeka raj lub piekło.

Codzienne praktyki i życie publiczne wiernych podporządkowane są pięciu nakazom, które od dawna uznawane są za „filary" – *arkan ad din* – islamu. Są to: wyznanie wiary – *szahada*, modlitwa – *salat*, post – *saum*, jałmużna nakazana prawem – *zakat* oraz pielgrzymka do Mekki – *hadżdż*. Każdy muzułmanin, który np. zaniedbywał obowiązkowej modlitwy lub nie wypełniał postu, zasługiwał na miano niewiernego – *kafir*, co mogło skutkować dla niego więzieniem. Prawnicy muzułmańscy przywiązywali wielką wagę do przepisów dotyczących wypełniania obowiązków religijnych przez muzułmanów i bardzo starannie je opracowali.

Przynajmniej jeden nurt w islamie – charydżyci[5], do godności szóstego filaru podnosił obowiązek prowadzenia świętej wojny z niewiernymi (*dżihad*) i to właśnie jej islam zawdzięcza niezwykłą ekspansję i światową potęgę[6]. Pogląd charydżytów na dżihad nie był zupełnie odosobniony, gdyż, podobnie jak oni, słynny średniowieczny prawnik i teolog ibn Tajmijja[7] głosił, ze dżihad był tak samo ważnym obowiązkiem wierzącego muzułmanina, jak pięć filarów islamu[8].

Także Albert Hourani, brytyjsko-libański uczony z ubiegłego wieku, przekonuje, że do tych szczególnych obowiązków wiernych dołączano zachętę, aby kroczyć drogą Boga (dżihad), co było tożsame z prowadzeniem walki na rzecz powiększenia panowania islamu[9].

---

[5] U swojego zarania społeczność islamu była monolitem, podzieliła się w czasie bitwy pod Siffin (657 r.) pomiędzy czwartym kalifem wybieralnym Alim a gubernatorem Syrii Muawiją, który pretendował do tytułu kalifa. Ogromna większość muzułmanów pozostała wierna „zwyczajowi Proroka" – sunna Tan Nabi, czyli zwyczajowi sunnickiemu. Powstały dwa ugrupowania mniejszościowe: charydżyci – chawaridż, czyli „wychodzący" i szyici, czyli zwolennicy „ugrupowania" – sziat Ali (partii Alego). Oba odłamy dały później początek innym, mniej lub bardziej radykalnym sektom muzułmańskim.

[6] P. Hitti, *Dzieje Arabów,* Warszawa 1969, PWN, s. 118.

[7] Taki ad-Din Abu al-Abbas Ahmad Ibn Abd al-Halim ibn Tajmijja (1263–1328). Średniowieczny teolog, jurysta, znawca literatury arabskiej i leksykograf, który zwalczał spekulację filozoficzną i zdecydowanie potępiał wszelkie wypaczenia pierwotnego islamu. Jego celem była całościowa reforma społeczności muzułmańskiej i państwa, z tych powodów krytykował reżim Mameluków. Poglądy ibn Tajmijji powstawały w sytuacji zagrożenia islamu przez wrogów zewnętrznych (obecność krzyżowców w Palestynie), oraz były skutkiem wewnętrznych sporów w łonie społeczności muzułmańskiej. Głównym celem, jaki sobie stawiał, był powrót do źródeł pierwotnego islamu, tj. Koranu i sunny, wierzył bowiem, że zakończenie sporów, powrót do pierwotnego islamu i oczyszczenie go z wszelkich fałszywych naleciałości pozwoli na uchronienie go przed wrogami. Jego poglądy uważane są za jedną z intelektualnych podstaw wahhabizmu, oficjalnej, ortodoksyjnej doktryny panującej we współczesnej Arabii Saudyjskiej. Również wielu współczesnych muzułmańskich radykałów w świecie sunnickim powołuje się na jego dzieła i czerpie z nich inspirację. Fundamentaliści islamscy XXI wieku w poglądach ibn Tajmijji znajdują uzasadnienie dla swoich tez pozwalających toczyć walkę nawet z rządem islamskim, jeśli zezwala on na stosowanie innego prawa niż szariat na swoim terytorium. Koncepcje ibn Tajmijji były studiowane m.in. w ramach nauki prawa islamskiego w obozach Al-Kaidy w Pakistanie czy Afganistanie.

[8] J. Gurulē, *Unfandingterror: The Legal Response to the Financing of Global Terrorism,* Northampton, Mass. 2008, s. 54. Warto dopowiedzieć, że ibn Tajmijja nie tolerował tych przywódców i duchownych, którzy według niego odchodzili od prawdziwego praktykowania wiary, zob. tamże.

[9] A. Hourani, *Historia Arabów*, Gdańsk 2002, Marabut, s. 76.

Warto pamiętać, że święta wojna pojawia się równocześnie z narodzinami islamu, religia ta powstawała bowiem w atmosferze walk i rozprzestrzeniała się dzięki zbrojnym zmaganiom, a islam właśnie dzięki podejmowaniu działań zbrojnych stał się religią o światowym zasięgu[10].

Próba umiejscowienia dżihadu w kontekście innych obowiązków religijnych ciążących na wiernych wymaga wywodu dotyczącego ścisłych, niekiedy nierozerwalnych związków pomiędzy religią a prawem w islamie. Należy bowiem wiedzieć, że wypowiedzi odnoszące się do autorytetu Koranu jako źródła prawa zobowiązującego do okazywania wiary i pobożności, były swego rodzaju konsekwencją i pośrednim obwieszczeniem prawa religijnego. Bardziej formalny i bezpośredni charakter obowiązującego prawa zyskiwały natomiast te wypowiedzi przekazane przez Mahometa, w których były zawarte nakazy wzywające do zachowania i obrony islamu, a nawet obietnice nagrody dla tych, którzy uznają religię objawioną w Koranie.

Jeszcze inny zespół przepisów, które miały wyraźny charakter nakazu religijnego, tworzyły wezwania do walki, wręcz wojny, za prawdziwą wiarę z jej wrogami. Pojawiły się nawet zachęty do męczeńskiej śmierci za wiarę, która miała zapewnić wiernemu bezpośrednią drogę do raju[11]. Apele wzywające do prowadzenia dżihadu w imię Allaha należy umieścić w grupie przepisów zawierających nakazy religijne wzywające do walki za wiarę.

Janusz Danecki twierdzi, że „dżihad" to jedno z najbardziej zagmatwanych i źle interpretowanych pojęć w kulturze europejskiej[12]. Identyczne stanowisko prezentuje irański szyita Seyyed Hossein Nasr, przekonując, że współcześnie na Zachodzie dżihad jest najbardziej szkalowanym i błędnie rozumianym pojęciem[13]. Przyczyną tych kontrowersji często może być przyjęta metodologia lub wyłącznie islamski bądź okcydentalny punkt widzenia. Muzułmańskie podejście, wspierane często przez autorów owładniętych metodologią politycznej poprawności, odrzuca wielowymiarowość i historyczny kontekst dżihadu, akcentując wyłącznie jego indywidualny i w zasadzie pacyfistyczny charakter. Autorzy ci podkreślają, że dżihad jest walką z własnymi słabościami po to, aby być lepszym muzułmaninem. Inni badacze z kolei wskazują na kolektywistyczny i zdecydowanie militarny charakter dżihadu i przez to określenie rozumieją wyłącznie ciążący na muzułmanach obowiązek walki z niewiernymi w celu rozszerzenia panowania islamu na całym świecie.

Próba wyjaśnienia wskazanych zawiłości i kontrowersji wymaga najpierw analizy pochodzenia i znaczenia pojęcia „dżihad".

Wspomniany już polski arabista J. Danecki przekonuje, że źródła błędnego rozumienia pojęcia „dżihad" tkwią głównie w tym, że często nie dostrzega się, że idea ta podlegała w islamie ewolucji i w różnym czasie była odmiennie interpretowana. Inne fałszywe założenie było konsekwencją ujmowania dżihadu wyłącznie w kategoriach

---

[10] J. Hauziński, *Dżihad we wczesnoislamskiej ideologii ekspansji*, „Zeszyty Naukowe Uniwersytetu Jagiellońskiego – Prace Historyczne" 1992, nr 102, s. 17 oraz G. Minois, *Kościół i wojna. Od Biblii do ery atomowej*, Warszawa 1998, Bellona, s. 89.

[11] J. Nosowski, *Przepisy prawne Koranu,* Warszawa 1971, s. 38–39. Jak dopowiada ten autor, sugestie uzupełnione są przestrogami zwróconymi do tych, którzy odrzucają treść objawienia koranicznego, tamże.

[12] J. Danecki, *Podstawowe wiadomości o islamie,* Warszawa 2002, Dialog, s. 251. Można by zapytać, dlaczego tylko w kulturze europejskiej? A co z kulturą azjatycką czy amerykańską? Swoimi wywodami Danecki niezbyt przekonująco stara się rozwikłać wskazane problemy. Por. też M. Saïd al-Ashmawy, *Islam and the Political Order*, Washington 1994, s. 69.

[13] S.H. Nasr, *Istota islamu. Trwałe wartości dla ludzkości*, Warszawa 2010, PAX, s. 215.

walki religijnej i tłumaczone było na języki europejskie jako „święta wojna" bądź „wojna religijna". Autor ten dowodzi, że również współczesne pojmowanie dżihadu źle tłumaczy zarówno koraniczne, jak i późniejsze rozumienie tego pojęcia[14].

Danecki umieszcza dżihad w kontekście innego pojęcia, którego pochodzenie etymologiczne jest podobne – *qital*. Termin „*qital*" oznacza walkę zbrojną, bicie się, zwalczanie innych. Z tych względów dżihad oznaczający dokładanie starań, podejmowanie wysiłków dla osiągnięcia jakiegoś celu jest terminem szerszym, w którego zakres znaczeniowy wchodzi *qital* – pojmowany jako walka zbrojna[15]. Zdaniem autora *Podstawowych wiadomości o islamie* w Koranie *qital* oznaczał zarówno walkę zaczepną, jak i obronną i zwykle występował w kontekście oznaczającym, że wyznawcy islamu podejmują walkę z największą odrazą[16].

Pozostawienie przez wytrawnego znawcę tematu takiej konstatacji bez szerszego komentarza może nieco zdumiewać, dla wojowniczych Beduinów bowiem, zarówno przed islamem, jak i później, wojna była istotą życia[17]. W ocenie Daneckiego *qital* miałby być walką obronną. Trudno jednak przyjąć tak jednoznaczną interpretację, ponieważ gwałt i przemoc były jednymi z podstawowych sposobów działania muzułmanów u zarania ich religii[18]. Warto w tym miejscu podkreślić, że po raz pierwszy (zwraca na to uwagę współczesny autor muzułmański Tariq Ramadan, wnuk Hassana al-Bany, założyciela Bractwa Muzułmańskiego) termin „dżihad" pojawia się w Koranie w surze XXV, ajat 52[19] i brzmi: *Nie słuchaj więc niewiernych i zwalczaj ich z wielkim zapałem, przy jego pomocy* [Koranu – przyp. aut. art.]. Tym samym nie do końca można zgodzić się ze stwierdzeniem, że wezwanie do walki przeciwko niewiernym ma charakter zmagań z własnymi słabościami.

Wracając do etymologii: termin „dżihad" występujący w Koranie jest masdarem (rzeczownikiem odsłownym) od *gahada* i początkowo znaczył: „podejmowanie wysiłku", „dokładanie starań" dla osiągnięcia jakiegoś celu. Osnowa *ĝ h d* oznacza:

---

[14] J. Danecki *Podstawowe wiadomości...,* s. 251–252. Por. też tenże, *Kłopoty z dżihadem,* w: *Islam a terroryzm,* A. Parzymies (red.), Warszawa 2003, Dialog, s. 45–58. W artykule tym autor prezentuje bardziej zróżnicowane stanowisko w kwestii dżihadu niż w swoich wcześniejszych publikacjach.

[15] Na oznaczenie walki zbrojnej prowadzonej w celu zabicia lub podporządkowania sobie przeciwnika Koran używa określenia *qital*, które pojawia się w tej księdze 33 razy. Z kolei termin „*harb"* oznaczający atak zbrojny lub walkę z niewiernymi występuje 6 razy. Natomiast termin „dżihad", rozumiany jako walka ze złem na wiele sposobów: sercem, językiem, piórem, ręką, ale też i mieczem, pojawia się 28 razy, por. M. Elass, *Co tak naprawdę mówi Koran. Chrześcijański przewodnik po świętej księdze islamu,* Warszawa 2009, Kefas, s. 186.

[16] Tamże, s. 252. Danecki przytacza tutaj surę II ajat 215: *zapisana wam została walka, choć jest ona wam wstrętna*. W przekładzie Bielawskiego jest to ajat 216 i brzmi on następująco: *przepisana wam jest walka, chociaż jest wam nienawistna*. A dalsze słowa: *Być może, czujecie wstręt do jakiejś rzeczy, choć jest dla was dobra*, można różnie interpretować, nawet jako zachętę do uczestnictwa w akcjach zbrojnych.

[17] Sam Danecki o okresie przedislamskim pisze: *Wojny międzyplemienne stanowiły charakterystyczną cechę życia tamtych czasów*, tenże, *Arabowie*, Warszawa 2001, PIW, s. 64. Można dopowiedzieć, że walki międzyplemienne i najazdy rabunkowe nie ustały również w pierwszych dziesięcioleciach islamu.

[18] Por. S.K. Samir, *Islam. 100 pytań*, w: G. Paolucci, C. Eid, *Islam. Sto pytań, Odpowiada Samir Khalil Samir*, Warszawa 2004, Pax, s. 37. Co znamienne, nawet bractwa sufickie (sufiowie to potoczne określenie należących do nich muzułmańskich mistyków) wywierały wpływ na politykę państw i władców, a także brały udział w wojnach, por. Z. Landowski, *Sufizm. Podstawowe informacje*, Warszawa 2010, TRIO, s. 56.

[19] T. Ramadan, *Śladami Proroka. Lekcje z życia Muhammada*, Wrocław 2011, Instytut Studiów nad Islamem, s. 60, s. 114. T. Ramadan przytacza nieco inne tłumaczenie słów Koranu i dokonuje odmiennej ich interpretacji, przekonując, że pierwotne i podstawowe rozumienie dżihadu oznacza *podejmowanie wysiłku, również „podejmowanie oporu"* rozumianego jako sprzeciw wobec ucisku i prześladowania, tamże, s. 61.

starać się, ubiegać, wytężać (siły), natężać się, dążyć do czegoś, walczyć o coś. W znaczeniu praktycznym i historycznym termin ten znaczy: prowadzić świętą wojnę przeciwko niewiernym, zatem dżihad oznacza walkę, świętą wojnę za wiarę, która jest obowiązkiem muzułmanów. Tym samym pojęcie „walki na drodze Boga" otrzymuje w Koranie dwa znaczenia: *qatala* oraz *gahada*. W pierwszym z nich silniej akcentuje się walkę zbrojną, z kolei drugi posiada szersze, bardziej abstrakcyjne znaczenie, ponieważ mocniej wskazuje na duchowe zaangażowanie w krzewienie islamu[20].

Jak wskazano wyżej, pojęcie „dżihad" występuje w Koranie zwłaszcza w połączeniu z terminem „*qital*", który oznacza walkę zbrojną. Tym samym walka zbrojna jako treść terminu *qital* wchodzi w zakres znaczeniowy *dżihadu*, a muzułmanie pierwszych wieków przez dżihad rozumieli głównie działanie na rzecz islamu, także poprzez walkę zbrojną przeciwko niewiernym[21].

U źródeł arabskich podbojów militarnych leżały wyprawy wojskowe Mahometa, które pokazywały jego następcom, że walka zbrojna jest w pełni dopuszczalnym i ważnym elementem nowej religii, nie tylko w przypadku jej obrony, ale także ekspansji. Warto też zaakcentować, że działaniom podejmowanym przez Proroka daleko było do pokojowych tendencji, tak charakterystycznych dla chrześcijaństwa pierwszych wieków[22].

Równie zasadne wydaje się stanowisko głoszące, że termin „dżihad" jest skrótem *dżihad fi sabil Allah* i oznacza zmagania w imię Allaha, a różne opracowania w islamskich słownikach czy leksykonach wskazują, że był ustanowiony jako boska instytucja w szczególnym celu poszerzania panowania islamu[23]. Trudno jest zatem zgodzić się z wyłączną próbą rozumienia dżihadu jako walki z własnymi słabościami czy podejmowania wojny z największą odrazą.

Obowiązek dżihadu (świętej wojny) wyprowadzono ze słów Koranu: *Zwalczajcie na drodze Boga tych którzy was zwalczają, lecz nie bądźcie najeźdźcami* (...) *I zwalczajcie ich, aż ustanie prześladowanie i religia będzie należeć do Boga* (II, 190–194). W wezwaniu tym dostrzec można wyraźny nakaz walki, którą muzułmanie powinni podejmować z niewiernymi, a walka ta ma być toczona aż do chwili, gdy islam zapanuje nad światem.

Święta wojna, rozumiana jako zbrojna ekspansja wspólnoty muzułmańskiej, jest aktem „miłym Allahowi", ponieważ pozwala rozszerzyć jego panowanie o nowych wyznawców, ci zaś z niewiernych, którzy odrzucą islam i nie zechcą podporządkować się muzułmańskiej władzy, stracą życie. Dżihad jest także aktem politycznym, zapewnia muzułmanom bezpieczeństwo oraz pozwala na zdobycze materialne, a wojownicy, którzy polegli w świętej wojnie, trafiają prosto do nieba.

Jerzy Nosowski uważa, że *nakaz walki za wiarę i zwalczanie wrogów tej wiary możemy zaliczyć do przepisów prawa dotyczących zewnętrznego wyrażania tej wiary przez jej wyznawców.* Według niego nakazy te stały się usprawiedliwieniem dla prowadzonych jeszcze przez Muhammada łupieżczych napadów na jego ideowych i politycznych przeciwników, a po śmierci Muhammada były głównym i zasadniczym

[20] J. Nosowski, *Przepisy prawne*..., s. 43.

[21] K. Kościelniak, *Dżihad. Święta wojna w islamie*, Kraków 2002, Wydawnictwo M, s. 22–23.

[22] H. Kennedy, *Wielkie arabskie podboje. Jak ekspansja islamu zmieniła świat*, Warszawa 2011, PWN, s. 50. Należy dodać, że w dobie Mahometa rozprzestrzenianie się islamu na Półwyspie Arabskim częściej było efektem działań dyplomatycznych niż militarnych.

[23] A.C. McCarthy, *The Grand Jihad: How Islam and the Left Sabotage America*, New York 2010, Encounter Books, s. 52.

pretekstem do zgodnego z prawem prowadzenia wojen zdobywczych, do terytorialnej i ideologicznej ekspansji[24].

Przynależność do wspólnoty wiernych sprzyjała przekonaniu, że wyznawcy islamu mają obowiązek wzajemnej troski o swoje sumienia. Ponadto powinni chronić muzułmańską wspólnotę i rozszerzać jej panowanie wszędzie, gdzie jest to tylko możliwe.

Islamski dżihad skierowany był nie tylko przeciwko wrogom spoza muzułmańskiej społeczności, ale również przeciwko niewiernym wewnątrz niej. Nakaz udziału w tak rozumianym dżihadzie wyprowadzono z następujących słów Koranu: *O, wy którzy wierzycie! Zwalczajcie tych, którzy są blisko was* (IX, 123).

Obowiązek podejmowania dżihadu nie był indywidualną powinnością każdego muzułmanina, lecz uznawano go za obowiązek zbiorowy, ciążący na całej *ummie* (społeczności muzułmańskiej), która powinna zapewnić potrzebną liczbę żołnierzy. Z czasem, po zakończeniu wielkich muzułmańskich podbojów i przystąpieniu Europy do ofensywy, dżihad zaczęto pojmować jako obronę, a nie atak[25].

W tym miejscu warto zauważyć, że wszystkie chronione prawem muzułmańskim przywileje i interesy dzieli się na dwie grupy: prawa Allaha i prawa indywidualne. Odpowiadają im dwie odmiany norm prawa muzułmańskiego. Wspólnie z nimi wydziela się nieraz i trzecią, która chroni prawa przynależne zarówno Allahowi, jak i osobom prywatnym. Co prawda szariat nie dokonuje rozróżnienia między życiem publicznym a prywatnym, ponieważ obejmuje wszystkie sfery stosunków międzyludzkich jako podległe prawu Allaha. Dzięki temu wzmacniane jest przekonanie, że normy te służą osiągnięciu celów islamu, czyli realizacji woli Allaha. Z tych względów najbardziej niebezpieczne przestępstwa kategorii hudud[26] są rozpatrywane jako naruszenie praw Allaha, przez które rozumie się naruszenie interesów całej społeczności muzułmańskiej. Do tej grupy przestępstw zalicza się m.in.: bunt, rozbój, apostazję, szpiegostwo, kradzież, cudzołóstwo, spożywanie alkoholu, a więc nie tylko niewypełnianie obowiązków religijnych (w rozumieniu religii takie zaniedbania są rzeczywiście przeciwne woli Allaha)[27], ale zwłaszcza czyny skierowane na szkodę muzułmańskiej społeczności. W powyższym kontekście uchylanie się od dżihadu byłoby uznane za zamach na „prawa Allaha".

Bernard Lewis twierdzi, że pozytywnym obowiązkiem przewidzianym przez prawników islamskich był dżihad rozumiany jako powinność całej wspólnoty muzułmańskiej w przypadku ataku, w przypadku obrony zaś jako powinność każdego muzułmanina z osobna. Samo pojęcie „dżihad", chociaż jest tłumaczone jako święta

[24] Por. J. Nosowski, *Przepisy prawne*..., s. 51–52.

[25] A. Hourani, *Historia Arabów*, s. 157. Analogicznie postrzegają obowiązek dżihadu J. i D. Sourdel dowodząc, że wojna sprawiedliwa, zwana świętą wojną, polegała na stałej walce z niewiernymi, aż do momentu, w którym nawrócą się oni na islam lub nie zaakceptują jego władzy. Obowiązek prowadzenia wojny z niewiernymi był oprócz *arkan ad din* obowiązkiem zbiorowym i odegrał istotną rolę w dziejach islamu, zwłaszcza w jego kontaktach ze światem niemuzułmańskim, por. J. i D. Sourdel, *Cywilizacja islamu (VII-XIII w.)*, Warszawa 1980, PIW, s. 121.

[26] Szeroko na temat najnowszej literatury dotyczącej tej kategorii przestępstw por. Ch.S. Warren, *Islamic Criminal Law. Oxford Bibliographies Online Research Guide,* Oxford 2010.

[27] N. Abiad, *Sharia, Muslim states and international human rights treaty obligations: a comparative study*, London 2008, s. 22.

wojna, to w rozumieniu koranicznym oznacza „dążenie ścieżką Boga" (*fi sabil Allah*)[28]. Część współczesnych autorów, nie tylko muzułmańskich, przekonuje, że dżihad to wyłącznie podążanie ścieżką Boga w sensie duchowym i moralnym[29]. Na poparcie tezy, że dżihad oznacza zmaganie się z własnymi słabościami i chęć zostania lepszym człowiekiem, współczesny europejski muzułmanin, Tariq Ramadan, przytacza następujące słowa (zdaniem autora artykułu warto je zacytować w całości, ponieważ najlepiej prezentują analizowane stanowisko): *Powracając z wyprawy do Hunajn, Prorok oznajmił: Powracamy z mniejszego dżihadu (wysiłek, opór, walka o zmiany na lepsze), aby podjąć większy dżihad. Towarzysze zapytali: Czym jest większy dżihad Posłańcu Boga? Odpowiedział: To walka z samym sobą (ego)*[30].

Warto jednak wiedzieć, że zdecydowana większość klasycznych uczonych islamskich odnosząc się do odpowiednich fragmentów Koranu i sunny analizowała dżihad z militarnego punktu widzenia[31].

Ojciec muzułmańskiego prawa międzynarodowego – Muhammad ibn al-Hasan al-Shaybani (749/50–805) stwierdził, że *Allah dał Prorokowi cztery miecze do walki z niewiernymi: pierwszy do walki z politeistami, z którymi walczył sam Mahomet, drugi dla zwalczania apostatów, których zwalczał kalif Abu Bakr, trzeci do walki z Ludami Księgi, z którymi walczył Umar, a czwarty na dysydentów, których zwalczał kalif Ali*[32].

Wspomniany wcześniej Al-Ghazali apelował o udział w dżihadzie przynajmniej raz w roku, mając na myśli walkę z niewiernymi, głosił bowiem: *...każdy musi wziąć udział w dżihadzie przynajmniej raz do roku... Wolno użyć katapulty przeciw nim* [niemuzułmanom – przyp. aut. art.]*, kiedy są w fortecy, nawet jeśli są wśród nich kobiety i dzieci. Wolno ich podpalić i/lub utopić...*[33]

Podobne stanowisko prezentował Abūl-Walīd Muhammad bin Ahmad bin Rušd, w Europie znany lepiej jako Awerroes (1126–1198), muzułmański uczony z arabskiej Hiszpanii, który wskazywał, że dżihad jest obowiązkiem kolektywnym, a nie indywidualnym, a każdy muzułmanin, który weźmie w nim udział i poniesie śmierć, trafi do raju. W takim kontekście należy odczytywać analizę Awerroesa dotyczącą interpretacji wersetów 95–100 z IV sury Koranu[34]. Śmierć w imię Allaha zatem w trakcie dżihadu

---

[28] Szerzej o tej kwestii por. R. Peters, *Jihad in Classical and Modern Islam,* s. 197, a także J.R. Willis, *In the Path of Allah: The Passion of Al-Hajj 'Umar: an Essay Into the Nature of Charisma in Islam*, London 1989, s. 29–56.

[29] W tym duchu prezentuje dżihad m.in. Tariq Ramadan, który przekonuje, że stały wzór dla muzułmanów wszystkich czasów – Mahomet – *Prowadzony przez swojego nauczyciela, stawiał opór temu, co w nim samym było najgorsze i ofiarował to, co było w nim najlepsze, gdyż takie było znaczenie dżihadu*, tenże, *Śladami Proroka...*, s. 247.

[30] Tamże, s. 224. Ramadan w przypisie wskazuje jedynie, że hadis ten został przekazany przez al-Bajhaqiego, ale nie podaje źródła tej wypowiedzi Mahometa w sposób bardziej naukowy. Warto zauważyć, że wiele hadisów, które przytacza ten autor, nie wskazuje dokładnie źródła, z którego pochodzi przytaczany tekst. Jest to istotny mankament tej pracy.

[31] B. Lewis, *Muzułmański Bliski Wschód*, Gdańsk 2003, Marabut, s. 220. Ciekawy, sumaryczny przegląd stanowisk myśli klasycznego islamu wobec dżihadu por. H.A. Haleem, *The Crescent and the Cross: Muslim and Christian Approaches to War and Peace*, New York 1998, MacMillan, s. 60–81.

[32] M. Khadduri, *War and Peace in the Law of Islam,* Baltimore 1955, Johns Hopkins Press, s. 74.

[33] Zob. przypis 2.

[34] Por. Awerroes, *The Chapter of Jihad from Averroes Legal Handbook Al-Bidayah,* w: *Jihad in Mediaeval and Modern Islam: The Chapter on Jihad from Averroes' Legal Handbook 'Bidāyat Al-mudjtahid' and the Treatise 'Koran and Fighting' by the Late Shaykh-al-Azhar, Mahmūd Shaltūt,* t. 5, tłum.R. Peters, Leiden 1977, s. 9. Odpowiednie słowa Koranu brzmią następująco: *Wywyższył Bóg gorliwie walczących swoimi dobrami i swoim życiem nad tych, którzy siedzą spokojnie, o jeden stopień.* (II, 95). *A kto wędruje*

jest najlepszą przepustką do raju[35], zresztą Koran przewiduje dla uczestników walki w imię Allaha także nagrody w życiu doczesnym, przyznając im łupy wojenne. Ci wszyscy natomiast, którzy polegli na „ścieżce Boga" zostają szahidami – męczennikami za wiarę – i idą prosto do raju. To właśnie w czasach arabskich podbojów za najwyższe świadectwo wiary muzułmanina w doktrynie muzułmańskiej uznano śmierć wiernego poniesioną w dżihadzie, wojnie w imię Boga. Podejście to potwierdzają liczne hadisy, które wskazują na wiele przywilejów przyznawanych męczennikom za wiarę[36]. Współcześni wyznawcy idei dżihadu rozumianego jako święta wojna z niewiernymi w celu poszerzenia panowania islamu, w pełni podzielają powyższe stanowisko i w imię realizacji swoich przekonań godzą się na ofiarę złożoną z własnego życia, wierząc, że czeka ich obiecana nagroda w raju.

Znamienne i warte szczególnego podkreślenia w tym miejscu jest to, że męczennikami w chrześcijaństwie były osoby, które ginęły w imię swojej wiary, pokornie godząc się na śmierć. W islamie męczennikami zostają zaś ci, którzy z bronią w ręku walczą w obronie swojej religii lub w celu jej ekspansji. Chrześcijański męczennik nie używał przemocy i był bezbronny, w islamie męczennikiem jest zaś ten, kto ginie z bronią w ręku, chociaż szariat uznaje również „niewalczących" męczenników.

Wspomniany już ibn Tajmijja twierdził, że powinnością wszystkich muzułmanów jest odpieranie najeźdźców, a także wszystkich odstępców od wiary. Dokonywać tego można przemocą w imię dżihadu, czyli świętej wojny. Według ibn Tajmijji dżihad powinien być skierowany nie tylko przeciwko heretykom, hipokrytom, apostatom czy niewiernym (wliczając żydów i chrześcijan), ale także przeciwko wszystkim muzułmanom, którzy nie chcą uczestniczyć w dżihadzie. Zarysowana przez niego koncepcja ukazywała stosunek islamu do świata niewiernych. Osadzała się ona na założeniu, że prawdziwy pokój i sprawiedliwy porządek społeczny zapanują na świecie dopiero wtedy, gdy islam odniesie zupełne zwycięstwo nad resztą świata. Muzułmanie nie mogą spocząć, aż do ostatecznego triumfu, ponieważ wszystkie inne religie i ideologie pragną pokonać islam i dążą do jego unicestwienia[37].

Z kolei wielki muzułmański myśliciel Ibn Chaldun[38] przekonywał w swoim sławnym dziele *Mukaddima*, że *W społeczności muzułmańskiej święta wojna jest*

na drodze Boga, ten znajdzie na ziemi liczne miejsca schronienia, rozległe. A kto wyjdzie ze swojego domu i wywędruje ku Bogu i Jego Posłańcowi, a potem dosięgnie go śmierć – to nagroda jego będzie u Boga (IV, 100).

[35] M. Khadduri, *Translators Introduction,* w: *The Islamic Law of Nations: Shaybānī's Siyar*, Baltimore 1966, Johns Hopkins Press, s. 15.

[36] S. Surdykowska, *Idea szahadatu w kulturze Iranu*, Warszawa 2006, Wydawnictwa Uniwersytetu Warszawskiego, s. 46.

[37] Por. M. Habeck, *Knowing the Enemy: Jihadist Ideology and the War on Terror*, New Haven–London 2006, Yale University Press, s. 21, a także W. Laqueur, *No End to War: Terrorism in the Twenty-First Century*, New York 2004, Continuum, s. 85.

[38] Chaldun Ibn Wali ad-Din`Abdar-Rahman (1332–1406). Wybitny średniowieczny humanista, historyk, historiozof, dyplomata i polityk arabski. Był nie tylko uczonym, ale brał również aktywny udział w życiu politycznym świata arabskiego swoich czasów jako dyplomata czy dowódca wojskowy. W czasie swoich misji dyplomatycznych spotykał się m.in. z królem Hiszpanii Piotrem Srogim i potężnym władcą mongolskim Tamerlanem. Odnosząc się do kwestii ustrojowo-politycznych, Ibn Chaldun przekonywał, że polityczny nierząd osłabia rozwój ekonomiczny kraju. Jako pierwszy stworzył w cywilizacji muzułmańskiej nową naukę o społeczeństwie, którą nazwał *ilm al-`uran* – nauka o społeczeństwie i kulturze ludzkiej.

obowiązkiem religijnym z powodu uniwersalności muzułmańskiej misji (i obowiązku) nawracania na islam poprzez perswazję lub użycie siły[39].

Należy w tym miejscu podkreślić, że tylko ten rodzaj wojny (dżihad) był sankcjonowany przez szariat, a wojna ta była nazywana wojną przeciwko niewiernym[40].

Wszystkie podręczniki prawa muzułmańskiego posiadały rozdziały omawiające dżihad pod kątem rozpoczęcia, prowadzenia i zakończenia działań zbrojnych, a także traktujące o kwestiach związanych z podziałem łupów wojennych. Warto przypomnieć, że jedna z sur Koranu (VIII) nosi tytuł *Łupy* i w dużej części jest poświęcona temu właśnie zagadnieniu. W ocenie autora artykułu niezwykle trudno byłoby uzasadnić kwestie regulujące podział łupów wojennych w kontekście wskazówek dotyczących duchowej walki z własnymi słabościami.

Ustalając reguły dżihadu, szariat nakazywał dobrze traktować tych, którzy nie brali udziału w walce, ale jednocześnie przyznawał zwycięzcom wiele praw wobec majątku podbitych i pokonanych, a także ich rodzin[41]. W kwestii zasad i warunków prowadzenia dżihadu muzułmańscy prawnicy często prezentowali różne stanowiska, jednak byli jednomyślni w fundamentalnej kwestii rozumienia dżihadu jako wojny toczonej z niewiernymi dla poszerzenia panowania islamu.

W klasycznym islamie dżihad rozumiany jako wojna z niewiernymi w celu poszerzenia panowania islamu jest religijnym obowiązkiem nałożonym na wiernego. Kiedy kraj niewiernych zostanie przejęty przez muzułmańskiego władcę, jego mieszkańcom są oferowane trzy możliwości. Po pierwsze: mogą oni przyjąć islam i stać się pełnoprawnymi obywatelami muzułmańskiego państwa, po drugie: mają możliwość zapłacenia podatku – *dżizja*, dzięki któremu niewierni kupują sobie opiekę islamu stając się *dhimmi*, jednak pod warunkiem, że nie są bałwochwalcami z Arabii, i po trzecie wreszcie: mają prawo wybrać śmierć od miecza; dotyczy to także tych, którzy nie chcą płacić *dżizja*. Dżihad podejmowany przez wyznawców Allaha uchodził za obowiązek religijny, który będzie trwał do czasu, dopóki cały świat nie zaakceptuje wiary muzułmańskiej albo nie uzna władzy muzułmanów. Ten ostatni przypadek dotyczył jedynie wyznawców tzw. ludów księgi, tj. chrześcijan i żydów, którzy po opłaceniu dodatkowych podatków i ukorzeniu się, mogli pozostać przy swojej wierze. Politeiści mogli wybierać jedynie między islamem lub śmiercią czy niewolą. Szariat zezwalał tym samym na prowadzenie wojny zarówno przeciwko niewiernym, jak i tym wiernym, którzy odstąpili od wiary. Prawo to wskazuje cztery kategorie ludzi, z którymi walczą muzułmanie: niewiernych, odstępców od wiary, buntowników i rozbójników[42], ale dżihad reguluje tylko dwa pierwsze, przyznając zwycięzcom szczególne prawa. Jako przykład można wskazać, że niemuzułmanów można brać do niewoli, lecz nie można tego dokonać w przypadku pokonanych rozbójników muzułmanów.

Należy zauważyć, że koncepcja świętej wojny jako walki toczonej w imię Boga i religii była znana na Bliskim Wschodzie już przed islamem, a odwołania do niej można znaleźć w Księdze Powtórzonego Prawa i Księdze Sędziów. Z idei tej korzystali także autorzy bizantyjscy, uzasadniając walki z Persami i wojny obronne z Arabami i Turkami.

---

[39] Cyt. za: G.J. Cutler, *Devoutly Violent or Nominally Peaceful? The Justification for Violence in Islam*, Virginia Beach 2008, s. 59.

[40] Por. R. Peters, *Introduction,* w: *Jihad in Mediaeval and Modern Islam: The Chapter on Jihad from Averroes' Legal Handbook*, s. 3.

[41] B. Lewis, *Muzułmański Bliski Wschód...*, s. 220.

[42] M. Khadduri, *War and Peace...* s. 74.

Warto jednak pamiętać, że były to wojny o ograniczonych celach, a ich konsekwencją miało być podbicie Ziemi Obiecanej i obrona chrześcijaństwa przed atakami pogan[43]. W przypadku islamskiego dżihadu chodzi o rozprzestrzenienie panowania islamu na cały świat, które nie musi polegać wyłącznie na nawracaniu siłą, lecz może być dokonywane przez usuwanie przeszkód w nawracaniu się na islam. Należy przypomnieć, że chrześcijaństwo uzyskało potęgę świecką i militarną dzięki oddolnym przemianom istniejącego wcześniej mocarstwa, islam zaś od zarania powstawał dzięki zbrojnym podbojom dokonywanym przez swoich wojowniczych wyznawców.

Co znamienne, nawet chrześcijańskie krucjaty, często utożsamiane z islamskim dżihadem, były jedynie spóźnioną i ograniczoną odpowiedzią na militarne zdobycze islamu. W przeciwieństwie do muzułmańskiej świętej wojny celem krucjat była obrona albo odzyskanie obszarów utraconych przez chrześcijan, ich podłożem zaś był entuzjazm religijny, a nie chęć podboju świata islamu[44].

Należy podkreślić, że współcześni zwolennicy dżihadu jako świętej wojny z niewiernymi dosłownie interpretują wersety Koranu, opierając się na literze świętej dla nich księgi i rezygnują z innej wykładni. Wyszukują w Koranie wersety, które są zgodne z ich postrzeganiem rzeczywistości, a inne odrzucają lub nadają im własną interpretację[45]. Polityczna interpretacja klasycznej doktryny jest oparta na założeniu, że islam odniesie ostateczne zwycięstwo. Islamscy prawnicy doby klasycznej (a wielu współczesnych również podziela ten pogląd) przekonywali, że świat jest podzielony na Świat (Dom) Islamu (*Dar al-Islam*) i Świat (Dom) Wojny (*Dar al-Harb*). Ponieważ jedynym prawowitym suwerenem jest Bóg, a jedyną słuszną formą rządów jest władza sprawowana na podstawie islamu i szariatu, to władcy Świata Wojny są zatem nieuprawnionymi do władzy uzurpatorami, dlatego też normalnym stanem rzeczy pomiędzy obu stronami jest wojna. W klasycznej doktrynie średniowiecznej przywódca państwa muzułmańskiego, tj. imam (kalif), może co najwyżej zawrzeć rozejm z przywódcami panującymi nad terytorium wojny maksymalnie na dziesięć lat, ale nie może zawrzeć trwałego pokoju. Dżihad nie miał na celu natychmiastowego nawrócenia na islam wszystkich narodów, ale raczej dążył do zapewnienia panowania Boga i jego prawa – szariatu – nad całym światem, zgodnie z koranicznym nakazem *Zwalczajcie ich, aż nie będzie już buntu i religia w całości będzie należeć do Boga* (VIII, 39).

Wielu współczesnych muzułmanów, odwołując się do terminu „dżihad", nie nadaje mu znaczenia duchowego czy pacyfistycznego, a raczej podkreśla agresywność działań i ich militarny charakter. Zarówno na płaszczyźnie socjologicznej, jak i historycznej, w odwołaniu do Koranu pojęcie to jest jednoznaczne i mówi o wojnie muzułmanów prowadzonej w imię Boga w obronie islamu lub w celu jego rozpowszechniania. Gdy władca muzułmański chce wypowiedzieć wojnę innemu krajowi islamskiemu, musi wcześniej wykazać jego niewiarę, gdyż według prawa islamskiego niedozwolona jest wojna prowadzona przeciwko braciom w wierze. Po takiej deklaracji wojna staje się dozwolona i ma charakter nieunikniony. Gdy Mahomet wypowiadał wojnę, wcześniej trzykrotnie składał swoim wrogom propozycję przyjęcia islamu, a kiedy nie wyrażali na to zgody, rozpoczynał przeciwko nim działania militarne. Współczesną ilustracją tej sytuacji może być konflikt iracko-irański, który odwoływał się do tego schematu.

---

[43] Por. B. Lewis, *Muzułmański Bliski Wschód...*, s. 221.

[44] Por. M.T. Zahajkiewicz, *Wojny w imię Boga? Jak spoglądać na średniowieczne wyprawy krzyżowe*, w: *Problemy współczesnego Kościoła*, M. Rusecki (red.), Lublin 1996, RW KUL, s. 310.

[45] W. Dietl, K. Hirschmann, R. Tophoven, *Terroryzm,* Warszawa 2009, PWN, s. 120.

Również sytuacja w Zatoce Perskiej jest analogiczna do postępowania Proroka w VII wieku, gdyż każda ze stron konfliktu ogłaszała siebie jako obrońcę islamu, a stronę przeciwną jako *kafir*, czyli niewierną[46].

Także muzułmańscy terroryści przekonują, że ich działalność jest oparta na wartościach islamu, a dżihad jest uprawnioną formą działania, której głównym celem jest zaprowadzenie islamskiego porządku opartego na szariacie. Ataki terrorystyczne mają być wymierzone tak samo w wojskowych, jak i w cywilów, ich celem jest zwłaszcza każdy Amerykanin oraz każdy jego sojusznik. Taki właśnie nakaz religijny wydano w 1998 r. podczas posiedzenia Światowego Frontu Islamskiego. Jego uczestnicy podzielali przekonanie, że im większa liczba ofiar, tym większa chwała dla Allaha[47].

Najważniejszym źródłem poznania doktryny i praktyki dżihadu jest Koran – uważany przez muzułmanów za dosłowny przekaz Boga dany światu za pośrednictwem proroka Mahometa[48]. Drugie po Koranie źródło muzułmańskiego prawa to Sunna, którą tworzą zbiory hadisów, to jest wypowiedzi, czynów i zachowań Mahometa. Niektóre z nich obrazują wprost postrzeganie dżihadu w klasycznym islamie jako walki zbrojnej, np. hadisy głoszące, że *raj leży w cieniu mieczy*, a dżihad jest obowiązkiem za panowania każdego władcy, zarówno pobożnego, jak i tyrana[49]. Najbardziej poważane zbiory przepisów, w tym zwłaszcza Sahih Buchari, zawierają wiele odniesień do dżihadu rozumianego jako zbrojna walka z niemuzułmanami[50].

Święta wojna za wiarę stanowi często dominujący problem w historii islamu, zwłaszcza na jego rubieżach, ponieważ żyjące tam ludy niosły nowo przyjętą wiarę za pomocą miecza[51]. Należy w tym miejscu podkreślić, że wojna i ekspansja terytorialna były priorytetem dla władców wczesnego państwa islamskiego, a islamscy juryści szybko zajęli się kwestią indywidualnego uczestnictwa wiernych w tym wydarzeniu. Pojawiło się pytanie: czy dżihad jest obowiązkiem, który każdy muzułmanin musi wykonać jak najlepiej, tak jak pielgrzymkę czy codzienną modlitwę? Istniała powszechna zgoda, że wstąpienie na ochotnika do armii jest czynem chwalebnym. Z praktycznego, wojskowego punktu widzenia ci niezdyscyplinowani ochotnicy mogli jednak przysporzyć więcej szkody niż pożytku. W prawie islamskim problem został rozwiązany poprzez wypracowanie przez doktrynę zasady „obowiązku zgodnie z potrzebą", co było zasługą wielkiego prawnika Abu Abdullaha Muhammada ibn Idrisa al-Shafi'iego (767–820), twórcy jednej z czterech sunnickich szkół prawa. Według tej koncepcji obowiązek dżihadu można uznać za spełniony dopóty, dopóki istnieje wystarczająca liczba ochot-

---

[46] S.K. Samir, *Islam. Sto pytań...*, s. 35–36.

[47] I. Witkowski, *Supertajne bronie islamu*, Warszawa 1999, WIS, s. 98.

[48] W Koranie występuje ponad dwieście wersetów dotyczących walki w imię Boga, por. M.A. Khan, *Islamic Jihad: A Legacy of Forced Conversion, Imperialism and Slavery,* New York 2009, s. 2.

[49] A.M. al-Hindi, *Kanz al-`Ummal*, cz. I, cyt. za*:* B. Lewis, *Muzułmański Bliski Wschód*, s. 221.

[50] W Sahih Buchari znajduje się 288 odwołań dotyczących walki w imię Allaha, por. http://www.searchtruth.com/book_display.php?book=52&translator=1&start=0&number=0 [dostęp: 17 VI 2012], w Sahih Muslim można znaleźć 81 odwołań do dżihadu, por. http://www.searchtruth.com/book_display.php?book=19&translator=2&start=0&number=0 [dostęp: 17 VI 2012], w sunnie zaś Abu Dawud – 179 odniesień do dżihadu, por. http://www.searchtruth.com/book_display.php?book=14&translator=3&start=0&number=0 [dostęp: 17 VI 2012].

[51] B. Lewis, *Muzułmański Bliski Wschód*, s. 222. Z czasem pojawiła się nawet pewna specyficzna odmiana dżihadu – dżihad ribat – na oznaczenie walki prowadzonej przez tych wiernych, którzy strzegą twierdz na obrzeżach islamu, przebywając w nich określony czas lub całe życie. „Ribat" to arabski termin oznaczający małą przygraniczną fortyfikację.

ników do jego wypełnienia. Jeśli jednak armie wroga nagłym najazdem zagrożą ziemi islamu, to obowiązek ten spoczywa na każdym muzułmaninie[52].

Współcześnie wielu uczonych, nie tylko muzułmańskich, ale także zachodnich, skłania się ku poglądowi, że dżihad to raczej walka duchowa i dlatego należy wyróżnić mały dżihad – *dżihad asghar* i wielki dżihad – *dżihad akbar*. Niekiedy nazywa się te rodzaje dżihadu odpowiednio: zewnętrzny i wewnętrzny dżihad, albo wyższy i niższy. Przez wielki dżihad należy rozumieć zmagania z własnymi słabościami i wadami, zatem odwołuje się on do wartości etycznych i duchowych. Z kolei mały dżihad to święta wojna toczona z niewiernymi w imię Allaha prowadzona w celu poszerzenia panowania islamu.

Zdaniem S.K. Samira interpretacja odwołująca się głównie do walki duchowej jest sprzeczna z islamską tradycją i współczesnym językiem. Należy bowiem z całą mocą podkreślić, że wszystkie ugrupowania muzułmańskie odwołujące się do terminu dzihad akcentują agresywność działań, a unikają skojarzeń mistycznych[53]. Wielu muzułmańskich przywódców religijnych, a także setki islamskich wydawnictw ostatnich lat traktują dżihad jako świętą wojnę w imię islamu, mając na myśli ekspansję tej religii w każdy możliwy sposób, z pełną aprobatą przemocy, włączając w to zamachy samobójcze podejmowane przez walczących w imię Allaha.

Ideolodzy Al-Kaidy odwołują się wprost do rozważań wspominanego ibn Tajmijji, który głosił, że *zgodna z prawem wojna jest zasadniczo dżihadem, którego celem jest udowodnienie, że religia należy całkowicie do Allaha, a jego słowo jest najważniejsze, dlatego według wszystkich muzułmanów ci, którzy stoją na drodze do tego celu, muszą być zwalczani*[54].

Podobnie jak ten średniowieczny uczony, również wielu współczesnych i wpływowych myślicieli muzułmańskich akcentuje agresywny i militarny aspekt dżihadu. I tak Sayyid Abul Ala Maududi przekonywał: *Islam chce zniszczyć wszelkie istniejące państwa i systemy rządowe, które sprzeciwiają się ideologii i celom islamu, niezależnie od krajów czy narodów, jakich dotyczy. Celem islamu jest ustanowienie państwa opartego na jego własnej koncepcji i ideologii, niezależnie od tego, jaki naród miałby tę wizję przyjąć, ani od tego, z obaleniem jakiego rządu ustanowienie państwa muzułmańskiego miałoby się wiązać. Z tych rozważań wyłania się wniosek oczywisty: celem islamskiego dżihadu jest wyeliminowanie wszystkich systemów niemuzułmańskich i wprowadzenie w ich miejsce rządów opartych na islamie. W tych rewolucyjnych zapędach islam nie zamierza ograniczać się do jednego kraju czy nawet grupy państw. Celem islamu jest rewolucja na skalę światową*[55].

Z kolei Hasan al-Bana (1906–1949), prekursor współczesnego islamizmu, założyciel ugrupowania Braci Muzułmanów, które pragnie przejąć pełnię władzy we współczesnym Egipcie, sformułował credo Braci Muzułmanów: *Prorok jest naszym wodzem, Koran naszym prawem, dżihad jest nasza drogą, śmierć dla Allaha największą nadzieją*[56].

---

[52] Por. też M. Khadduri, *War and Peace*..., s. 83–85.

[53] S.K. Samir, *Islam. Sto pytań*..., s. 35.

[54] Cyt. za: M. Saīd Ramadān Būtī, *Jihad in Islam: how to understand & practise it*, Damascus 1995, s. 90.

[55] S.A. Ala Mududi, *Dżihad w islamie,* Bejrut 1980, s. 9, za: N. Darwish, *Okrucieństwo w majestacie prawa*..., s. 16.

[56] J. Gurule, *Unfanding terror: The Legal Response*..., s. 57.

Według Majida Khadduriego, jednego z wielkich dwudziestowiecznych muzułmańskich autorytetów w tej kwestii: dżihad to doktryna permanentnej walki, nieustającej wojny[57]. Podobne stanowisko zajmował Sayyid Qutb (1906–1966), czołowy teoretyk Bractwa Muzułmańskiego, dla którego dżihad był narzędziem rozprzestrzeniania wszelkimi możliwymi środkami nieustannej rewolucji społecznej[58]. Z kolei inny, współczesny islamski autor przekonuje, że dżihad jest pierwszą twierdzą islamskiej społeczności i świata islamu[59], mając zapewne na uwadze ideę głoszącą, że najlepszą obroną jest atak.

Interesującą rekapitulacją stosunku do dżihadu współczesnych muzułmanów mogą być poglądy Abd al-Salama Faraja (1954–1982), egipskiego teoretyka, który wyłożył swoje koncepcje w pracy *Al-Faridah al-Gha'ibah* (*Zaniedbany Obowiązek*). Książka ta odgrywa istotną rolę w rozwoju islamskiego ekstremizmu na przełomie XX i XXI wieku. Sam tytuł pracy wskazuje, że dżihad stał się, inaczej niż pięć filarów islamu, „zaniedbanym obowiązkiem" wśród współczesnych muzułmanów[60]. Autor pracy przekonywał, że zarówno Koran, jak i hadisy wzywały wyznawców islamu do walki na rzecz Boga. Według niego rozumienie dżihadu jako walki było i jest czymś, co muzułmanie powinni przyjmować dosłownie, nie jest to zatem walka z własnymi słabościami i dążenie do bycia pobożnym muzułmaninem, lecz raczej walka o ekspansję islamu w służbie Allahowi. Muzułmanie są powołani, aby być żołnierzami islamu, a prawdziwi żołnierze islamu są chętni do korzystania z wszelkich dostępnych środków w celu osiągnięcia swoich sprawiedliwych celów. Nagrodą w niebie dla męczenników będzie raj, a dla żyjących na ziemi – prawdziwe państwo islamskie, które powstanie w przyszłości na całej kuli ziemskiej[61].

Wydaje się, że stanowisko Faraja podziela wielu muzułmanów. Przekonują o tym dodatkowo działania podejmowane przez licznych współczesnych radykalnych wyznawców islamu, które niekiedy spotykają się z przychylną reakcją, a prawie zawsze z brakiem krytyki przez ogół umiarkowanych wyznawców Allaha. Należy wiedzieć, że zamachy terrorystyczne przeprowadzone przez odwołujących się do islamu sprawców rzadko spotykały się z potępieniem przez współwyznawców zamieszkujących kraje islamskie. Niekiedy nawet zabójców uznawano za bohaterów. W pogrzebie 22-letniego Shahzada Tanweera (urodzonego w Bradford w Anglii zamachowca z Londynu w 2005 r.) uczestniczyły w Pakistanie dziesiątki tysięcy ludzi, dla których był on szahidem – męczennikiem za wiarę (swoją drogą niezwykle interesujące byłyby zakrojone na szeroką skalę badania opinii publicznej w krajach islamskich dotyczące kwestii rozumienia pojęcia dżihad przez współczesnych wyznawców islamu).

Przykładem potwierdzającym powyższą tezę może być to, że najsłynniejszy zwolennik militarnego rozumienia dżihadu Osama bin Laden 23 sierpnia 1996 r.,

---

[57] M. Khadduri, *War and Peace*...., s. 64.

[58] Szerzej na temat jego poglądów por. J. Zdanowski, *Współczesna muzułmańska myśl społeczno-polityczna. Nurt Braci Muzułmanów,* Warszawa 2009, ASKON, s. 62–71, 130–136, 143–150, 159–166, 185–188, 194–196.

[59] M. Saīd Ramadān Būtī, *Jihad in Islam*..., s. 90.

[60] Po raz pierwszy książkę tę opublikowano w Kairze w 1980 r. Została ona rozprowadzona wśród zwolenników Braci Muzułmanów, a z czasem wywarła znaczny wpływ na liczne rzesze młodych wyznawców islamu. Faraj był zamieszany w zamordowanie prezydenta Egiptu Anwara Sadata i został stracony w 1982 r.

[61] Szerzej na temat poglądów Faraja por. D. Aaron, *In Their Own Words: Voices of Jihad*, Santa Monica 2008, RAND, s. 62–66.

otoczony żołnierzami Al-Kaidy i setkami bojowników islamskich z Algierii, Anglii, Egiptu, Libanu, Jemenu, Iranu, Pakistanu oraz Arabii Saudyjskiej, ogłosił *Deklarację dżihadu wobec Amerykanów okupujących kraj dwóch Świętych Miejsc*[62], rozumiejąc przez dżihad walkę zbrojną toczoną przez muzułmanów z niewiernymi.

Warto także pamiętać, że wiele obecnie działających islamskich ugrupowań ekstremistycznych w swojej nazwie używa terminu „dżihad", np.: Al-Dżihad z Egiptu, Międzynarodowy Islamski Front Dżihadu przeciwko Żydom i Chrześcijanom[63] czy Ruch Dżihad z Bangladeszu. Do zamachów w Londynie przyznała się nieznana wcześniej Tajna Organizacja Al-Kaidy Dżihad w Europie. Podobnie działający od 1982 r. w Libanie Hezbollah nazywany jest nie tylko Partią Boga, ale także i Islamskim Dżihadem lub Islamskim Dżihadem na rzecz Wyzwolenia Palestyny. Nie tylko na Bliskim Wschodzie, ale także w innych rejonach świata, jak np. w Azji czy w Afryce, działają islamskie ugrupowania wykorzystujące w swojej nazwie słowo dżihad[64]. Żadna z wymienionych organizacji nie rozumie dżihadu jako wewnętrznej walki toczonej z własnymi słabościami, ale pojmuje go jako zbrojną walkę z niewiernymi w celu rozszerzenia panowania islamu na cały świat. Również wielu muzułmańskich imamów, np. w Wielkiej Brytanii, Francji, Hiszpanii, Włoszech czy Niemczech, popiera takie rozumienie świętej wojny[65].

Współcześnie, w dobie dominacji poprawności politycznej, autorzy muzułmańscy, ale także bardzo wielu uczonych niemuzułmanów, próbuje przekonywać, że pojmowanie dżihadu jako zbrojnej walki w imię krzewienia islamu jest błędne i wynika z deformacji islamu i treści zawartych w Koranie. Autor niniejszego artykułu bardziej skłania się ku interpretacji zaproponowanej przez S.K. Samira, który dowodzi, że istnieją dwie możliwości odczytania Koranu i Sunny, zgodnie z zasadą interpretacji Koranu zwaną regułą „znoszącego i zniesionego", w myśl której Bóg wydając jakiekolwiek polecenie, może później wydać polecenie zmieniające to poprzednie. Wielu uczonych podejmowało to zagadnienie, ale niestety nie doszli oni do jednoznacznych ustaleń i dlatego ciągle możliwe są odmienne wykładnie treści koranicznych. Podobne stanowisko prezentuje wspomniany H. Kennedy, który zauważa, że Koran zawiera treści akcentujące pokojową argumentację i dyskusję z niemuzułmanami: *Wzywaj ku drodze twego Pana z mądrością i pięknym napomnieniem! Rozmawiaj z nimi w najlepszy sposób! Zaprawdę, twój Pan zna najlepiej tych, którzy zeszli z Jego drogi; i On zna najlepiej tych, którzy idą drogą prostą!* (XVI, 125), a z drugiej strony zawiera wezwania do znacznie bardziej wrogich i agresywnych działań wobec niewiernych, zwłaszcza ajat 5 sury IX, zwany wersetem miecza, który głosi: *A kiedy miną święte miesiące, wtedy zabijajcie bałwochwalców, tam gdzie ich znajdziecie; chwytajcie ich, oblegajcie i przygotowujcie dla nich wszelkie zasadzki! Ale jeśli oni się nawrócą i będą*

---

[62] P.L. Williams, *Al-Kaida. Międzynarodowy terroryzm, zorganizowana przestępczość i nadciągająca apokalipsa,* Poznań 2007, Zysk i S-ka, s. 69.

[63] J. Zawadzki, *Międzynarodowy terroryzm samobójczy główną koncepcją prowadzenia walki przez Al-Kaidę,* w: *Ewolucja terroryzmu na przełomie XX i XXI wieku,* M.J. Malinowski, R. Ożarowski, W. Grabowski (red.), Gdańsk 2009, Wydawnictwo Uniwersytetu Gdańskiego, s. 201.

[64] D. Duda, *Terroryzm islamski*, Kraków 2002, Wydawnictwo Uniwersytetu Jagiellońskiego, s. 45–67.

[65] Jako przykład można tu wskazać słynnego szejka Yousufaal-Qaradawi oraz imamów Abu Hamzę i Abu Katadę z Wielkiej Brytanii, imama Alego Ibrahima El Soudany, Egipcjanina deportowanego z Francji do swego rodzinnego kraju za „apologię dżihadu", hiszpańskiego imama meczetu w Léridzie Abdelwahaba Houzi, a także wielu innych.

odprawiać modlitwę, i dawać jałmużnę, to dajcie im wolną drogę. Zaprawdę, Bóg jest przebaczający, litościwy![66]

Przedstawić można zatem dwa stanowiska: jedno zachęcające do tolerancji i pokojowego rozstrzygania wszelkich sporów i drugie – równie uprawnione – wzywające do walki zbrojnej w celu krzewienia islamu. Co znamienne, oba stanowiska są poprawne z metodologicznego punktu widzenia. Główny problem polega bowiem na tym, że w islamie treści zawarte w Koranie, niezależnie od miejsca, w którym się znajdują, nigdy nie mogą utracić ważności. Muzułmanie uważają bowiem, że ich święta księga została podyktowana i dlatego nie można dokonywać jej interpretacji, tak jak czynią to np. chrześcijanie w przypadku Pisma Świętego. Z tych względów doktryna nie może rozwijać się po zredagowaniu Koranu, a wysiłek muzułmańskich jurystów skupił się na odpowiednim stosowaniu świętych tekstów w określonych sytuacjach. Ten odmienny stosunek chrześcijan i muzułmanów do treści zawartych w ich świętych księgach jest przyczyną tego, że islamscy prawnicy muszą nauczać, że wyborów życiowych należy dokonywać albo na podstawie koranicznego wezwania do tolerancji, albo wspomnianego wyżej „wersetu miecza", ponieważ żadnego ajatu Koranu nie można unieważnić.

Z tych względów, co warto podkreślić raz jeszcze, ciągle możliwe są dwie interpretacje: agresywna i pokojowa – obie uprawnione z metodologicznego punktu widzenia. Aby zlikwidować ten dualizm metodologiczny niezbędny byłby uznany przez wszystkich muzułmanów autorytet religijny, który wskazałby jedno rozstrzygnięcie, ponieważ jednak on nie istnieje, to rozwiązanie takie jest praktycznie niemożliwe[67].

W związku z powyższym ekstremiści mordują w imię szariatu i panowania islamu, a żaden muzułmanin nie może im powiedzieć: *Nie jesteście prawdziwymi wyznawcami islamu*, ale co najwyżej może jedynie stwierdzić: *Wasze rozumienie Koranu nie jest naszym*. To janusowe oblicze charakteryzuje islam od chwili powstania do dnia dzisiejszego. Z jednej strony cechuje go dżihad – walka zbrojna podejmowana w imię poszerzenia panowania islamu, a z drugiej – hasło głoszące, że *Nie ma przymusu w religii* (Koran, II, 256).

Opierajac się na przytoczonych powyżej stanowiskach, w pełni uprawniona jest konstatacja Daniela Pipesa, że dla większości muzułmanów we współczesnym świecie klasyczne pojęcie dżihadu wywołuje nadal duży rezonans wśród szerokich rzesz wyznawców islamu i ciągle aktualne są spostrzeżenia wybitnego francuskiego znawcy problematyki Alfreda Morabi, który w 1993 r. napisał, że agresywny i militarny dżihad wypracowany przez islamskich jurystów i teologów wciąż cieszy się sympatią wielu muzułmanów. Co prawda współcześni apologeci upiększają obraz tej religijnej powinności, malując ją tak, aby odpowiadała dzisiejszym normom praw człowieka, jednak wyznawcy Allaha nie uznają tych retuszy, ponieważ *Ogromna większość muzułmanów pozostaje nadal pod duchowym władaniem prawa* (...)*, którego kluczowym wymogiem jest żądanie, nie mówiąc już o nadziei, by Słowo Boga zatryumfowało wszędzie na świecie*[68].

Niektórzy znawcy problematyki przekonują, że idea dżihadu odgrywała doniosłą rolę zarówno w myśli politycznej islamu, jak i w życiu muzułmanów jedynie do lat

---

[66] H. Kennedy, *Wielkie arabskie podboje*..., s. 51.

[67] S.K. Samir, *Islam. Sto pytań*..., s. 40.

[68] Por. D. Pipes, *Jihad and the Professors,* Commentary, November 2002.

dwudziestych ubiegłego wieku[69]. W ocenie autora artykułu założenie to jest błędne, ponieważ i dzisiaj koncepcja ta, jak starano się wykazać powyżej, ponownie zyskuje na znaczeniu. G. Weigel przekonuje nawet, że muzułmański radykalizm dążący do konfrontacji z Zachodem w oparciu o ideę dżihadu nie powinien być określany „fundamentalizmem" ani „islamizmem", lecz należy nazwać go „dżihadyzmem"[70]. Wyznawcami tej ideologii są muzułmanie, których dążeniem jest stworzenie globalnego kalifatu – ogólnoświatowego państwa muzułmańskiego. Z kolei R.J. Neuhaus definiuje dżihadyzm jako *inspirowaną religijnie ideologię głoszącą, że użycie wszelkich dostępnych środków w celu opanowania całego świata przez islam jest obowiązkiem moralnym każdego muzułmanina*[71]. Można tutaj dopowiedzieć, że celem tej walki nie jest zmuszenie wszystkich niewiernych do przyjęcia islamu, ale dążenie do wprowadzenia szariatu na całej ziemi. W przekonaniu autora artykułu dżihadyzm jest nowym kierunkiem w islamskiej myśli politycznej zapoczątkowanym przez Hassana al-Banę i Sayyida Qutba jako bunt przeciwko Zachodowi w celu ustanowienia islamskiego porządku na całym globie przy wykorzystaniu wszelkich możliwych środków. Zdaniem dżihadystów rządy islamu, pokój i powszechny dobrobyt uda się zaprowadzić jedynie przy pomocy dżihadu.

W pełni uprawniona jest teza głosząca, że współcześnie termin „dżihad" jest jednym z najbardziej nośnych[72] i kontrowersyjnych pojęć zarówno w islamie, jak i w nieislamskiej myśli politycznej, ponieważ zwolennicy dżihadyzmu oddziałują nie tylko na cywilizację judeochrześcijańską, rozumianą potocznie jako Zachód, ale również np. na myśl polityczną Indii czy Chin, choćby z racji problemów, które stwarzają liczne mniejszości muzułmańskie zamieszkujące te państwa. Wydaje się uprawniona teza, że chociaż dzisiaj dla dżihadystów głównym wrogiem jest Zachód, to zgodnie z ich celem ostatecznym po pokonaniu dhimmi[73] na Zachodzie przyjdzie czas na bałwochwalców na Wschodzie.

Widać zatem wyraźnie, że problem wypracowania stosunku do dżihadu nie jest wyłączną sprawą Okcydentu, również Orient nie jest od niego wolny. Tym samym święta wojna jest współcześnie, z racji metod działań podejmowanych przez jej zwolenników, jednym z najważniejszych zagrożeń globalnych oczekujących na wypracowanie w miarę spójnego stanowiska przez państwa, na które wywiera wpływ. Należy także podkreślić, że dopóki dżihadyści będą pojmowali dżihad jako instrument służący muzułmanom do narzucenia całemu światu panowania szariatu, dopóty dru-

---

[69] Tak uważają np. J. Kenny, M. Köylü, *Philosophy of the Muslim World: Authors and Principal Themes*, Washington 2003, s. 155.

[70] G. Weigel, *Wiara, rozum i wojna z dżihadyzmem. Wezwanie do działania*, Warszawa 2009, Fronda, s. 47. Najpopularniejsza wyszukiwarka internetowa Google po wpisaniu angielskiego terminu „jihadism" podaje 522 000 wyniki, (dane z 14 lipca 2012 r.)

[71] Cyt. za: G. Weigel, *Wiara, rozum i wojna z dżihadyzmem...,* s. 47.

[72] Por. dla przykładu następujące pozycje: B.R. Barber, *Dżihad kontra McŚwiat*, Warszawa 2000, MUZA, A. Rashid, *Dżihad. Narodziny wojującego islamu w Azji Środkowej,* tłum. A. i M. Falkowscy, Warszawa 2003, Dialog; M. Bonner, *Jihad in Islamic History: Doctrines and Practice*, Princeton NJ 2006, Princeton University Press; J. Kepel, *Jihad: the trail of political Islam*, London–New York 2006, Grove Press; R. Peters, *Jihad in classical and modern Islam: a reader*, Princeton NJ 2008, M.A. Khan, *Islamic Jihad...*; A.C. McCarthy, *The Grand Jihad: How Islam and the Left Sabotage America*, New York 2010. Z polskich autorów należy wymienić wspomnianą pracę ks. K. Kościelniaka, *Dżihad. Święta wojna w islamie*, Kraków 2002.

[73] Dhimmi to żydzi, chrześcijanie i sabejczycy żyjący w krajach muzułmańskich. Nie posiadają oni pełni praw i płacą większe podatki niż muzułmanie.

gorzędne znaczenie będzie miał podział na mały i wielki dżihad oraz wszelkie próby wykazania tego, która interpretacja jest poprawna. Równie mało przekonująco będą brzmieć głosy tych wszystkich, którzy starają się bagatelizować problem, akcentując, że radykalni muzułmanie stanowią tylko nieliczny odsetek wyznawców Allaha. Niestety, milczące przyzwolenie większości nie pozwala na stoicyzm, trzeba bowiem pamiętać, że świadome walczące mniejszości, dla których życie nie jest najwyższą wartością, często pociągały za sobą niezdecydowanych. Warto również mieć na uwadze liczby. Nawet jeśli ekstremiści stanowią mniej niż dziesięć procent wyznawców islamu, to np. trzy procent z półtora miliarda (niekiedy szacunki wskazują nawet na większą liczbę muzułmanów) stanowi 45 milionów.

Abstrakt

Celem artykułu jest próba wyjaśnienia kontrowersji i nieporozumień narosłych wokół muzułmańskiej koncepcji świętej wojny – dżihadu. Idea dżihadu została ukazana w kontekście innych obowiązków nałożonych na muzułmanów. Autor dokonuje historycznego przeglądu wybranych stanowisk i analizy leksykalnej badanego zagadnienia. Omawiając dżihad z dwóch punktów widzenia: jako agresywną wojnę z niewiernymi z jednej strony i walkę, jaką toczą wyznawcy Allaha z własnymi słabościami, aby stać się lepszymi muzułmanami z drugiej strony, autor stara się wykazać metodologiczną słuszność obu stanowisk. Jednak w jego ocenie wielu współczesnych muzułmanów odwołując się do terminu „dżihad", nie nadaje mu znaczenia duchowego czy pacyfistycznego, a raczej podkreśla agresywność działań i ich militarny charakter. Zarówno na płaszczyźnie socjologicznej, jak i historycznej w odwołaniu do Koranu pojęcie dżihadu jest jednoznaczne i mówi o wojnie muzułmanów prowadzonej w imię Boga w obronie lub w celu rozpowszechniania islamu i w taki sposób był rozumiany przez wielkich muzułmańskich jurystów.

W konkluzji autor próbuje dowieść, że dżihad pojmowany jako święta wojna z niewiernymi i będący jego konsekwencją dżihadyzm są jednymi z najbardziej niebezpiecznych wyzwań przed jakimi stoi współczesny świat. Celem walki, którą toczą dżihadyści, nie jest zmuszenie wszystkich niewiernych do przyjęcia islamu, ale dążenie do wprowadzenia islamskiego prawa – szariatu – na całej ziemi. Z tych powodów dżihadyzm jest problemem globalnym i nie dotyczy tylko Zachodu.

W ocenie autora dżihadyzm jest nowym kierunkiem w islamskiej myśli politycznej, zapoczątkowanym przez Hassana al-Banę i Sayyida Qutba, jako bunt przeciwko Zachodowi w celu ustanowienia islamskiego porządku na całym globie przy wykorzystaniu wszelkich możliwych środków. W przekonaniu dżihadystów rządy islamu, pokój i powszechny dobrobyt uda się zaprowadzić jedynie przy pomocy dżihadu – świętej wojny z niewiernymi.

Przedstawione przez autora wywody w pełni uprawniają do postawienia tezy, że chociaż dzisiaj dla dżihadystów głównym wrogiem jest Zachód, to zgodnie z ich celem ostatecznym po pokonaniu dhimmi na Zachodzie przyjdzie czas na bałwochwalców na Wschodzie.

Abstract

The aim of the article is to clear the controversies and misunderstandings behind the concept of the Muslim holy war – Jihad. The article presents Jihad in relation to other

obligations that are imposed on Muslims. Next, the author offers a historical overview of selected opinions and a lexical analysis of the idea. In his analysis of two particular points of view: Jihad as an aggressive war against non-Muslims, on the one hand, and the struggle that Allah's followers wage against their own weaknesses in order to become better Muslims, on the other hand, the author tries to prove the methodological legitimacy of both approaches. Still, he believes that many contemporary Muslims do not refer to Jihad meaning the spiritual or pacifistic struggle, but aggressive and military activities. Both sociologically and historically, based on the teachings of Qur'an Jihad unequivocally means Muslim warfare in the name of God in order to protect or promote Islam as it was understood by great Muslim jurists.

In conclusion, the author proves that Jihad was perceived as a holy war against the non-believers, as the consequent Jihadism, are the most dangerous challenges that the modern world has to face. The aim of the Jihadist war is not to force all Non-Muslims to convert to Islam, but to introduce Shariat law all over the world. Therefore, Jihad is a global issue that concerns not only the Western world.

The author believes that Jihadism is a new direction in the Islamist political belief that was first expressed by Hassan al-Bana and Sayyid Qutba in their protest against the West. Its aim was to establish a global Islamist rule using any means available. Jihadists believe that the Islamist rule, peace and general prosperity can only be achieved by means of Jihad – the holy war against non-believers.

The author proves that although Jihadists consider the West to be their enemy, their ultimate goal, after they defeat dhimmis in the West, is to crack down on the idolaters in the East.

Kacper Rękawek

Przyczynek do badań nad przywództwem w organizacjach terrorystycznych

Większość badań i ekspertyz poświęconych terroryzmowi i jego zwalczaniu koncentruje się na dokonanych a posteriori analizach pojedynczych przypadków (tzw. case'ów), tzn. na historii, działalności, osiągnięciach, porażkach itd. konkretnej organizacji terrorystycznej lub na przyjętych przez dane państwo metodach jej zwalczania[1]. W ostatnich latach sytuacja ta jednak uległa zmianie, a uwaga badaczy, ekspertów i naukowców w coraz większym stopniu zaczęła skupiać się na wcześniej zaniedbanych obszarach „studiów nad terroryzmem". Przykładem jest problem końca terroryzmu, tzn. w jaki sposób organizacje terrorystyczne i terroryści zaprzestają udziału w działalności nielegalnej i antypaństwowej i co się z nimi dzieje w następstwie takich decyzji[2]. W warunkach nieustającej „globalnej wojny z terroryzmem" takie badania automatycznie przyciągają uwagę decydentów, których nadrzędnym celem jest minimalizacja zagrożenia ze strony organizacji terrorystycznych. Chcąc sprostać nowym realiom związanym z badaniami nad terroryzmem i zapewnić swoim publikacjom większą relewantność, studenci kierunków związanych z bezpieczenstwem państwa (w tym autor[3]), zachęceni wynikami badań nad indywidualnymi losami członków organizacji terrorystycznych oraz losami całych organizacji terrorystycznych[4], rozpoczęli studia nad zjawiskiem końca terroryzmu, niejednokrotnie w odniesieniu do analizowanych przez siebie wcześniej indywidualnych przypadków terrorystycznych[5].

Co ciekawe, podczas studiów nad końcem terroryzmu stosunkowo mało uwagi poświęcano zagadnieniom przywództwa w organizacjach terrorystycznych i analizie dalszych losów osób kierujących takimi strukturami[6]. Powody takiego stanu rzeczy mogą być różne. Istotne znaczenie może tu mieć domniemana, postępująca, decentralizacja zagrożenia terrorystycznego, które w ostatnich latach ewoluowało z dala od

---

[1] Nadal aktualna analiza stanu dyscypliny „studiów nad terroryzmem" jest zawarta w: A. Silke, *The Impact of 9/11 on Research on Terrorism*, w: M. Ranstorp (red.), *Mapping terrorism research: state of the art, gaps and future direction*, Abingdon 2007, Routledge, s. 76–94.

[2] Jednym z prekursorów badań nad końcem terroryzmem był Paul Wilkinson. Zob.: *Contemporary Research on Terrorism*, Aberdeen 1987, Aberdeen University Press.

[3] Zob. K. Rekawek, *How 'terrorism' does not end: the case of the Official Irish Republican Army*, „Critical Studies on Terrorism" 2008, nr 3, s. 359–76.

[4] Zob. *Leaving Terrorism Behind: Individual and Collective Disengagement*, T. Bjorgo, J. Horgan (red.), Abingdon 2009, Routledge; A. K. Cronin, *How Terrorism Ends: Understanding the Decline and Demise of Terrorist Campaigns*, Princeton 2009, Princeton University Press; J. Horgan, *Walking Away from Terrorism: Accounts of Disengagement from Radical and Extremist Movements*, Abingdon 2009, Routledge.

[5] Jednym z najnowszych przykładów studiów nad końcem terroryzmu jest publikacja: F. Reinares, *Exit From Terrorism: A Qualitative Empirical Study on Disengagement and Deradicalization Among Members of ETA*, „Terrorism and Political Violence" 2011, nr 5, s. 780–803.

[6] Wyjątkiem są badania Jenny Jordan, która skupiała się przede wszystkim na kwestii efektywności fizycznej likwidacji przywódców organizacji terrorystycznych jako jednej z metod zwalczania terroryzmu. Zob. J. Jordan, *When Heads Roll: Assessing the Effectiveness of Leadership Decapitation*, „Security Studies" 2009, nr 4, s. 719–55.

działań prowadzonych przez szerzej znane organizacje terrorystyczne w stronę spisków podejmowanych przez grupy terrorystów – ochotników[7]. Takie założenie prowadzi do wniosku o niemożności ustalenia hierarchii i struktury ciągle ewoluujących, małych i niepodlegających niczyim rozkazom komórek terrorystycznych. Nie zmienia to jednak faktu, że różne instytucje nadal utrzymują i aktualizują listy osób i organizacji uznanych za terrorystyczne, co stanowi podstawę do prowadzenia działań antyterrorystycznych m.in. przez organy ścigania, wojsko i służby specjalne[8]. Krytycy mogą uznać takie podejście za wyraz niedostosowania współczesnych państw do realiów walki z aktorami społecznymi (sieciowymi), którzy nie działają w zhierarchizowanych strukturach organizacyjnych. Faktem jest jednak, że wiele oddolnych, samodzielnych i spontanicznych, spisków terrorystycznych nie zakończyło się sukcesem, a najskuteczniejsze z nich, m.in. ataki z 11 września 2001 r., są dziełem znanych i istniejących od lat organizacji terrorystycznych, które w swoich działaniach przyjmują zasady i elementy wojny sieciowej. W konsekwencji używanie list koncentrujących się na bardziej tradycyjnych formach organizacyjnych terroryzmu do dokumentowania skali zagrożenia terrorystycznego nie musi być podejściem błędnym. Powinno to także zachęcić badaczy do ustalenia sukcesji przywództwa w istniejących organizacjach terrorystycznych, co może mieć duże znaczenie dla decydentów zainteresowanych skutecznymi metodami wpływania na terrorystów poprzez podejmowanie określonych działań wymierzonych w ich przywódców.

W 2011 r., tuż przed dziesiątą rocznicą ataków terrorystycznych z 11 września 2001 r., autor niniejszego artykułu postanowił wypełnić lukę badawczą dotyczącą losów przywódców organizacji terrorystycznych i implikacji sposobów zaprzestawania przez nich działalności, dla polityki antyterrorystycznej państw demokratycznych. Wyniki badań przedstawił w analizie pt. *How Terrorist Leaders End: Implications for the Future of the Struggle with Al-Qaeda* (dosł.: *Jak kończą przywódcy terrorystyczni: implikacje dla przyszłości zmagań z Al-Kaidą*) wydanej w serii „Policy Papers" Polskiego Instytutu Spraw Międzynarodowych (PISM)[9]. Artykuł był analizą losów przywódców 48 organizacji terrorystycznych, które w 2011 r. znajdowały się na liście Foreign Terrorist Organizations (FTO) amerykańskiego Departamentu Stanu[10].

Podczas przygotowywania analizy, o której mowa, autorowi udało się zidentyfikować 114 przywódców (osoby stojące na czele danej struktury organizacyjnej), którzy łącznie przez ok. 1018 lat zarządzali lub nadal zarządzają „swoimi" organizacjami terrorystycznymi[11]. Oznacza to, że statystycznie każdy z nich pełnił (lub pełni) swoją funkcję ok. 8,85 roku, tj. wyjątkowo długo jak na osoby stojące na czele nielegalnych, tajnych i zbrojnych struktur prowadzących działalność antypaństwową. Oczywiście nie każda

[7] Więcej na temat zdecentralizowanych (ale nie tylko zdecentralizowanych) spisków terrorystycznych w: P. Nesser, *Chronology of Jihadism in Western Europe 1994–2007: Planned, Prepared, and Executed Terrorist Attacks*, „Studies in Conflict & Terrorism" 2008, nr 10, s. 924–946.

[8] Listy te posiadają m.in. Stany Zjednoczone, Wielka Brytania, Federacja Rosyjska i Unia Europejska.

[9] K. Rękawek, *How Terrorist Leaders End: Implications for the Future of the Struggle with al-Qaeda* [online], http://www.pism.pl/files/?id_plik=8305 [dostęp: 3 XII 2012].

[10] FTO są oficjalnie „desygnowane" przez sekretarza stanu, jeśli stwierdzi on, że dana organizacja jest organizacją „zagraniczną", że jest zaangażowana w działania terrorystyczne lub utrzymuje zdolność i intencje do kontynuowania swojego zaangażowania w terroryzm oraz zagraża bezpieczeństwu Stanów Zjednoczonych lub jego obywateli. Zob. http://www.uscis.gov/ilink/docView/SLB/HTML/SLB/0-0-0-1/0-0-0-29/0-0-0-5017.htm [dostęp: 3 XII 2012].

[11] W 2012 r. na liście znalazły się 122 osoby – zob. załącznik do tego artykułu.

z tych osób miała (lub ma) możliwość sprawowania władzy tak długo (vide przypadki przywódców Al-Kaidy w Arabii Saudyjskiej czy Al-Kaidy na Półwyspie Arabskim), a powyższe statystyki zawyża chociażby przypadek Osamy bin Ladena, który stał na czele Al-Kaidy przez ok. 23 lata. Ze 114 zidentyfikowanych przywódców 86 zakończyło już swoje „kariery", a jedynie 28 nadal kontynuuje działalność terrorystyczną na czele kierowanych przez siebie organizacji. Z 86 „nieaktywnych" przywódców 40 zostało aresztowanych, 26 zginęło z rąk organów ścigania, dwóch w wyniku działań innych organizacji terrorystycznych, a jeden w wyniku wewnętrznych sporów w kierowanej przez siebie organizacji (Carlos Castaño Gil ze Zjednoczonych Sił Samoobrony Kolumbii). Pięciu przywódców terrorystycznych zmarło z przyczyn naturalnych, czterech zakończyło działalność i przeszło na emeryturę, trzech odsunięto od władzy i nie zostali oni pozbawieni życia. Z pozostałych pięciu jeden zrezygnował z prowadzenia dalszej działalności, jeden dobrowolnie oddał władzę, jeden dokonał rozłamu w organizacji terrorystycznej i założył nową, jeden popełnił samobójstwo i jeden oddał się w ręce organów ścigania[12].

Różnorodność losów przywódców organizacji terrorystycznych oraz niejednokrotnie ich zaskakująca długowieczność doprowadziły autora do wniosków, które wydawały się przeczyć teorii o pełnionej przez nich dominującej roli w kierowanych przez siebie strukturach. Wiele organizacji znajdujących się na liście FTO przetrwało bowiem utratę swoich domniemanych charyzmatycznych liderów i było w stanie dostosować się do zmieniających się warunków dla ich funkcjonowania w różnych państwach. Autor niniejszego opracowania dość ostrożnie podchodził do zbyt optymistycznych założeń związanych z potencjalnym „końcem Al-Kaidy", który miał nastąpić po śmierci Osamy bin Ladena, i rekomendował skupienie uwagi organów ścigania i służb specjalnych nie na kolejnym „emirze", Ajmanie al-Zawahirim, ale na wyróżniających się członkach organizacji jako na jego potencjalnych następcach. Pozbawienie ich szans na uzyskanie wyższego statusu w organizacji miałoby doprowadzić do jej szybszego upadku, ponieważ w wyniku aresztowań lub fizycznej likwidacji co zdolniejszych jednostek na czele Al-Kaidy stanęłyby osoby o mniejszm potencjale działania i mniejszych umiejętnościach.

W rok po ukazaniu się wyzej wymienionej analizy autor rozpoczął prace nad uaktualnieniem wyników swoich badań dotyczących kwestii przywództwa w organizacjach terrorystycznych. Podczas gromadzenia informacji do załącznika[13], w którym była zawarta oryginalna baza danych na temat przywódców organizacji terrorystycznych, autor natrafił jednak na wiele problemów i wyzwań. Ich podejmowanie i pokonywanie, nie zawsze zakończone sukcesem, było impulsem do przygotowania niniejszego artykułu, który w pierwotnych zamierzeniach miał być przeniesieniem uaktualnionych anglojęzycznych badań autora na rynek polskich publikacji naukowych. Konkluzje płynące z ostatnich badań autora mogą mieć poważne konsekwencje dla osób, które chcą obrać terroryzm i jego zwalczanie za cel swoich badań naukowych oraz dla decydentów, którzy chcieliby skorzystać z wyników takich badań w procesach decyzyjnych związanych z bezpieczeństwem państwa. Dalszej części artykułu nie należy jednak traktować jako wezwania do porzucenia badań nad sposobami ewentualnego rozprawienia się z terroryzmem oraz przywódcami organizacji terrorystycznych, lecz jako krytykę

[12] K. Rękawek, *How Terrorist Leaders End*..., s. 3.

[13] K. Rękawek, *Appendix: Terrorist Leaders Dataset* [online], http://www.pism.pl/files/?id_plik=8306 [dostęp: 3 XII 2012].

porzucania badań jakościowych dotyczących terroryzmu na rzecz zbytniego polegania na dominujących, zwłaszcza w Stanach Zjednoczonych, badaniach ilościowych, które, jak w latach 2011–2012 przekonał się autor, nie mogą dać satysfakcjonującej odpowiedzi na wszystkie stawiane przez badaczy, decydentów i ekspertów pytania.

Zdaniem dr. Adama Dolnika z Uniwersytetu Wollongong w Australii, jednego z najbardziej znanych badaczy terroryzmu międzynarodowego, każdy, kto bada kwestie przywództwa w organizacjach terrorystycznych:

1) nie wie, co naprawdę „dzieje się wewnątrz grupy terrorystycznej",
2) chcąc rozwikłać problem nr 1, często stara się ująć najważniejsze osoby w danej organizacji w klasyfikację opartą na systemie rankingowym, tzn. nadużywa terminów typu „numer 1, 2, 3, 4" itd. w organizacji, które nie oddają rzeczywistego statusu konkretnej jednostki w grupie, organizacji czy siatce terrorystycznej,
3) nie bierze pod uwagę znaczących różnic w funkcjonowaniu organizacji terrorystycznych, w których rola przywódców jest często zróżnicowana[14].

Dobrą i aktualną ilustracją tez A. Dolnika jest sytuacja z listopada 2012 r., kiedy to Izrael zlikwidował „dowódcę" Hamasu[15]. Odbiorcy takiej wiadomości, w tym większość badaczy terroryzmu (z wyjątkiem znawców problematyki terroryzmu bliskowschodniego i Hamasu), nie są w stanie stwierdzić, jak ważną pozycję w organizacji zajmował zabity Ahmed al-Jabari (problem nr 1). W konsekwencji próbuje się umieścić al-Jabariego w kadrze dowódczej Hamasu i rozstrzygnąć, czy w tej organizacji terrorystycznej w danym momencie ważniejszą rolę odgrywają przywódcy polityczni, czy „wojskowi" (de facto: terrorystyczni). Jest to problem numer 2. Takie rozważania niekoniecznie pomagają badaczowi w rozwikłaniu zagadki przywództwa w Hamasie, ponieważ organizacja ta ma więcej niż jedno centrum władzy politycznej (Gaza i do niedawna Damaszek, a obecnie Kair), co dodatkowo komplikuje wcześniejsze ustalenia. Nie oznacza to jednak, że sytuacja przedstawia się podobnie w przypadku innych organizacji terrorystycznych (problem nr 3).

Wnioski dr. A. Dolnika i analiza przypadku Jabariego[16] uwypuklają największy dylemat ekspertów i naukowców próbujących zmierzyć się z kwestią przywództwa w organizacjach terrorystycznych, tj. nadużywanie lub niekonsekwentne używanie przez nich, a także m.in. przez członków organizacji terrorystycznych[17], pracowników organów ścigania i służb powołanych do zwalczania terroryzmu oraz dziennikarzy

---

[14] Komunikacja mejlowa autora z dr. Dolnikiem, 26 listopada 2012 r.

[15] Ch. Lister, *Hamas sources report alleged appointment of new militant leader*, „Jane's Terrorism & Security Monitor" January 2013, nr 13.

[16] Wyniki analizy dotyczącej przywództwa np. w baskijskiej ETA (kierowanej równocześnie przez trójkę przywódców – politycznego, „militarnego" i logistycznego), egipskiej Grupy Islamskiej (funkcjonującej równolegle do pozornie niezależnego od niej skrzydła politycznego – Partii Budowy i Rozwoju), Al-Kaidy w Iraku, AKI (oprócz działalności terrorystycznej prowadzacej także działalność polityczną, propagandową i w mniejszym stopniu charytatwno-społeczną), irlandzkich ugrupowań republikańskich (mających kierownictwo kolegialne) byłyby podobne do tej przeprowadzonej w odniesieniu do Hamasu. Struktury prowadzących różne typy działalności (Grupa Islamska, AKI) lub posiadających różne typy kolegialnego kierownictwa (ETA, CIRA, RIRA) są zdecydowanie trudniejsze w zbadaniu pod kątem przywództwa niż organizacje zdominowane przez charyzmatycznego lidera lub skoncentrowane tylko na jednym, np. terrorystycznym, typie działalności.

[17] Badania autora przeprowadzone w Irlandii Północnej w latach 2006–2011 dostarczyły mu wielu przykładów zachowań, kiedy to byli członkowie np. Irlandzkiej Armii Republikańskiej używali słów „przywódca" i „przywódcy" w szerokim i zamiennym znaczeniu, nie określając jednoznacznie, kto naprawdę stał na czele organizacji lub jej elementów składowych, niejednokrotnie koncentrując się na perspektywie lokalnej.

i innych przedstawicieli mediów, słów „przywódca" i „lider". Konsekwencją tego jest rozmycie i zniekształcenie wiedzy na temat konkretnej grupy, organizacji lub siatki terrorystycznej. Niepewność co do faktycznego przywództwa w strukturach, o których mowa, może prowadzić także do wniosków kwestionujących już posiadaną wiedzę dotyczącą przywództwa w organizacjach nielegalnych (nie tylko terrorystycznych) i w konsekwencji do nadania im cech (np. sieciowość, płaska struktura), których w rzeczywistości nie mają. Wzrost liczby „liderów" może sugerować także fizyczny rozrost danej organizacji terrorystycznej, która ma np. rozbudowaną kadrę zarządzającą rozrzuconą po całym świecie (Al-Kaida i emirzy jej regionalnych spółek córek lub organizacji afiliowanych) i która z własnej woli nadaje wiele pozornie wysokich stanowisk swoim członkom (fronty w FARC, dowódcy batalionów i frontów w Emiracie Kaukaskim, dowódcy brygad w irlandzkich republikańskich grupach terrorystycznych) lub która jest tak słaba, że przywódcę każdej z jej nielicznych kilkuosobowych komórek media i eksperci nazywają „liderem" organizacji lub w najgorszym razie jej frakcji (przypadek filipińskiej Grupy Abu Sayyafa).

Nawet jeśli dana organizacja nie próbuje w sztuczny sposób wykreować wrażenia o swoim dużym potencjale i sile, to badacze niejednokrotnie stają przed problemem rozszyfrowania kwestii przywództwa w sytuacji, gdy emanacja terroryzmu na danym terenie jest szeroka. Termin „alphabet soup" (dosł. zupa z małymi kluskami), używany m.in. w odniesieniu do dużej liczby organizacji terrorystycznych operujących w Pakistanie i na pograniczu afgańsko-pakistańskim[18], obrazuje dylematy każdego, kto chciałby poznać historie pakistańskich terrorystów islamistycznych. Ich organizacje mają podobne nazwy, szkolą się i mają schronienie na tym samym terenie, często współdziałają ze sobą, np. podczas działań wymierzonych w Indie, oraz tworzą organizacyjne efemerydy (jak np. Brygada 313[19]), skupiające tylko niektórych ze swoich członków. Ustalenie przywództwa w ich strukturach, pomimo dość daleko posuniętego zhierarhizowania tych organizacji, jest trudne i nie może się obejść bez współpracy zwalczających je organów ścigania i służb specjalnych. Oczywiście jest to rozwiązanie niedostępne dla większości badaczy i ekspertów, a nawiązanie takiej współpracy też z reguły nie oznacza możliwości publikowania wyników badań w źródłach powszechnie dostępnych.

Innym problemem dla badaczy przywództwa w organizacjach terrorystycznych jest niemożność stwierdzenia, czy dana organizacja nadal istnieje, i w związku z tym, czy losy jej przywódców w ogóle warto brać pod uwagę w swoich rozważaniach. Idealnym przykładem takiej sytuacji jest Organizacja Abu Nidala (OAN), której przywódca nie żyje od 10 lat i która dokonała ostatniego ataku terrorystycznego w 1998 r.[20] Nie zmienia to jednak faktu, że OAN jest nadal uznawana przez Stany Zjednoczone za FTO, co pozwala zakładać, że nadal działa. Nic nie wiadomo natomiast o ewentualnym następcy charyzmatycznego byłego przywódcy.

Pytania o dalsze funkcjonowanie organizacji terrorystycznych można zadać, badając także inne z FTO, m.in. japońskie Aum Shinrikyo, które od 2000 r. działa

[18] Zob. na przykład: P. Bergen, *What's Working in Pakistan* [online], http://www.newamerica.net/node/69900 [dostęp: 4 XII 2012].

[19] B. Roggio, *Al-Qaeda leader Ilyas Kashmiri spotted at Taliban meeting* [online], http://www.longwarjournal.org/archives/2012/03/al_qaeda_leader_ilya.php [dostęp: 4 XII 2012].

[20] Zob. *Global Terrorism Database* [online], http://www.start.umd.edu/gtd/search/Results.aspx?search=abu+nidal&sa.x=0&sa.y=0&sa=Search [dostęp: 4 XII 2012].

pod inną nazwą i oficjalnie odżegnuje się od działalności terrorystycznej. Podobnie Libijski Ruch Islamski – organizacja powstała na gruzach ciągle uznawanej za FTO Libijskiej Islamskiej Grupy Zbrojnej. Nieco inaczej rzecz się ma z organizacjami, których liczebność została znacznie osłabiona przez aresztowania. Badacz w takich sytuacjach może stracić kontrolę nad uaktualnianiem nazwisk kolejnych przywódców, którzy mogą nawet nie zdążyć z przeprowadzeniem jakichkolwiek znaczących działań terrorystycznych (baskijska ETA[21], irlandzkie ugrupowania republikańskie – CIRA, RIRA, do niedawna także peruwiański Świetlisty Szlak[22]). Podobnie jest w przypadku organizacji, które najprawdopodobniej są pogrążone w walkach wewnętrznych i nikt spoza ich struktur nie jest w stanie z całą pewnością odtworzyć historii sukcesji ich przywództwa (al-Shabaab w 2011 r.[23], w mniejszym stopniu podzielona na frakcje geograficzne Al-Kaida w Islamskim Maghrebie[24]).

Decentralizacja lub koalicyjny charakter organizacji terrorystycznych (palestyńskie Brygady Męczenników al-Aksa, iracki Kata'ib Hizballah[25]) również nie sprzyjają możliwości poddania ocenie i przedstawieniu historii przywództwa w ich strukturach, ponieważ badacze znają jedynie „najpopularniejszych" liderów (np. Marwana Barghoutiego lub Abu Mahdiego al-Muhandisa), ale niekoniecznie przywódców całości tych organizacji.

Jeszcze trudniejsza do ustalenia jest kwestia, czy konkretny przywódca nadal sprawuje swoje rządy pomimo np. aresztowania czy ukrywania się, co w znaczny sposób ogranicza jego kontrolę nad daną organizacją. W tej sytuacji jest m.in. kurdyjska PKK, której przywódca, Abdullah Ocalan, przebywa w tureckim więzieniu, ale bez którego wiedzy i zgody jego byli podkomendni nie zdecydują się np. na pokojowe rozwiązanie kwestii kurdyjskiej w Turcji. Innym przykładem są przypadki, gdy charyzmatyczni przywódcy organizacji terrorystycznych, np. Pakistańczycy Maulana Masood Azhar z Armii Proroka (Jaish-e-Mohammed), Akram Lahori z Lashkar i Jhangvi, Qari Saifullah Akhtar z Harakat-ul Jihad Islami lub Hafiz Saeed z Lashkar-e Tayyiba (LeT, Armia Czystych), są na krótko aresztowani, a następnie wypuszczani z więzień. Kwestia odzyskania przez nich poprzednich stanowisk w kierowanych przez nich organizacjach terrorystycznych jest sprawą dyskusyjną (byłoby to niemożliwe np. w irlandzkich ugrupowaniach republikańskich), ale trudno wyobrazić sobie LeT pod kierownictwem kogokolwiek innego niż Saeed. W niektórych sytuacjach nie można jednak udowodnić im dalszego kierowania organizacjami, co skłoniło autora do zakwalifikowania ich jako

[21] *Suspected head of Basque separatist group seized in France* [online], http://www.euronews.com/2012/10/28/suspected-head-of-basque-separatist-group-seized-in-france/ [dostęp: 4 XII 2012].

[22] *Peru Captures Shining Path Leader In Upper Huallaga* [online], http://www.peruviantimes.com/05/peru-captures-shining-path-leader-in-upper-huallaga/15474 [dostęp: 4 XII 2012].

[23] *Interview with Al Shabaab Intel Officer* [online], http://www.somaliareport.com/index.php/post/2281 [dostęp: 4 XII 2012].

[24] J.P. Filiu, *Al-Qa`ida in the Islamic Maghreb. A Case Study in the Opportunism of Global Jihad* [online], http://www.ctc.usma.edu/posts/al-qaida-in-the-islamic-maghreb-a-case-study-in-the-opportunism-of-global-jihad [dostęp: 4 XII 2012].

[25] Kata'ib Hizballah jest oskarżany o przyjmowanie pomocy od Iranu, co jedynie komplikuje próby ustalenia jego rzeczywistego przywództwa i wpływu, jaki jego sponsorzy i opiekunowie mogą mieć na podejmowane przez tę luźną organizację działania. Podobnie może być z inną FTO – Indyjskimi Mudżahedinami, którzy są oskarżani o przyjmowanie pomocy i rozkazów od pakistańskich służb specjalnych.

byłych przywódców organizacji terrorystycznych, ale to niekoniecznie musi być zgodne z prawdą[26].

Jeszcze innym przypadkiem są sytuacje, gdy przywódca kojarzony z jedną organizacją (np. Abu Bakar Bashir, założyciel indonezyjskiej Jemaah Islamiya, która pomimo licznych wewnętrznych podziałów i osłabienia jest nadal uznawana za FTO[27]) zakłada kolejną organizację, która po jakimś czasie trafia na listę amerykańskiego Departamentu Stanu (Jemaah Ansharut Tauhid). Trudno ustalić, w jakim stopniu taka osoba kontroluje swoją poprzednią organizację tuż przed założeniem kolejnej i jaka jest jej rzeczywista funkcja w nowej strukturze.

Problemów badaczom terroryzmu dostarczają także organizacje, w których ważną rolę odgrywają więzi rodzinne. Idealnym przykładem jest tu grecka Rewolucyjna Organizacja 17 Listopada (17N), której działalność zakończyły najprawdopodobniej aresztowania z 2002 r. (nadal jednak jest uznawana za FTO), kolumbijskie Zjednoczone Siły Samoobrony Kolumbii (AUC), w których dominujące role odgrywali bracia Castaño Gil, oraz tzw. Siatka Haqqaniego, którą kieruje Jalaluddin Haqqani i jego syn Sirajuddin Haqqani. W takiej sytuacji kwestią dyskusyjną pozostaje rzeczywiste przywództwo w tych organizacjach, które w drodze nieformalnych porozumień mogło lub może się często zmieniać, przechodząc z rąk do rąk w obrębie jednej rodziny. Co ciekawe, taki model zarządzania grupą zbrojną nie zawsze przynosi sukcesy – w wypadku kolumbijskiego AUC doszło najprawdopodobniej do sporu pomiędzy braćmi kierującymi organizacją. Spór ten zakończyło zlecenie zamordowania Carlosa Castaño Gila przez jego brata Vincente[28].

Podsumowanie

Niniejszy artykuł należy traktować jako podsumowanie wniosków z badań prowadzonych przez autora w latach 2011–2012 r., których celem było opisanie losów przywódców FTO. Badania te miały pozwolić na ustalenie, czy usunięcie przywódcy grupy, organizacji lub siatki terrorystycznej rzeczywiście może doprowadzić do ich końca. Wynikiem tych badań, przynajmniej w odniesieniu do ustabilizowanych i istniejących od dawna struktur znajdujących się na liście FTO, była konkluzja dotycząca stosunkowo dużej zdolności adaptacyjnej terrorystów, których przywódcy najczęściej utrzymywali się na swoich stanowiskach dość długo i często skutecznie wychowywali lub promowali swoich następców.

Należy jednak zaznaczyć, że wynik badań jest obarczony znacznym ryzykiem błędu, ponieważ autor podczas zbierania danych potrzebnych do sporządzenia załącznika do powyższego artykułu zmagał się z wieloma problemami. Brak precyzji wielu z jego ustaleń może być uznany za powód do porzucenia dalszego zestawiania podobnej bazy danych i niewyciągania pochopnych wniosków ze zgromadzonych informacji. W opinii autora należy jednak kontynuować podobne badania, które wydają się wskazywać na ograniczoną słuszność kierowania wysiłków przez jednostki antyterrorystyczne przeciwko przywódcom grup, organizacji i siatek terrorystycznych, których zmiana

[26] W podobnej sytuacji do aresztowanych przywódców organizacji terrorystycznych są także ci, którzy pozostają w ukryciu, np. Ahmad ‘Abd al-Karim al-Sa‘di z libańskiego Asbat al-Ansar.

[27] *Jemaah Islamiya (JI)* [online], http://www.nctc.gov/site/groups/ji.html [dostęp: 4 XII 2012].

[28] *Colombia convicts No. 1 fugitive paramilitary boss* [online], http://www.boston.com/news/world/latinamerica/articles/2011/03/17/colombia_convicts_no_1_fugitive_paramilitary_boss/ [dostęp: 4 XII 2012].

często nie wpływa na skuteczność kierowanych przez nich struktur. W celu udowodnienia lub obalenia tej tezy konieczne jest kontynuowanie niepopularnych obecnie w studiach nad terroryzmem badań o charakterze komparatywnym (niejednokrotnie poświęconych pojedynczym przypadkom), które pozwolą na dokładne ustalenie losów poszczególnych przywódców struktur terrorystycznych. Może to oznaczać położenie mniejszego nacisku na badania ilościowe, uważane dotychczas za najbardziej miarodajne w procesie formułowania jednoznacznych konkluzji dla decydentów i osób odpowiedzialnych za bezpieczeństwo państwa.

Tabela. Zidentyfikowani przywódcy terrorystyczni i ich losy.

Nazwa FTO (angielskie nazwy z oryginalnej listy FTO)	Liczba i nazwiska przywódców FTO	Okres sprawowania władzy w FTO	Zakończenie działalności przez przywódców FTO
Abu Nidala Organization	Sabri al-Banna (Abu Nidal)	1974–2002	samobójstwo
Abu Sayyaf Group[1)]	Abdurajik Abubakar Janjalani	1991–1998	zabity przez służby specjalne/ /wojsko/organy ścigania
	Abubakar Khadaffy Janjalani	1998–2006	zabity przez służby specjalne/ /wojsko/organy ścigania
	Radulan Sahiron	2006–2008	zabity przez służby specjalne/ /wojsko/organy ścigania
Al Aqsa Martyrs Brigades[2)]	Marwan Barghouti	2000–2002	aresztowany
Al-Shabaab	Abdi Godane/Abu Zubeyr[3)]	2006–2010	usunięty ze stanowiska
	Ibrahim al-Afghani	2010–do dziś?	czynny
Ansar al Islam/ /Ansar al-Sunna	Mullah Kreka Abu Abdullah al Shafii[4] Abu Hashim Muhammad bin Abdul Rahman al Ibrahim[5)]	2001–2002/03 2003–2010 2012–do dziś	aresztowany (lub deportowany) aresztowany czynny
Aum Shinrikyo	Shoko Asahara Fumihiro Joyu	1987–1995 1995–2000	aresztowany emerytura – grupa zmienia swoją nazwę i odchodzi od działalności terrorystycznej

[1)] Zob. prace Z. Abuzy: *The Demise of the Abu Sayyaf Group in the Southern Philippines*, [online], http://www.ctc.usma.edu/posts/the-demise-of-the-abu-sayyaf-group-in-the-southern-philippines; *On the defensive* [online], http://www.simmons.edu/undergraduate/academics/departments/politicalscience/docs/Abuza_Intelligence Review_4_07.pdf, *The Philippines Chips Away at the Abu Sayyaf Group's Strength* [online], http://www.ctc.usma.edu/posts/the-philippines-chips-away-at-the-abu-sayyaf-group's-strength. Data dostępu do materiałów internetowych podanych w tym załączniku to w każdym przypadku 9 XII 2012.

[2)] *Profile: Al-Aqsa Martyrs' Brigades* [online], http://news.bbc.co.uk/2/hi/middle_east/1760492.stm.

[3)] *Al-Shabaab's problems over the future of Colonel Hassan Dahir 'Aweys'* [online], http://www.waltainfo.com/index.php?option=com_content&task=view&id=25041&Itemid=82.

[4)] *Abu Abdullah Al Shafi'l, leader of Ansar al Islam arrested* [online], http://www.thaindian.com/newsportal/world/abu-abdullah-al-shafil-leader-of-ansar-al-islam-arrested_100358018.html.

Asbat al-Ansar[6)]	Sheik Hisham Shreidi	1989/90 –1991	zabity przez inną organizację terrorystyczną
	Ahmad ‘Abd al-Karim al-Sa‘di, alias Abu Mihjin	1991–do dziś	czynny, ale się ukrywa – organizacją dowodzi jego brat – Abu Tariq[7)]
basque Homeland and Liberty – ETA	Txomin Iturbe[8)]	1983[19)]–1986	aresztowany (lub deportowany)
	José Antonio Urritikoechea	1986–1989	aresztowany
	Francisco Mugica Garmendia[9)]	1989–1992	aresztowany
	Mikel Albizu Iriarte[10)]	1993–2004	aresztowany
	Javier Lopez Pena[11)]	2006–2008	aresztowany
	Garikoitz Aspiazu Rubina[12)]	2008	aresztowany
	Aitzol Irionda	2008	aresztowany
	Jurdan Martitegi Lizaso [13)]	2008–2009	aresztowany
	Aitor Elizaran Aguilar[14)]	2009	aresztowany
	Ibon Gogeascoetxea Arronategi[15)]	2008/09–2010	aresztowany
	Mikel Kabikoitz Carrera Sarobe[16)]	2010	aresztowany
	Alejandro Zobaran Arriola [17)]	2010–2011	aresztowany
	Izaskun Lesaka[18)]	2012?	aresztowany

[5)] Zob.: http://www.longwarjournal.org/archives/2012/01/ansar_al_islam_names.php.

[6)] *Asbat al-Ansar* [online], http://www.nctc.gov/site/groups/asbat_al_ansar.html.

[7)] *Asbat al-Ansar (AAA*) [online], http://www.aph.gov.au/house/committee/pjcis/six%20terrorist/AAA.pdf.

[8)] *El dirigente de ETA Txomin Iturbe murió el viernes en Argelia en un accidente de tráfico* [online], http://www.elpais.com/articulo/espana/ITURBE_ABASOLO/_DOMINGO_/TXOMIN/ARGELIA/ETA/dirigente/ETA/Txomin/Iturbe/murio/viernes/Argelia/accidente/trafico/elpepiesp/19870302elpepinac_1/Tes?print=1.

[9)] Zob. http://www.laresistenciaaeta.org/basedatos/detalleeta.php?id=6.

[10)] P. Rolfe, *Alleged Leader of ETA Is Captured in France* [online], http://www.washingtonpost.com/wp-dyn/articles/A4630-2004Oct3.html.

[11)] F. Govan, *Eta leader Francisco Javier Lopez Pena arrested in France* [online], http://www.telegraph.co.uk/news/2000809/Eta-leader-Francisco-Javier-Lopez-Pena-arrested-in-France.html.

[12)] *France captures top ETA leader* [online], http://www.csmonitor.com/World/2008/1118/p06s01-wogn.html.

[13)] *France holds Eta ‘military chief’* [online], http://news.bbc.co.uk/2/hi/8006511.stm.

[14)] *Aitor Elizarán Aguilar, otro producto de la ‘kale borroka’* [online], http://www.ideal.es/granada/20091019/espana/aitor-elizaran-aguilar-otro-200910191253.html.

[15)] B. Bond, *ETA leader arrested in France* [online], http://www.telegraph.co.uk/news/worldnews/europe/spain/7338332/ETA-leader-arrested-in-France.html.

[16)] *Suspected Eta leader arrested in France* [online], http://www.independent.co.uk/news/world/europe/suspected-eta-leader-arrested-in-france-1978793.html.

[17)] *ETA: les 4 membres présumés arrêtés à Willencourt mis en examen et écroués* [online], http://www.lavoixdunord.fr/France_Monde/actualite/Secteur_France_Monde/2011/03/15/article_eta-les-4-membres-presumes-arretes-a-willencourt.shtml.

[18)] Zob. http://www.euronews.com/2012/10/28/suspected-head-of-basque-separatist-group-seized-in-france/.

communist Party of the Philippines/ New People's Army (CPP/NPA)	Jose Maria Sison	1969	czynny; powrócił z dobrowolnego wygnania
continuity Irish Republican Army (CIRA)	Daithí O´ Conaill[20)]	1986–1991	śmierć z przyczyn naturalnych
gama'a al-Islamiyya (Islamic Group)	Umar Abd al-Rahman	1973–?[24)]	aresztowany
	Rifai Ahmed Taha	?–?	aresztowany
	Safwat 'Abd Al-Ghani[21)]	? –?	aresztowany
	Karam Zuhdi[22)]	? –?	aresztowany
	Issam Darabla[23)]		czynny
HAMAS[25)]	Ahmed Yassin	1987–2004	zabity przez służby specjalne/ /wojsko/organy ścigania
	Abd al-Aziz Rantisi	2004	zabity przez służby specjalne/ /wojsko/organy ścigania
	Khaled Mashal	2004–do dziś	czynny
Harakat ul-Jihad--i-Islami/Bangladesh (HUJI-B)[26)]	Shawkat Osman	1992– 2011[27)]	czynny
harakat ul-Mujahidin (HUM)[28)]	Fazlur Rehman Khalil	1985–2000?	emerytura
	Farooq Kashmiri Khalil	2000–do dziś	czynny
hizballah (Party of God)[29)]	Subhi al-Tufayli	1989–1991	usunięty ze stanowiska
	Abbas Musawi	1991–1992	zabity przez służby specjalne/ /wojsko/organy ścigania
	Hassan Nasrallah	1992–do dziś	czynny

[19)] W 1983 r. resztki ETApm (polityczno-wojskowej) połączyły się z ETAm (wojskową), tworząc organizację, którą dziś określa się mianem ETA.

[20)] *CIRA bomb adds to growing crisis in the peace process* [online], http://archives.tcm.ie/irishexaminer/2000/02/07/current/opinionpage_9.htm.

[21)] *Al-Gama'a Al-Islamiyya leadership's ideological reversal* [online], http://armiesofliberation.com/archives/2006/12/22/al-gamaa-al-islamiyya-leaderships-ideological-reversal/.

[22)] J. Halawi, *Time for a historic reconcilliation?* [online], http://weekly.ahram.org.eg/2002/592/eg4.htm.

[23)] *Egypt's Al-Gama'a Forms Party* [online], http://www.thememriblog.org/blog_personal/en/38677.htm.

[24)] Zob. *Militant Ideology Atlas* [online], http://www.ctc.usma.edu/wp-content/uploads/2010/06/Atlas-ResearchCompendium1.pdf.

[25)] M. Levitt, *HAMAS. Politics, Charity and Terrorism in the Service of Jihad*, London 2006, Yale University Press, s. 33–52.

[26)] Zob. http://www.satp.org/satporgtp/countries/bangladesh/terroristoutfits/Huj.htm.

[27)] Zob. http://www.satp.org/satporgtp/countries/bangladesh/.

[28)] Zob. http://www.satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/harkatul_mujahideen.htm.

[29)] Zob. G. C. Gambill, Z. K. Abdelnour, *Hezbollah: Between Tehran and Damascus* [online], http://www.meforum.org/meib/articles/0202_l1.htm; R. Bergman, *The Secret War with Iran. The 30-Yeat Covert Struggle for Control of a 'Rogue' State*, Oxford 2008, One World, s. 51–63.

islamic Jihad Group/Islamic Jihad Union (IJU)[30]	Nadzhmiddin Kamoldinovich Jalolov (Abu Yahya)	2002– 2009[31]	zabity przez służby specjalne/ /wojsko/organy ścigania
Islamic Movement of Uzbekistan[32]	Juma Namangani	1998–2001	zabity przez służby specjalne/ /wojsko/organy ścigania
	Tohir Yo'ldosh	2001–2009	zabity przez służby specjalne/ /wojsko/organy ścigania
	Usman Jan	2009– 2012	zabity przez służby specjalne/ /wojsko/organy ścigania
	Usman Ghazi[33]	2012	czynny
jaish-e-Mohammed (JEM) (Army of Mohammed)[34]	Maulana Masood Azhar	2000–do dziś	czynny
Jemaah Islamiya organization (JI)[35]	Abu Bakar Bashir	1993–2000	aresztowany
	Abu Rusdan	2000–2003	aresztowany
	Abu Dujana	2003–2007	aresztowany
	Hambali	?–?	aresztowany
	Azahari bin Husin	?–2005	zabity przez służby specjalne/ /wojsko/organy ścigania
	Zarkasih	? –?	aresztowany
Kahane Chai (Kach)	Binyamin Ze'ev Kahane	1990–2000	zabity przez inną organizację terrorystyczną
	Efraim Hershkovits[36]	2001–2003	emerytura
Kata'ib Hizballah (KH)[37]	Abu Mahdi al-Muhandis (Jamal Ja'far Muhammad)	2003–do dziś	czynny
Kongra-Gel (KGK, kiedyś Kurdistan Workers' Party, PKK, KADEK)	Abdullah Ocalan	1978–1999	aresztowany
	Murat Karayilan	1999–do dziś	czynny
lashkar-e Tayyiba (LT) (Army of the Righteous)[38]	Hafiz Saeed	1990–2001	aresztowany

[30] R. Sandee, *The Islamic Jihad Union* [online], http://www.nefafoundation.org/miscellaneous/FeaturedDocs/nefaijuoct08.pdf.

[31] *US-Bombe tötet Sauerland-Drahtzieher* [online], http://www.bz-berlin.de/aktuell/welt/us-bombe-toetet-sauerland-drahtzieher-article605155.html.

[32] B. Roggio, *Islamic Movement of Uzbekistan confirms leader Tahir Yuldashev killed* [online], http://www.longwarjournal.org/archives/2010/08/islamic_movement_of_1.php ; C. Moore, *The Rise and Fall of the Islamic Jihad Union: What Next for Uzbek Terror Networks?* [online], http://www.jamestown.org/programs/gta/single/?tx_ttnews%5Btt_news%5D=36251&tx_ttnews%5BbackPid%5D=457&no_cache=1.

[33] Zob. http://www.longwarjournal.org/archives/2012/08/imu_announces_death_1.php.

[34] Zob. http://www.satp.org/satporgtp/countries/india/states/jandk/terrorist_outfits/jaish_e_mohammad_mujahideen_e_tanzeem.htm.

[35] Z. Abuza, *Abu Dujana: Jemaah Islamiyah's New al-Qaeda Linked Leader* [online], http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=723.

[36] *Global Terrorist Organisations* [online], http://www.worldstatesmen.org/Terrorist.html.

[37] Zob. http://www.pvtr.org/pdf/GroupProfiles/Kata'ibHezbollah-05March10.pdf.

[38] S. Tankel, *Lashkar-e-Taiba. Past Operations and Future Prospects* [online], http://newamerica.net/sites/newamerica.net/files/policydocs/Tankel_LeT_0.pdf.

Lashkar i Jhangvi (LJ) [39]	Malik Ishaq[40]	1996–1997	aresztowany
	Riaz Basra[41]	1996/97–2002	zabity przez służby specjalne/ /wojsko/organy ścigania
	Akram Lahori	2002	aresztowany
liberation Tigers of Tamil Eelam (LTTE) [42]	Vellupillai Prabakharan	1976–2009	zabity przez służby specjalne/ /wojsko/organy ścigania
libyan Islamic Fighting Group (LIFG) [43]	Abd al-Ghaffar al-Duwadi	1992–1995	aresztowany
	Abu Abdullah al-Sadiq (Abd al Hakim-Belhadj)	1995–?	aresztowany
	Abu Layth al Libi[44]	2007–2008	zabity przez służby specjalne/ /wojsko/organy ścigania
moroccan Islamic Combatant Group (GICM)[45]	Mohamed Guerbouzi (?)	1998(?) – do dziś	czynny
National Liberation Army (ELN)	Fabio Vásquez Castaño[46]	1964–1973	śmierć z przyczyn naturalnych
	Antonio García Manuel Pérez Martínez[47]	1973–1998	śmierć z przyczyn naturalnych
	Nicolás Rodríguez Bautista[48]	1998–do dziś	czynny
Palestine Liberation Front (PLF)	Ahmed Jibril	1959–1967/77	odejście z organizacji
	Muhammad Zaidan (Abu Abbas)	1977–2003	aresztowany
Palestinian Islamic Jihad (PIJ)	Fathi Shaqaqi	1979–1995	zabity przez służby specjalne/ /wojsko/organy ścigania
	Ramadan Abdullah Mohammad Shallah[49]	1995–do dziś	czynny

[39] FTO była od początku zarządzana przez triumwirat przywódców. Zob. A. Roul, *Lashkar-e-Jhangvi: Sectarian Violence in Pakistan and Ties to International Terrorism* [online], http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=497.

[40] B. Roggio, *Pakistan releases Lashkar-e-Jhangvi commander* [online], http://www.longwarjournal.org/threat-matrix/archives/2011/07/pakistan_releases_lashkar-e-jh.php.

[41] Zob. http://www.satp.org/satporgtp/countries/pakistan/terroristoutfits/lej.htm.

[42] A. Bandarage, *The Separatist Conflict in Sri Lanka*, London 2009, Routledge, s. 66.

[43] Zob. C. Tawil, *Brothers in arms: the story of al-Qa'ida and the Arab jihadists*, London 2010, SAQI, s. 53, 64, 181.

[44] *A strike against al-Qaeda* [online], http://www.economist.com/node/10632193?story_id=10632193.

[45] M. Darif, *The Morrocan Combat Group* [online], http://www.realinstitutoelcano.org/analisis/465/ARI-51-2004-I.pdf.

[46] *Cronologia del ELN* [online], http://www.semana.com/documents/Doc-4_2006216.pdf.

[47] *La cuna de los Curas Guerilleros* [online], http://www.eln-voces.com/index.php?option=com_content&view=article&id=153:nacio1insu099&catid=44:identidad&Itemid=110.

[48] *La muerte del 'Cura Perez' echa sombras en el dialogo colombiano* [online], http://www.pagina12.com.ar/1998/98-04/98-04-08/pag22.htm.

[49] FBI, *Most Wanted Terrorists – Ramadan Abdullah Mohammad Shallah* [online], http://www.fbi.gov/wanted/wanted_terrorists/ramadan-abdullah-mohammad-shallah/view.

popular Front for the Liberation of Palestine (PFLP) [50]	George Habash	1967–2000	emerytura
	Abu Ali Mustafa[51]	2000–2001	zabity przez służby specjalne/ /wojsko/organy ścigania
	Ahmed Sadat	2001–2002[53]	aresztowany
	Ahmed Jibril[52]	2002–do dziś	czynny
pFLP-General Command (PFLP-GC)	Ahmed Jibril	1968–do dziś	czynny
al-Qaida in Iraq (AQI)	Abu Musab al Zarqawi	2004–2006	zabity przez służby specjalne/ /wojsko/organy ścigania
	Abu Hamza al Mujahir	2006–2010[55]	zabity przez służby specjalne/ /wojsko/organy ścigania
	Nasser al Din Allah Abu Suleiman	2010– do dziś	czynny
	Abu Bakr al-Baghdadi al-Husseini al-Qurshi[54]	2010(?)–2012	aresztowany
al-Qa'ida (AQ)	Osama bin Laden	1988–2011	zabity przez służby specjalne/ /wojsko/organy ścigania
	Ayman al Zawahiri	2011–do dziś	czynny
al-Qa'ida in the Arabian Peninsula (AQAP) [56]	Yusuf al-Uyayri	1997–2001, 2002–2003	zabity przez służby specjalne/ /wojsko/organy ścigania
	Abd al Rahim al Nashiri	2002	aresztowany
	Khaled Ali Hajj	2003–2004	zabity przez służby specjalne/ /wojsko/organy ścigania
	Abdel Aziz Issa Abdul-Mohsin Al-Muqrin	2004	zabity przez służby specjalne/ /wojsko/organy ścigania
	Sa'ud al-Utaybi	2004–2005	zabity przez służby specjalne/ /wojsko/organy ścigania
	Salih al-Alawi	2005	zabity przez służby specjalne/ /wojsko/organy ścigania
	Fahd al-Juwayr	2005–2006	zabity przez służby specjalne/ /wojsko/organy ścigania
	Nasir Abdel Karim al-Wuhayshi[57]	2009–do dziś	czynny

[50] Zob. *PFLP, DFLP, PFLP-GC, Palestinian leftists* [online], http://www.cfr.org/israel/pflp-dflp-pflp-gc-palestinian-leftists/p9128.

[51] *Israel kills key Palestinian leader* [online], http://news.bbc.co.uk/2/hi/middle_east/1511515.stm.

[52] Zob. http://www.cfr.org/israel/pflp-dflp-pflp-gc-palestinian-leftists/p9128.

[53] *Jailed PFLP leader: Only a one-state solution is possible*" [online], http://www.haaretz.com/news/diplomacy-defense/jailed-pflp-leader-only-a-one-state-solution-is-possible-1.288412.

[54] Zob. http://www.aljazeera.com/news/middleeast/2012/12/201212214201962755.html.

[55] *U.S.: Al-Qaida in Iraq warlord slain* [online], http://rss.msnbc.msn.com/id/36664251/ns/world_news-mideastn_africa/.

[56] Zob. T. Hegghammer, *Jihad in Saudi Arabia. Violence and Pan-Islamism since 1979*, London, Cambridge University Press.

[57] *Al-Qa'ida in the Arabian Peninsula (AQAP*) [online], http://www.nctc.gov/site/groups/aqap.html.

al-Qaida in the Islamic Maghreb (formerly GSPC)[58]	Hassan Hattab	1998–2003	rezygnacja z członkowstwa w FTO
	Nabil Sahraoui	2003–2004	zabity przez służby specjalne/ /wojsko/organy ścigania
	Abdelmalek Droukdal	2004–do dziś [59]	czynny
Real IRA (RIRA)	Michael McKevitt	1997–2002	usunięty z organizacji[60]
revolutionary Armed Forces of Colombia (FARC)	Manuel Marulanda	1964–2008	śmierć z przyczyn naturalnych
	Alfonso Cano[61]	2008–2011	zabity przez służby specjalne/ /wojsko/organy ścigania
	Timoleón Jiménez alias Timochenko[62]	2011–do dziś	czynny
Revolutionary Organisation 17 November (17N)	Alexandros Giotopoulos	?–2002	aresztowany
	Dimitris Koufondinas	1975–2002	poddał się władzom
Revolutionary People's Liberation Party/Front (DHKP/C)	Dursun Karataş	1978–2008	śmierć z przyczyn naturalnych
	Zerrin Sarı[63]	2008–do dziś	czynny
Revolutionary Struggle (RS)	Nikos Maziotis[64]	2003–2010	aresztowany
shining Path (Sendero Luminoso, SL)[65]	Abimael Reynoso Guzmán	1980–1992	aresztowany
	Oscar Ramírez Durand	1992–1999	aresztowany
	Comrade Artemio[66]	1999–2012	aresztowany
united Self-Defense Forces of Colombia (AUC)	Carlos Castaño Gil	1997–2004	zabity w wyniku wewnętrznych sporów w FTO
	Vicente Castaño Gil[67]	2004–2006	czynny?
Harakat-ul Jihad Islami (HUJI)	Qari Saifullah Akhtar	1980[68]–2004– (możliwe, że do dziś)	aresztowany

[58] Zob. C. Tawil, *Brothers in arms*..., s. 194–195.

[59] G.D. Porter, *The Impact of Bin Ladin's Death on AQIM in North Africa* [online], http://www.ctc.usma.edu/posts/the-impact-of-bin-ladin's-death-on-aqim-in-north-africa.

[60] D. McKittrick, *Real IRA rift exposed by prisoners' scathing attack* [online], http://www.independent.co.uk/news/uk/home-news/real-ira-rift-exposed-by-prisoners-scathing-attack-608261.html.

[61] S. Brodzinsky, *New FARC offensive suggests shift in Colombian rebels' strategy* [online], http://www.csmonitor.com/World/Americas/2011/0616/New-FARC-offensive-suggests-shift-in-Colombian-rebels-strategy 08827729.

[62] Zob. http://www.reuters.com/article/2011/11/16/us-colombia-rebels-idUSTRE7AF2DJ20111116.

[63] *DHKP/C leader buried, another lead figure caught in Greek Cyprus* [online], http://www.today-szaman.com/newsDetail_getNewsById.action?load=detay&link=150338.

[64] *Terrorist suspects freed pending trial* [online], http://www.phantis.com/news/terrorist--suspects-freed-pending-trial.

[65] Zob. F. Hyland, *Peru's Shining Path Gaining Ground?* [online], http://www.jamestown.org/single/?no_cache=1&tx_ttnews%5Btt_news%5D=4393.

[66] Zob. http://www.peruviantimes.com/05/peru-captures-shining-path-leader-in-upper--huallaga/15474/

[67] *Colombia convicts No. 1 fugitive paramilitary boss* [online], http://www.boston.com/news/world/latinamerica/articles/2011/03/17/colombia_convicts_no_1_fugitive_paramilitary_boss/.

[68] Zob. http://www.satp.org/satporgtp/countries/pakistan/terroristoutfits/HUJI.HTM.

Tehrik-e Taliban Pakistan (TTP)[69]	Baitullah Mehsud	2007–2009	zabity przez służby specjalne/ /wojsko/organy ścigania
	Hakimullah Mehsud	2009–do dziś	czynny
Jundallah[70]	Abdolmalek Rigi	2003–2010	aresztowany
	Muhammad Dhahir Baluch[71]	2010–do dziś	czynny
Army of Islam (AOI)[72]	Mumtaz Dughmush	2005–do dziś	czynny
Indian Mujahede-en (IM)	?	?	?
Jemaah Anshorut Tauhid (JAT)	Abu Bakar Ba'asyir	2008–do dziś	czynny
Abdallah Azzam Brigades (AAB)	Majid bin Muhammad al Majid[73]	2012–do dziś	czynny
Haqqani Network (HQN)	Jalaluddin Haqqani	?–?	czynny

[69] Zob. S.S. Shahzad, *Inside Al-Qaeda and the Taliban. Beyond bin Laden and 9/11*, London 2011, Pluto Press.

[70] S. Peterson, *Iran, still haunted by Jundallah attacks, blames West* [online] http://www.csmonitor.com/World/Middle-East/2010/1215/Iran-still-haunted-by-Jundallah-attacks-blames-West.

[71] Zob. http://www.aljazeera.com/news/middleeast/2010/02/201022816304613842 2.html.

[72] *Army Of Islam Designation* [online], http://www.voanews.com/policy/editorials/Army-Of-Islam-Designation-123116233.html.

[73] Zob. http://www.longwarjournal.org/archives/2012/06/abdullah_azzam_briga.php.

Źródło: Opracowanie własne autora.

Abstrakt

W ciągu ostatnich 12 lat „studia nad terroryzmem" zyskały na popularności w środowisku akademickim i eksperckim. W przeszłości większość z nich dotyczyła badań nad pojedynczymi aspektami działalności konkretnej organizacji terrorystycznej, tj. nad jej historią, działalnością, osiągnięciami, porażkami itd., lub przyjętych przez dane państwo metod jej zwalczania. Ostatnie lata to początek nowego trendu – studiów nad końcem terroryzmu. Studia te dotyczą wielu stron działalności organizacji terrorystycznych, w niewielkim jednak stopniu skupiają się na analizowaniu roli i funkcji przywódców grup, organizacji i siatek terrorystycznych. Niniejszy artykuł jest analizą próby badawczego wypełnienia tej luki oraz zapisem ustaleń odnoszących się do sukcesji terrorystycznego przywództwa w 51 organizacjach uznanych przez amerykański Departament Stanu za „zagraniczne organizacje terrorystyczne" (*foreign terrorist organizations* – FTOs). Wynikiem tej analizy jest konkluzja dotycząca dość dużej zdolności adaptacyjnej terrorystów, których przywódcy najczęściej utrzymywali się (lub utrzymują) na swoich stanowiskach przez długi okres i często skutecznie wychowują lub promują swoich następców.

Inną konkluzją jest przeświadczenie o słabościach procesu gromadzenia informacji – z analizy wynika, że brakuje wiadomości na temat rzeczywistej sytuacji danej grupy terrorystycznej. W takim przypadku tworzenie baz danych i przeprowadzanie badań statystycznych dotyczących grup, organizacji i siatek terrorystycznych jest trudne i wymaga powrotu do coraz mniej popularnego podejścia komparatywnego oraz skupiania uwagi badawczej na pojedynczych przypadkach aktów terrorystycznych, co powinno ułatwiać dokładne ustalenie sukcesji przywództwa w strukturach terrorystycznych.

Abstract

In the last 12 years "the studies on terrorism" have gained in popularity in the academic and expert circles. In the past, most of them concerned single aspects of the activity of a specific terrorist organization, i.e. its history, actions, achievements, defeats, etc., or methods of fighting terrorism that are applied by a specific country. In the last few years a new trend has emerged – studies on the end of terrorism. These studies concern many aspects of the activity of terrorist organizations, but they focus on analyzing the role and function of leaders of terrorist groups, organizations and networks only to a negligible extent. The article is an analysis of an attempt to fill a research gap in this question, and an analysis of the succession leaders of 51 organizations regarded by the American Department of State as "foreign terrorist organizations" (FTOs). The result of the analysis is a conclusion regarding a quite significant adaptive capability of terrorists, whose leaders most often held (or hold) their posts for a long period of time and often train or promote their successors effectively.

Another conclusion concerns the weaknesses of the process of information gathering. The analysis shows that there is no information on the actual situation of specific terrorist groups. In such case creating databases and conducting statistical research concerning terrorist groups, organizations and networks is very difficult and requires a return to a less and less popular comparative approach and focus of the research on single terrorist act, which should facilitate precise determination of the succession of leadership in terrorist structures.

Magdalena Adamczuk

Czeczeńskie kobiety w strategii działania bojowników kaukaskich

Terroryzm jako zjawisko jest od wielu lat szczegółowo analizowany przez badaczy i analityków. Mimo to jednak nadal brakuje jednoznacznej odpowiedzi na pytanie zasadnicze, tzn. co decyduje o sięganiu po tę konkretnie metodę realizacji celów przez organizacje terrorystyczne i pojedynczych terrorystów?

Po ponad dekadzie amerykańskiej „wojny z terroryzmem" USA oraz państwa je wspierające wciąż są zagrożone aktywnością o charakterze terrorystycznym. Pomimo doskonalenia narodowych mechanizmów przeciwdziałania terroryzmowi i wewnętrznych procedur reagowania na to zagrożenie, terroryzm jest nadal obecny i to w coraz to nowszych i doskonalszych formach. Jedną z nich jest niewątpliwie angażowanie kobiet do aktywnej walki z „wrogiem" oraz wykorzystywanie ich na coraz szerszą skalę do samobójczych misji. Rozpatrując udział kobiet w działalności terrorystycznej motywowanej ideologią islamską, należy zauważyć, że do lat 70. XX wieku[1] nie odnotowano żadnego zamachu, którego bezpośrednim sprawcą byłaby muzułmanka. To, że obecnie coraz częściej się je angażuje, może świadczyć o determinacji liderów organizacji terrorystycznych w ich dążeniach do zniszczenia świata zachodniego. Ale może być to także oznaka słabości i braku efektów dotychczasowych działań prowadzonych przez kobiety[2]. Doskonalenie procedur bezpieczeństwa i środków zapobiegania zagrożeniom skłaniają ugrupowania islamistyczne do poszukiwania nowych sposobów walki, które dawałyby im przewagę taktyczną. Rola kobiet w ogólnej strategii islamskich ekstremistów zazwyczaj była sprowadzana do działań logistyczno-zabezpieczających, wspierających aktywność bojowników. Istotne znaczenie ma tu wychowywanie i ukierunkowywanie dzieci w duchu prowadzenia dżihadu, niezależnie od tego, czy dzieje się to w Czeczenii, Palestynie, Iraku czy w innych krajach muzułmańskich. *To być może najważniejsza rola, jaką kobiety mają do odegrania w dżihadzie: wychować własne dzieci w taki sposób, ażeby stały się odważne i czułe, śmiałe i wrażliwe oraz by nie bały się nikogo poza Allachem. Wychować je w ten sposób nie tylko w duchu, ale i w znaczeniu zdolności fizycznych i wyszkolenia. A wychować tak nie tylko chłopców, ale i dziewczynki. Kluczem jest wpojenie im tych wartości, kiedy jeszcze są malutkie. Nie czekajcie z rozpoczęciem, aż będą miały 7 lat, ponieważ wtedy może być już za późno!*[3].

---

[1] Do pierwszego zamachu samobójczego dokonanego przez kobiety doszło 9 maja 1985 r. w Libanie. Przeprowadziła go członkini Syryjskiej Socjalistyczno-Narodowej Partii (SSNP) Khyadali San. Z kolei 27 stycznia 2002 r. Wafa Idris, pierwsza samobójczyni izraelska, dokonała zamachu w Jerozolimie.

[2] W sierpniu 2001 r. Najwyższa Rada Islamska wydała fatwę (tj. opinię wysokiego uczonego-teologa muzułmańskiego wyjaśniającą kontrowersję teologiczną, teologiczno-prawną lub czysto prawną. Fatwa jest wydawana wyłącznie na piśmie – przyp. red). zachęcającą palestyńskie kobiety do walki z niewiernymi również w formie bezpośredniego uczestniczenia w zamachach. W maju 2004 r. Jusuf al-Karadawi – egipski duchowny, wydał fatwę, w której interpretował dokonany przez kobietę atak samobójczy jako „akt męczeństwa w służbie Allacha", stwierdzając, że kobieta może uczestniczyć w dżihadzie nawet bez pozwolenia swojego męża, za: B. Bolechów, *Terroryzm, aktorzy, statyści, widownie,* Warszawa 2010, Wydawnictwo Naukowe PWN, s. 201.

[3] *Rola sióstr w dżihadzie* [online], http://qoqaz.bizland.com [dostęp: 10 X 2012].

Kobiety są wykorzystywane także podczas rekrutowania potencjalnych zamachowców-samobójców. Zazwyczaj wzbudzają większe zaufanie społeczne, przez co efektywność procesu rekrutacyjnego jest większa. Dodatkowo pozyskiwanie innych kobiet przez kobiety wywołuje określony efekt społeczny świadczący o słuszności sprawy, o jaką walczą bojownicy, a tym samym wzmacnia oddziaływanie na potencjalnych rekrutów i zwiększa liczbę walczących. Nie bez znaczenia dla rekrutacji jest również wykorzystywanie więzi rodzinnych. Na przykład Arbi Barajew zwerbował dwie kuzynki[4], a Raisa Ganijewa co najmniej pięć kobiet, w tym dwie swoje siostry, które później wzięły udział w zamachu podczas spektaklu *Nord-Ost* w Moskwie.

Z punktu widzenia strategii działania ugrupowań religijnych decyzja o wykorzystywaniu kobiet do przeprowadzania zamachów wywołuje pewien dysonans między korzyściami operacyjnymi i społecznymi a oporem kulturowym. Wynik końcowy, który przynosi dodatkowe korzyści, przeważa jednak przy podejmowaniu decyzji o ich zaangażowaniu w działania terrorystyczne. Już sam zamach samobójczy wywiera ogromny wpływ psychologiczny na społeczeństwo, sieje strach i panikę. Jeśli przeprowadza go kobieta, to jego wydźwięk medialny i spektakularność są zdecydowanie większe. Jeszcze do roku 2000 zamach samobójczy dokonany przez czeczeńską szahidkę był poza wyobrażeniem społecznym, a profil kaukaskiego zamachowca w żaden sposób nie był utożsamiany z powszechnym stereotypem kobiety jako osoby nieskłonnej do używania przemocy, słabszej, wrażliwej i niegroźnej. To sprawiało, że muzułmanki nie znajdowały się w kręgu zainteresowań służb policyjnych i specjalnych i łatwiej im było uniknąć przeszukań. Dawało to bojownikom przewagę taktyczną, skutecznie wykorzystywaną w kolejnych latach konfliktu. Paradoksalnie jednak, jak pokazują badania, kobiety są zazwyczaj bardziej zdeterminowane i bezwzględne, są bardziej tolerancyjne, jeśli chodzi o cierpienie fizyczne i psychiczne, oraz są zdolne do większego poświęcenia się dla idei, zwłaszcza jeśli ta staje się sensem ich życia.

Zjawisko i psychologia kobiecego dżihadu nie są do końca zbadane, w związku z czym trudno dostosować właściwe i efektywne środki prewencyjne i systemy osłabiające procesy radykalizacji i indoktrynacji ewentualnych zamachowczyń. W połączeniu z faktem, iż zamachom samobójczym z założenia trudno jest przeciwdziałać, a ściganie ich współsprawców (inspiratorów) jest skomplikowane, zamachy dokonywane przez kobiety powodują dodatkowe zaskoczenie i zwiększają szanse powodzenia ataku.

Wielowątkowe prace badawcze nad fenomenem czeczeńskich „czarnych wdów”[5] rozpoczęto po spektakularnym ataku na teatr na Dubrowce (Moskwa), przeprowadzonego w trakcie spektaklu *Nord-Ost*. Wówczas to 19 kobiet z materiałami przymocowanymi do ciała i 21 bojowników wzięło ponad 800 zakładników[6]. Liczba kobiet zaangażowanych w ten atak była jak do tej pory niespotykana i wywołała grozę oraz obawy o skalę radykalizacji czeczeńskich kobiet i wzrost potencjału operacyjnego terrorystów. Podobnie po ataku na szkołę w Biesłanie w 2004 r.[7] nastąpił przełom w myśleniu o granicy okrucieństwa, jakiego mogą dokonać rzekomo walczący o nie-

[4] Chawa Barajewa, Luiza Magomadowa – pierwsze czeczeńskie szahidki, które 6 czerwca 2000 r dokonały zamachu na bazę wojskową w Alkhan-Yurt w Czeczenii 6, patrz: tabela, poz. 1.

[5] Termin „czarne wdowy” został utworzony na potrzeby mediów przez zachodnie społeczeństwa i rosyjskich dziennikarzy. Większość „czarnych wdów” to muzułmanki, wdowy po bojownikach kaukaskich, ubierające się w tradycyjne czarne burki. Pierwsze „czarne wdowy” zostały zwerbowane przez czeczeńskich bojowników, prawdopodobnie pod przywództwem Szamila Basajewa.

[6] Patrz: tabela, poz. 5.

[7] Patrz: tabela, poz. 19.

podległość Czeczeni. Zamach był spektakularny, gdyż terroryści po raz pierwszy na tak szeroką skalę wykorzystali jako zakładników dzieci, które w konsekwencji padły ich ofiarami. Spowodowało to zarówno w Rosji, jak i w krajach kaukaskich poczucie wszechogarniającego niebezpieczeństwa i, wbrew oczekiwaniom zamachowców, zupełny brak zrozumienia dla ich sprawy w ogólnoświatowej opinii.

Wymienione wyżej argumenty – niewątpliwie przemawiające za skutecznością ataków – ukazują jednak punkt widzenia jedynie inspiratorów, pomysłodawców (liderów organizacji), którymi nie zawsze są same zamachowczynie. Kobieca natura wydaje się stać w sprzeczności z zadawaniem bólu i śmierci innym (zwłaszcza dzieciom i matkom). Udział kobiet w przeprowadzaniu samobójczych zamachów niewątpliwie nadał nowy wymiar postrzeganiu tego typu zjawiska.

Można wysnuć kilka hipotez, które w pewnym stopniu mogą pomóc zrozumieć psychologię i psychospołeczne aspekty zamachów (samobójczych) dokonywanych przez muzułmanki. Po pierwsze, z racji wyznawanej religii i kultywowanej idei męczeńskiej śmierci oczywiste wydaje się, że kobiety te giną w imię Allacha. Co jednak w sytuacji, gdy kobieta nie jest fanatyczną ekstremistką? W takiej sytuacji powodem podjęcia decyzji o przeprowadzeniu zamachu może być na przykład niezadowolenie z życia, niezrozumienie społeczne i depresja, które w połączeniu z umiejętną manipulacją przynoszą określony skutek. Z kolei, biorąc pod uwagę specyfikę takich rejonów, jak rejon kaukaski lub rejon konfliktu palestyńsko-izraelskiego, potwierdzenie znalazłaby teza, że giną one za kraj, w imię jego niepodległości i suwerenności oraz z zemsty za cierpienia, jakich doświadczyły lub jakich doświadczyli ich bliscy. A jeśli kobiety nie chcą ginąć, a są do tego zmuszane za pomocą środków odurzających lub szantażu moralnego, gdy są jedynie narzędziem, które uskutecznia strategię działania danej organizacji?. Czy ocena ich działań będzie jednoznaczna, a wina określona jedynie na podstawie skutku? Zawężając analizę zamachów do aktów dokonywanych jedynie przez czeczeńskie „czarne wdowy", należy zadać pytanie, czy każda z nich działa z podobnych pobudek. Fenomen „czarnych wdów" jest zagadnieniem niezwykle interesującym z punktu widzenia badania terroryzmu, równocześnie jednak niezmiernie trudnym do jednoznacznej oceny.

1. Motywy podejmowania działań terrorystycznych w zależności od rejonu świata

Rozpatrując problem samobójczych zamachów dokonywanych przez kobiety, do których dochodzi z niejednakową intensywnością w różnych rejonach świata, należy zwrócić uwagę na różnorodny profil psychologiczny tych kobiet, środowisko, w jakim żyją, i motywy, dla których podejmują się aktywności zbrojnej.

W kulturze krajów muzułmańskich męczeńska śmierć, na którą decydują się przede wszystkim kobiety, nie zawsze jest pochwalana. Wystarczy porównać, jak są odbierane przez opinię publiczną dokonujące zamachów Palestynki, a jak czeczeńskie „czarne wdowy". W świadomości Palestyńczyków i w palestyńskich mediach aktywność terrorystyczna jest ukazywana jako konieczność reagowania i właściwa odpowiedź na przemoc ze strony Izraela. Męczennicy są uznawani za bohaterów ginących za naród, a szerzące się powszechnie propaganda i specjalne programy edukacyjne dla najmłodszych od najwcześniejszych lat kształtują w dzieciach pragnienie oddania życia za Allacha i Palestynę. W Rosji natomiast panuje milczenie. (…) *Wstydliwe milczenie. Nikt nie chce znać nazwisk tych kobiet, nikt nie chce wiedzieć, dlaczego zdecydowały*

się umrzeć. Rodzice odwracają wzrok, gdy pytać o ich zmarłe córki. W Palestynie bycie terrorystką-samobójczynią jest zaszczytem, tutaj zaś hańbą. Wszyscy milczą (…)[8].

W innych rejonach świata uciekanie się do zamachów z udziałem kobiet jest elementem nowej taktyki wykorzystywanej bezpośrednio przez organizacje lub pośrednio do indoktrynowania społeczeństwa i prowadzenia propagandy islamistycznej. Zanim zamachy zaczęły przeprowadzać kobiety, to wielu samobójczych ataków dokonali mężczyźni. Ale w Czeczenii to właśnie kobiety zapoczątkowały walkę w tej formie. Prawdopodobnie ma to związek z kodeksem honorowym Czeczenów, zgodnie z którym samobójstwo jest tchórzostwem, zemsta za krzywdy natomiast jest w społeczeństwie mocno zakorzeniona. Morderstwo powinno być pomszczone morderstwem. Kobiety mają jednak zezwolenie na dokonanie zemsty samodzielnie tylko w sytuacji, gdy w ich rodzinach nie ma żadnych mężczyzn. Jest to warunek, który niewątpliwie ma duży wpływ na fakt, że „czarne wdowy" to w większości kobiety, które straciły mężów, synów czy całe rodziny w czasie konfliktu rosyjsko-czeczeńskiego.

Badając zamachy „czarnych wdów" na podstawie ogólnodostępnych informacji, można się dowiedzieć, że zdarzały się przypadki, gdy inspiratorzy, nie mając przekonania o gotowości kobiety do złożenia ofiary z siebie, zdalnie detonowali przymocowany do niej pas szahida lub ładunek umieszczony np. w jej plecaku[9]. W Palestynie kobiety dokonują eksplozji zazwyczaj samodzielnie.

W przeciwieństwie do ugrupowań nacjonalistycznych w Palestynie czy Afganistanie, kobiety czeczeńskie od początku brały aktywny udział w walce o wolność i akceptowały przemoc w kwestiach politycznych. Także w takich krajach jak Irak czy Pakistan kobiety włączyły się do zbrojnego dżihadu znacznie później niż kobiety w Czeczenii. W Iraku punktem zwrotnym było zaaprobowanie przez iracką Al-Kaidę włączenia kobiet do wszystkich faz operacji terrorystycznych w roku 2003. Od tego czasu nastąpił intensywny proces ich radykalizacji, który w niektórych przypadkach w połączeniu z desperacją (wynikającą m.in. z hańby, odarcia z godności, braku środków do życia) sprawił, że decydują się na śmierć. Z kolei w Pakistanie pierwszy zamach dokonany przez szahidkę odnotowano dopiero w grudniu 2007 r.

Zamachowczynie z różnych rejonów konfliktów stanowią cały przekrój społeczny. Motywy ich działań, pomimo wielu cech wspólnych, nie pozwalają jednak określić ogólnego, uniwersalnego ich profilu. Chcąc dokonać analizy terroryzmu reprezentowanego przez Czeczenki, należy uwzględnić specyficzne środowisko, w jakim żyją, i okrucieństwa konfliktu rosyjsko-czeczeńskiego, jakiego doświadczają od lat.

2. Ogólny obraz konfliktu czeczeńsko-rosyjskiego

Należy zwrócić uwagę na zmianę, jaka zaszła w trakcie konfliktu czeczeńsko-rosyjskiego na przestrzeni ostatnich lat. Niewątpliwie działania z lat 90. XX wieku wymierzone w Rosję miały podłoże nacjonalistyczne i niepodległościowe. Poparcie społeczne dla działań bojowników było nieporównywalnie większe od obecnego. Narody kaukaskie, szczególnie Czeczeni, w wyniku cierpienia, przedłużającego się konfliktu i braku perspektyw na satysfakcjonujący obie strony kompromis, wydają się być już wyczerpani, a głęboko zakorzeniona u nich idea niepodległościowa

[8] J. Jusik, *Narzeczone Allacha. Terrorystki-samobójczynie z Czeczenii*, Katowice 2006, Videograf II, s. 10.

[9] Zarema Inarkajewa, patrz: tabela, poz. 4.

i silna motywacja do walki słabną. W czasie pierwszej wojny czeczeńsko-rosyjskiej (1994–1996) ataki były wymierzone głównie w rosyjskich żołnierzy i w przedstawicieli władz. Nie było żadnych samobójczych zamachów bombowych w wykonaniu Czeczenek. Zamachy, w których ginęli cywile, nie były standardem. Standardem stały się dopiero w następnej fazie intensyfikacji walk (2000–2009)[10]. Pojawienie się „czarnych wdów" wywołało w społeczeństwie lęk, tak pożądany przez terrorystów.

Od roku 1999 na terenie Czeczenii zaczęło obowiązywać prawo szariatu. Miało to swoje odbicie w czasie drugiej wojny czeczeńskiej, której głównym motywem nie było już dążenie do utworzenia wolnej Czeczenii, ale wielkiego kalifatu opartego na szariacie. Otworzyło to nowe drzwi do werbowania bojowników i uświadomiło muzułmanom obowiązek walki i poświęcenia dla Allacha. Zmianie uległy również cele działań. W poczuciu zamachowców ataki na osoby cywilne i zamachy samobójcze kobiet zaczęły być moralnie usprawiedliwione. Zaczęto również wyznaczać cele znajdujące się daleko poza granicami kraju. Zamach z 11 września 2001 r. w USA przełożył się również na sytuację w Rosji. Prezydent Putin wykazywał wzmożoną aktywność, aby działania bojowników kaukaskich były zakwalifikowane przez zachodnią społeczność jako jeden z frontów wojny z terroryzmem i globalne starcie Zachodu z islamem. Rok później, 23 października 2002 r., doszło do spektakularnego zamachu w Moskwie na teatr na Dubrowce, o czym była już wcześniej mowa. Czeczeńskie komando pod przywództwem Mowsara Barajewa wzięło ponad 800 zakładników podczas trwania spektaklu *Nord-Ost*. Terroryści zażądali zakończenia wojny rosyjsko-czeczeńskiej i wycofania z Czeczenii rosyjskich wojsk. W ataku wzięło udział 40 bojowników, w tym aż 19 „czarnych wdów". Dzięki nim liderzy wojny zdefiniowali siebie na nowo. Rosyjski rząd, marginalizując nacjonalistyczne cele Czeczenów, dążył do skupienia międzynarodowej uwagi na ich związku z globalnym ruchem dżihadystów[11]. Kreml ogłosił się uczestnikiem ogólnoświatowej krucjaty przeciw terroryzmowi spod znaku Al-Kaidy, a radykalnych czeczeńskich komendantów przedstawiał jako bojowników dżihadu[12].

Ciekawa w tym kontekście jest wypowiedź Szamila Basajewa, który jeszcze w maju 2002 r. powiedział, że *w dzisiejszych czasach ukształtowała sie taka sytuacja, gdy zachodnie rządy, a w pierwszej kolejności Ameryka, straszą cały świat terroryzmem. Oni wymyślili ten bardzo wygodny termin „międzynarodowy terroryzm", pod który można podciągnąć praktycznie każdego człowieka i każde państwo. Najbardziej interesujące jest to, że nie potrzeba żadnych dowodów, nikt się ich nie domaga. Cały świat znajduje się jakby w hipnozie, a ludzie prowadzeni są ku jakiejś przepaści, za którą jest tylko bezkres.* (…) *a gdzie się podziała tak zwana domniemana niewinność, gdzie się podziało prawo każdego człowieka do obrony, gdzie prawo człowieka do tego, aby się wytłumaczyć, aby mieć możliwość powiedzieć choćby słowo, zrobiłem to lub nie zrobiłem tego. Nikt o nic nie pyta* (…).[13]

---

[10] Na temat pierwszego samobójczego zamachu dokonanego przez czeczeńskie szahidki – Chawę Barajewą i Luizę Magomadową – patrz tabela 1, poz. 1.

[11] *Are the Chechen Black Widows Creating a New Culture?* [online] http://www.planetdata.net/ct/articles.php?story=36&page=2 [dostęp: 15 V 2012].

[12] *Milczenie czarnych wdów* [online], http://www.focus.pl/historia/artykuly/zobacz/publikacje/milczenie-czarnych-wdow/ [dostęp: 8 X 2012].

[13] A. Podrabinek, *Wywiad z Szamilem Basajewem* [online], 15 maja 2002 r., http://czeczenia.com.pl/content/view/586/144/ [dostęp: 15 X 2012].

3. Czeczeńskie szahidki – ofiary czy żądne zemsty morderczynie?

Obraz czeczeńskich szahidek jest często upraszczany i sprowadzany do obrazu kobiet zdesperowanych po stracie najbliższych z rąk rosyjskich żołnierzy – kobiety, dla których jedynym sensem życia staje się zemsta. Medialny wydźwięk zamachów przeprowadzanych przez kobiety ma z góry narzuconą pejoratywną ocenę, bez szerszego spojrzenia na cały proces „stawania się terrorystką" czy szukania prawdy i docierania do źródeł problemu. „Czarne wdowy" to nie typy współczesnych „samotnych wilków"[14]. Za każdą z takich kobiet stoi jej osobista motywacja, a często także naiwność, którą ktoś umiejętnie wykorzystuje do swoich politycznych celów. Pod przykryciem pomocy w ich zmaganiach z traumą przygotowuje się je do roli męczennic. Ktoś te męczennice zaopatruje w materiały wybuchowe i uczy obsługiwać urządzenia detonujące. Za każdym zamachem stoi zorganizowana sieć rekrutacyjno-indoktrynacyjna, której liderzy, wykorzystując sytuację społeczną i polityczną w Czeczenii, przygotowują skuteczne narzędzie siejące panikę i ciągły strach. Biorąc pod uwagę wiele innych czynników niezależnych od zamachowczyń, wydaje się, że nie sposób dokonać jednoznacznej oceny ich działań. Dlatego warto prześledzić główne motywy, którymi się kierują w swej terrorystycznej działalności.

Motywacja Czeczenów często różni się od tej, jaką przedstawiają rosyjskie władze, dyskredytując działania bojowników kaukaskich. Ukazują „czarne wdowy" jako kobiety werbowane spośród najbardziej ułomnych umysłowo mieszkanek aułów, przechodzące szkolenia w specjalnych górskich obozach, w których są gwałcone, narkotyzowane, hipnotyzowane, po czym stają się niezawodnymi, bezmyślnymi i bezwolnymi „żywymi bombami"[15]. Można tu przytoczyć przykład Elzy Gasujewej, która dokonała zamachu na generała Gajdara Gadżyjewa[16]. Wiadomo, że zamach ten był finansowany przez oddział Szamila Basajewa, jednak Elza nie dokonała tego czynu z pobudek czysto religijnych czy nacjonalistycznych. Jej mąż został aresztowany w czasie operacji „oczyszczającej" na terenie Urus-Martanu, po czym na jej oczach brutalnie zamordowany właśnie przez Gadżyjewa. Po ataku pojawił się oficjalny komunikat FSB przedstawiający Gasujewę jako wahabicką fanatyczkę, która dokonała zamachu na zasłużonego organizatora pokojowego życia Czeczenii. Gajdar Gadżyjew pośmiertnie otrzymał tytuł Bohatera Rosji[17].

---

[14] Warto zauważyć, że współcześnie można wyróżnić dwa typy zamachów dokonywanych przez indywidualne osoby: *lone wolf terrorism* i *solo terrorism*. O taktyce „samotnego wilka" *(lone wolf)* mówimy wtedy, gdy zamachy są całkowicie odizolowane od zorganizowanej grupy czy komórki terrorystycznej; *lone wolf* dotyczy jednak sytuacji, kiedy zamachów dokonują osoby, które nie są i nie były bezpośrednio ani pośrednio związane z organizacją terrorystyczną i nie podlegają jej dowództwu. Inspirację do podjęcia dżihadu skupioną na atakowaniu „miękkich" celów za pomocą wszelkich dostępnych środków czerpią m.in. z mediów i internetu, dzięki którym przeszły intensywną i gwałtowną radykalizację. Z kolei *solo terrorism* charakteryzuje się tym, że poszczególnych zamachów dokonują osoby, które z własnej inicjatywy szukają kontaktu z organizacjami terrorystycznymi, nie są jednak ich członkami, a jedynie sympatykami. Zradykalizowana, głównie przez internet, jednostka może planować i dokonywać ataku zgodnie z instrukcją i sugestią innych osób lub po odbyciu wcześniejszego szkolenia w obozach treningowych czy przebywaniu w strefie „konfliktu". W konsekwencji jednak działa indywidualnie i bez powiązań z grupą.

[15] *Milczenie czarnych* … [dostęp: 8 X 2012].

[16] Patrz: tabela, poz. 3.

[17] *Samobójczynie z Czeczenii* [online], http://www.polityka.pl/swiat/analizy/1504698,1,samobojczynie-z-czeczenii.read [dostęp: 20 X 2012].

Główne motywy działania czeczeńskich kobiet można uogólnić i w pewnym uproszczeniu sklasyfikować w następujący sposób:

- **Osobista trauma powiązana z motywem społecznym.** Na podstawie przeprowadzonych analiz stwierdzono, że w żadnym z przypadków nie dostrzeżono poważnych typowych zaburzeń osobowości kobiet-samobójczyń przed podjęciem decyzji o włączeniu się do dżihadu. Dowiedziono jednak, że każda z nich doświadczyła głębokiej traumy i stresu pourazowego, a także zaburzeń dysocjacyjnych, które stanowią mechanizm obronny przed doznanymi urazami psychicznymi. Wydaje się więc, że trauma jest silnym bodźcem, który popycha je na drogę męczeństwa, ale nie jedynym. Nie wiadomo, czy jeśli wyżej wymieniony motyw byłby jedyny, nie wzmocniony innymi motywami, to odniósłby skutek w postaci samobójczej śmierci[18].

Ekstremalne doświadczenia, jakich doświadczały Czeczenki, wiążą się m.in. ze stratą najbliższych członków rodziny (mężów, dzieci) w wyniku bombardowań, wybuchów min lądowych czy w wyniku tzw. czystek przeprowadzanych przez rosyjskich żołnierzy. W wielu przypadkach skutkowało to u nich kryzysem psychicznym, depresją, społecznym wyobcowaniem i izolacją oraz agresją i silnym pragnieniem zemsty[19]. W wielu wypadkach po doznanej krzywdzie kobiety z własnej inicjatywy szukały kontaktu z przedstawicielami ideologii wahabickiej, silnie rozprzestrzenionej na terenach kaukaskich. Część z nich była związana z bojownikami już wcześniej poprzez więzy krwi czy małżeństwo i w wysokim stopniu świadoma działań, jakie podejmują ich bliscy.

Kandydatki na szahidki są poddawane indoktrynacji, a na kilka tygodni przed planowanym atakiem są izolowane od świata zewnętrznego w obozach szkoleniowych, w których poprzez odpowiednią psychomanipulację i wykorzystanie traumy, jakiej doświadczyły, określa się im na nowo sens życia i podsyca u nich chęć zemsty.

Czynnikiem, który potęguje motyw traumy jako elementu warunkującego dokonanie zamachu, jest kwestia postrzegania przez społeczeństwo kobiet odrzuconych przez mężów, które zostały zhańbione z powodu niewierności lub stosunków pozamałżeńskich czy posiadania nieślubnych dzieci. Śmierć męczennicy ma zmazać jej winę i przywrócić honor. Przypadki celowego wykorzystywania seksualnego kobiet przez członków organizacji, aby móc je później szantażować ujawnieniem czynów czy taśm z nagraniem, prawdopodobnie również miały miejsce w Czeczenii. W takich przypadkach z jednej strony społeczna presja, a z drugiej strach stają się silniejsze niż instynkt samozachowawczy skrzywdzonej kobiety.

Część „czarnych wdów" była emocjonalnie związana z bojownikami, co zwiększało ich gorliwość i łatwość manipulowania nimi przez mężczyzn, którzy zachęcali je do terrorystycznej aktywności w imię Allacha. Tak na przykład było w przypadku Zaremy Inarkajewej, którą mężczyzna odwiózł na miejsce planowanego ataku, a wcześniej wymusił na niej nagranie, w którym mówiła o męczeńskiej śmierci i miłości do Allacha. Następnie zdalnie zdetonował ładunek (kobieta została ranna, ale przeżyła – patrz: tabela, poz. 4)[20]. Podobnie rzecz się miała z Zulichan Elichadżijewą, która

[18] A. Speckhard, K. Akhmedova, *Black Widows: The Chechen Female Suicide Terrorists* [online], http://mediaresearchhub.ssrc.org/black-widows-the-chechen-female-suicide-terrorists/attachment [dostęp: 3 X 2012].

[19] Tamże.

[20] Zamach z 5 lutego 2002 r., Grozny, Zawodskoj. Inarkajewa, gdy była już w budynku, w którym miała zdetonować ładunek, zdjęła plecak z materiałami wybuchowymi, co pozwoliło jej uniknąć śmierci. Nieświadomy jej zachowania mężczyzna zdalnie, z samochodu, zdetonował ładunek. W zamachu zginęły

postanowiła zostać męczennicą, aby uwolnić się od grzechu kazirodczego związku i grzesznej miłości.[21]

- **Zemsta**

Poglądy na temat moralnej podstawy zemsty panujące w społeczeństwie czeczeńskim są specyficzne. Etos zemsty za krzywdy i śmierć najbliższych jest często społecznie akceptowany. *Czeczeńskie dziewczęta, które wysadziły się w powietrze, miały za co się zemścić* (*rodzice zabici w bombardowaniach, bracia partyzanci, którzy polegli z rąk żołnierzy bądź zniknęli w jakimś rosyjskim „obozie filtracji"), a właśnie w zamachach kamikadze dostrzegły jedyny sposób, by tego dokonać. (...) W fanatyzmie znalazły jedyną pociechę dla swojej desperacji. W ich zdeformowanych przez wojnę umysłach islamski radykalizm doskonale połączył się ze starą plemienną zasadą zemsty – tragiczną mieszanką, która zapełniła Czeczenię potencjalnymi kamikadze. Jest to radykalizm nieznający granic*[22].

- **Ideologia religijna**

Trudno doszukiwać się w atakach samobójczych przeprowadzanych przez Czeczenki powodów czysto religijnych i łączyć je z islamem, gdyż dla większości islam stanowi jedynie element inspirujący i pozwalający nadać danemu czynowi odcień męczeństwa i traktować go jako przejaw chęci życia w raju. Osoby, które przeszły osobistą traumę, pozbawione wiary w wartości dotychczas nadrzędne, niejako same szukają nowego sensu życia i określenia swego światopoglądu na nowo. W przypadku dysocjacji i poczucia alienacji społecznej ideologia dżihadu łatwo wypełnia pustkę powstałą po tragicznych wydarzeniach, daje ujście, choć pozornie, negatywnym instynktom i uwalnia od psychicznych urazów. W takiej sytuacji zniekształcony obraz islamu jest umiejętnie wykorzystywany przez członków organizacji terrorystycznych i służy jedynie do osiągnięcia celów politycznych.

- **Zmuszanie do zamachów**

Kobiety dokonują samobójczych zamachów nie zawsze z własnej inicjatywy. Często pozbawione wsparcia młode dziewczyny są sprzedawane czy oddawane w ręce organizacji terrorystycznych za zgodą rodziny. Rzekomo kobietom, które się sprzeciwiają, lub tym, które nie są dostatecznie silnie zindoktrynowane i gotowe świadomie oddać życie, są podawane środki psychotropowe i odurzające[23]. Doskonałym przykładem kobiet, które nie do końca były świadome działań, jakie miały przeprowadzić, są zamachowczynie na teatr na Dubrowce. Materiał wybuchowy, który miały umieszczony w pasach szahida, okazał się nie być przystosowany do detonacji. W czasie szturmu kilka kobiet próbowało samodzielnie odpalić ładunek, ale się nie powiodło. Wszystkie zginęły od strzału w głowę z rąk rosyjskich komandosów. Z relacji rodzin wynika, że niektóre z nich, będąc prze-

23 osoby, a 17 zostało rannych. Inarkajewa jest pierwszą z „czarnych wdów", które przeżyły dokonywany przez siebie zamach. Została aresztowana, a dzięki jej zeznaniom wiadomo zdecydowanie więcej na temat procesu werbowania i indoktrynacji kobiet przez bojowników kaukaskich.

[21] *Szago, nie myśl, że Cię nie kocham lub o tobie nie myślę. Nie mam nikogo poza tobą na całym świecie i dlatego postanowiłam zostać bojowniczką w imię Allacha. (...). Nie idź tam, gdzie ukrywają się rebelianci, weź po prostu pas i bądź wojownikiem w imię Allacha. Potem będziemy mogli być razem. Nie pozostawaj na Ziemi, Szago. Przychodź szybko do mnie. Zostaw wszystko wszystkich za sobą (...)*, fragment listu pożegnalnego. Zob. J. Jusik, *Narzeczone Allacha*..., s. 112.

[22] *Czarne wdowy z Czeczenii* [online], www.tolerancja.pl/files/Dzieci_c.pdf, za: M. Manicangeli, *I kamikaze nella storia*, 2004, Datanews [dostęp: 28 X 2012].

[23] Wspomniana już wcześniej niedoszła samobójczyni Zarema Inarkajewa została zmanipulowana przez swojego kochanka. Była nieświadoma zadania, które miała wykonać – zlecono jej tylko „dostarczenie przesyłki". Przed zamachem była przez wiele dni narkotyzowana, o czym zeznała po zatrzymaniu.

konanymi, że wrócą żywe, zdecydowały się na udział w akcji z powodów finansowych; inne przekonane o powrocie do swych domów miały wykupione przez inspiratorów bilety podróżne w obie strony.

4. Zamachy z udziałem „czarnych wdów"

Dotychczas czeczeńskie „czarne wdowy" dokonały samodzielnie (bądź brały udział) w 27 zamachach samobójczych, w których łącznie zginęło 955 osób, a 2066[24] zostało rannych. Po raz pierwszy tę formę ataku wykorzystano w Czeczenii, w Ałchan-Jurcie, 7 czerwca 2000 r. Zamachu dokonały 17-letnia Chawa Barajewa[25] i jej 16-letnia koleżanka Luiza Magomedowa. Wykorzystując ciężarówkę UAZ wypełnioną materiałami wybuchowymi, podjechały pod biuro komendatury wojskowej, zabijając 15 rosyjskich żołnierzy. Był to moment przełomowy w strategii działań bojowników kaukaskich. Od tego czasu zamachy samobójcze kobiet stały się coraz powszechniejsze.

Po ataku na teatr na Dubrowce Szamil Basajew ogłosił powstanie żeńskiego islamskiego batalionu męczenników Rijadus Salichin[26] (znanego również pod nazwą Ogród Męczenników lub Rajskie Namioty). Według informacji przekazanych przez służby bezpieczeństwa około czterdziestu przeszkolonych i gotowych do akcji szahidek zostało ulokowanych w różnych rejonach Rosji. Prawdopodobnie jednymi z nich były Zulichan Elichadżyjewa i Miriam Szaripowa. Przeprowadziły one podwójny atak samobójczy na lotnisku w Tuszynie[27]. W samym tylko 2003 r. batalion Rijadus Salichin był odpowiedzialny za zamach przeprowadzony 14 maja w Ilishan-Jurcie (w jego wyniku 59 osób zostało zabitych, a 111 rannych) oraz za wybuch bomby w autobusie niedaleko bazy rosyjskich pilotów Air Force w Mozdoku (Osetia Północna) dokonany 5 czerwca przez Lidę Khildehorojewę (17 zabitych i 16 rannych).

Po okresie nasilonych ataków czeczeńskich szahidek w latach 2003–2004 i ich mniejszej aktywności w kolejnych latach, a także po śmierci Basajewa w 2006 r., w roku 2009 Doku Umarow ogłosił reaktywację Rijadus-Salichin i zintensyfikowanie zamachów dokonywanych przez szahidki[28].

---

[24] W tym w Biesłanie, gdzie brały udział dwie kobiety (385 zabitych, 730 rannych).

[25] Kuzynka jednego z najbardziej fanatycznych czeczeńskich komendantów polowych Arabi Barajewa (nazwana później „Mieczem Hidżabu"). W pozostawionym nagraniu wideo Barajewa zawarła swoje przesłanie: *Świetnie wiem, co robię. Raj ma swoją cenę i to jest ta cena za Raj. Tak, siostry, nadszedł nasz czas. Po tym, jak nieprzyjaciele zabili wszystkich naszych mężczyzn, naszych braci, ojców, synów i męczenników, nie pozostaje nic innego, jak tylko podjąć nasze zadanie, by ich pomścić. Nadeszła zatem chwila, byśmy i my wzięły w ręce broń w obronie naszej sprawy, naszej ziemi, przed wszystkimi tymi, którzy przynieśli nam śmierć. I nie można spocząć nawet, jeśli miałybyśmy zamienić się w męczennice na drodze do Allacha. Nie zatrzymamy się. Allach jest wielki* (…), za: K. Kęciek, *Szachidki i czarne wdowy* [online], http://www.przeglad-tygodnik.pl /index.php?site=artykul&id=7776 [dostęp: 20 X 2012].

[26] *Gdy nasze szahidy przybędą ponownie, ich jedynym celem będzie zadanie wrogowi maksymalnych strat. Zachwycamy się ich męstwem i zdecydowaniem. Oby Allach pozwolił nam równie dostojnie zakończyć swoje życie na Jego szlaku i w imię Jego. Allach Akbar* – amir batalionu Rijadus-Salihin-Abdullach Szamil Abu-Idrys (arabskie nazwisko Szamila Basajewa), http://iczkeria.fm.interia.pl/2004-07.html [dostęp: 6 VIII 2012].

[27] Patrz: tabela, poz. 11.

[28] *Bezpieczeństwo Mistrzostw Europy w Piłce Nożnej Euro 2012*, rozdz. III – *Zagrożenie terroryzmem podczas imprez masowych w kontekście zamachów w Rosji i na terenie Kaukazu Północnego*, K. Liedel, P. Piasecka (red. nauk.), Warszawa 2011, Difin.

Tabela. Statystyka zamachów przeprowadzanych na terenach kaukaskich przez kobiety w latach 2000–2012.

Lp.	Data	Miejsce	Zamachowiec	Ogólna liczba terro-rystów	Kobiety	Mężczyźni	Ofiary śmier-telne	Ranni	Zakład-nicy	Skutek dla terrorysty	Motyw (powiązania)	Sposób przeprowadzenia ataku
1	7 VI 2000	Czeczenia, Alkhan-Yurt, baza wojskowa	Chawa Barajewa, Luiza Magomadowa	2	2	0	2	5	0	śmierć	manipulacja przez mężczyznę, nieszczęśliwa miłości	ciężarówka wypełniona materiałem wybuchowym
2	XII 2000	Czeczenia, budynek Ministerstwa Spraw Wewnętrznych	Mareta Dudujewa	1	1	0	?	?	0	ranna, później zmarła	b.d.	b.d.
3	29 XI 2001	Czeczenia, Urus-Martan, dowództwo wojskowe	Elza Gasujewa	1	1	0	1	3	0	śmierć	zemsta, osobista nienawiść do wroga – mąż zginął z rąk żołnierzy rosyjskich, brat wskutek wybuchu miny; zwerbowana przez oddział Basajewa, który także finansował zamach	pas szahida
4	5 II 2002	Czeczenia, Grozny, Zawodskoj	Zarema Inarkajewa	1	1	0	23	17	0	ranna	zmanipulowana przez kochanka, nieświadoma zadania – miała dostarczyć przesyłkę, narkotyzowana, przed planowanym zamachem	plecak wypełniony materiałem wybuchowym, detonacja zdalna

5	23–26 X 2002	Moskwa, Dubrowka, spektakl „Nord-Ost”	Raiman Kurbanowa, Koku Chadzijewa, Aiman Chadzijewa, Seimat Alijewa, Asset Giszłurkajewa, Malisza Mutajewa, Zareta Bajrakowa, Luiza Bakujewa, Chadsztad Sulumbekowna Ganijewa, Fatima Sulumbekowna Ganijewa, Sura Bizijewa, Marina Bisułtanowa, Liana Chusenowa, Saira Jupajewa, Madina Dugajewa (?), Marjam Sura Marszugowa (wdowa po Salimchanie Achmadowie), Dżesira Witalijewa	40	19	21	129	644	800	śmierć	różne	wzięcie zakładników; zakładnicy zabici strzałem w głowę; pomimo pasów szahida kobiety nie dokonały samodetonacji
6	27 XII 2002	Czeczenia, Grozny, teren rządowy	b.d.	3	1	2	83	ok. 200	0	śmierć	b.d	dwie ciężarówki wypełnione materiałem wybuchowym
7	12 V 2003	Czeczenia, Ilishan-Jurt, budynek rządowy	Shakhida Baimuratowa	3	1	2	59	111	0	śmierć	niepotwierdzone informacje – rzekomo wdowa po bojowniku zmarłym na początku II wojny czecz-ros.	ciężarówka wypełniona materiałami wybuchowymi
8	14 V 2003	Czeczenia, Iliskhan-Yurt, festiwal religijny	Shahidat Shahbulatowa, Zulay Abdurzakowa	2	2	0	18	145	0	śmierć	b.d	pas szahida

9	5 VI 2003	Osetia Północna, Mozdok,baza rosyjskich pilotów Air Force	Lida Khildehorojewa	1	1	0	17	16	0	śmierć	b.d	bomba w autobusie
10	20 VI 2003	Czeczenia, Grozny, budynek rządowy	Zakira Abdulazimowa	2	1	1	6	38	0	śmierć	b.d	ciężarówka wypełniona materiałami wybuchowymi
11	5 VII 2003	lotnisko w Tuszyno, Moskwa, koncert rockowy	Zulichan Elichadżijewa, Zinajda Alijewa	2	2	0	14	60	0	śmierć	Zulichan Elichadżijewa – śmierć w imię Allacha jako zmazanie grzechu miłości kazirodczdzej; Zinajda Alijewa – trauma po aborcji, do której zmusił ją mąż bojownik. Po jego śmierci podjęła decyzję o śmierci własnej.	pas szahida
12	11 VII 2003	Moskwa, kawiarnia „Mon Cafe”	Zarema Muszachojewa	1	1	0	1	0	0	przeżyła	depresja, brak perspektyw; nie mając innego pomysłu na siebie, postanowiła przyłączyć się do wahabitów. „Przyjaciel” zaproponował jej 1000 dol. oraz obiecał opiekę nad jej córką i rodziną. Po nieudanym zamachu skazana na 20 lat więzienia.	pas szahida, poddała się policji pozostawiając ładunek

13	27 VII 2003	Czeczenia, Grozny, budynek bazy wojskowej	Mariam Tashukhadjiewa	1	1	0	?	?	0	śmierć	b.d.	pas szahida
14	5 XII 2003	Czeczenia		2	1	1	46	ok. 150	0	śmierć	b.d.	wybuch w pociągu podmiejskim
15	9 XII 2003	Moskwa, pobliże Kremla i budynku Dumy Państwowej	Khadishat Mangeriyewa	1	1	0	6	14	0	śmierć	wdowa po czeczeńskim bojowniku Rusłanie Mangerijewie, który zginął podczas operacji wojskowej w lipcu poprzedniego roku	pas szahida - detonacja zdalna
16	25 VIII 2004	samolot TU-134 Moskwa – Wołgorad, lot 1303	Sazita Jebirhanova	1	1	0	43	0	0	śmierć	odsunieta od męża bo nie mogła mieć dzieci, piętnowana z tego powodu jako niepełnowartościowa kobieta	detonacja ładunku w samolocie
17	25 VIII 2004	zamach na samolot TU-154 Moskwa–Soczi, lot 1047	Aminat Nogajewa	1	1	0	42	0	0	śmierć	uprowadzona przez bojowników, pozbawiona kontaktu z rodziną przez 3 lata przed dokonaniem zamachu	detonacja ładunku w samolocie
18	1–3 IX 2004	atak na szkołę w Biesłanie	32 bojowników, w tym dwie kobiety – Roza Nogaejewa i Mariam Tuborowa	32	2	30	385	730	1100	śmierć	b.d.	wzięcie zakładników przez terrorystów; w ostateczności szturm komandosów z użyciem gazu łzawiącego

19	15 IX 2004	Inguszetia, biuro FSB	b.d.	2	1	1	2	31	0	śmierć	b.d	b.d
20	6 XI 2008	Władykaukaz w Osetii Północnej	b.d.	1	1	0	12	40	0	śmierć	b.d	pas szahida – detonacja na przystanku w pobliżu ruchliwego targu w centrum miasta
21	16 IX 2009	Zawodskoj, Okręg Grozny – Mir Street w pobliżu Fashion House	b.d.	1	1	0	0	8	b.d	śmierć	b.d	pas szahida
22	29 III 2010	Rosja, Moskwa, podwójny atak na metro	Dzhennet Abdurakhmanowa, Maryam Sharipowa	2	2	0	40	102	0	śmierć	wdowa po Umalacie Magomedowie, który został zabity przez siły rosyjskie 31 grudnia 2009 r.; Maryam Sharipowa, żona Magomeda Wagabowa, jednego z przywódców bojowników dagestańskich	pas szahida
23	7 III 2012	Dagestan, Karabudakhkent, punkt kontrolny policji	Aminat Ibragimowa	1	1	0	5	2	b.d.	śmierć	żona Zaura Zagirowa, jednego z liderów bojowników, który został zabity w Dagestanie w lutym 2012 podczas operacji specjalnej wojsk rosyjskich	pas szahida

24	3 V 2012	Dagestan, Machaczkała, 2 wybuchy oraz atak na posterunek policji	Muslimat Alijewa	2	1	1	14	100	b.d	b.d	rodzeństwo Alijewej było zaangażowanie w działalność ekstremistyczną; na miesiąc przed atakiem zniknęło z domu i przyłączyło się do bojowników	materiały wybuchowe umieszczone w samochodach
25	28 VIII 2012	Dagestan, Chirkei, wybuch w domu Szejka Said-Afandi Al-Chirkawiego przywódcy duchowego	Aminat Kurbanowa		1	b.d	7	b.d.		b.d	jej dwaj byli małżonkowie byli islamskimi bojownikami, obecny również	pas szahida
26	**SUMA**			**106**	**48**	**59**	**955**	**2066**	**1900**			

Źródło: Opracowanie własne na podstawie informacji ogólnodostępnych.

5. Taktyka zamachów przeprowadzanych przez „czarne wdowy”

Jedną z najczęściej stosowanych technik przeprowadzania zamachów przez czeczeńskie szahidki jest wykorzystywanie w tym celu ciężarówek wypełnionych materiałem wybuchowym, detonowanym zdalnie przez „opiekuna” akcji lub bezpośrednio przez kobietę. Druga to wykorzystanie pasa szahida lub plecaka wypełnionego plastycznym materiałem wybuchowym zmieszanym z częściami metalowymi, gwoździami i granatami ręcznymi maksymalizującymi siłę rażenia i zwiększającymi liczbę ofiar. Zamachów przy użyciu samochodów dokonywano głównie w pobliżu ważnych strategicznie budynków czy punktów kontrolnych policji. Poza tym do jednego ataku doszło w pociągu[29], a do dwóch w samolotach[30] i w metrze[31]. Nie można pominąć też dwóch największych jak do tej pory przypadków przetrzymywania zakładników[32].

W początkowej fazie konfliktu ataki były kierowane przeciwko konkretnym celom policyjno-wojskowym. Z czasem, jak już wspomniano wyżej, zaczęto dokonywać zamachów spektakularnych, mających zadać jak największe straty wrogowi, bez względu na to, czy ofiarami będą postronni obywatele i dzieci, czy żołnierze. W momencie „zglobalizowania” konfliktu czeczeńsko-rosyjskiego po roku 2000 nastąpiło terytorialne rozszerzenie działań wojennych. Bojownicy rozpoczęli kampanie terrorystyczne w miejscach oddalonych od jądra konfliktu. Nadal jednak prawie połowa ataków jest przeprowadzanych w Czeczenii, mniej w Moskwie i w południowej Rosji.

W wielu przypadkach przyszła męczennica składała przed zamachem oświadczenie lub nagrywano jej wypowiedź o jej religijnej żarliwości i podjęciu przez nią decyzji o ewentualnej samobójczej śmierci w imię Allacha jako o największym zaszczycie połączonym z ideą nacjonalizmu religijnego. Rozpatrując problem zamachów terrorystcznych organizowanych przez kobiety w tym kontekście, należy stwierdzić, że z analizy biografii poszczególnych szahidek wiadomo, iż fundamentalizm religijny nie był głównym motywem ich decyzji.

Największa koncentracja ataków samobójczych dokonywanych przez kobiety nastąpiła latem 2003 r., po czeczeńskim referendum konstytucyjnym z 23 marca 2003 r., podczas którego przyjęto konstytucję Czeczenii określającą republikę jako nieodłączną część Federacji Rosyjskiej. W latach 2006–2007 nie odnotowano żadnego zamachu z udziałem „czarnych wdów”. W kolejnych latach jednak przeprowadziły one sześć ataków (w tym podwójny atak na moskiewskie metro w 2010 r., który przypomniał społeczeństwu rosyjskiemu i całemu światu, że wojna trwa nadal). Zginęło w nich ok. 80 osób.

Podsumowanie

Podsumowując rozważania, trudno jest jednoznacznie przychylić się do tylko jednej z hipotez przedstawionych w niniejszym artykule. Analiza wykazuje, że na decyzję czeczeńskich kobiet o podjęciu samobójczej misji ma wpływ złożona i skomplikowana interakcja czynników socjopolitycznych i psychologicznych, które są

[29] 5 grudnia, 2003 r. w Czeczenii – brak bliższych danych.

[30] Zamach na dwa samoloty TU-134 Moskwa–Wołgorad (lot 1303) oraz TU-154 Moskwa–Soczi (lot 1047) dokonany przez Sazita Jebirhanowa i Aminat Nogajewą 25 sierpnia 2004 r.

[31] Podwójny atak na stacji metra w Moskwie, przeprowadzony 29 marca 2010 r.

[32] Atak na teatr w Moskwie – październik 2002 r. (około 800 zakładników) oraz szkołę w Biesłanie we wrześniu 2004 (około 1100 zakładników).

mieszanką traumy i desperacji, a także manipulacji i indoktrynacji religijnej. Wszystkie te kobiety łączą tragiczne wydarzenia, za każdą z nich jednak kryje się inny, indywidualny, bodziec, który doprowadza je do postępowania skrajnego. Trudno zaakceptować sytuację, w której kobieta świadomie i dobrowolnie staje się zabójcą niewinnych osób, w tym dzieci, w imię osobistej zemsty czy w imię Allacha. Nie da się jednak zaprzeczyć faktom. Zapewne trzeba też wypośrodkować doniesienia i opinie obu stron konfliktu czeczeńsko-rosyjskiego i motywy ich radykalnych działań.

Niewątpliwie zniekształcona interpretacja islamu pomaga inspiratorom zamachów przekonać skrzywdzone i pozbawione środków do życia kobiety, a takich po latach wyczerpującej wojny jest zapewne wiele, do dokonywania ataków. Zamachy samobójcze przez nie przeprowadzone nie są zwieńczeniem ich pragnienia śmierci w imię Allacha. Radykalizacja postaw, którą często osiągają na krótko przed wykonaniem zadania, jest wartością dodaną, a nie decydującą. Wiele kobiet skorzystało z tej nowo powstałej możliwości wzięcia czynnego udziału w walce i rozpoczęło działania wykraczające poza ich tradycyjną rolę społeczną[33]. „Czarne wdowy" różnią się od siebie wiekiem, wykształceniem, środowiskiem, w jakim żyją, i religijnością, co sprawia dodatkowe trudności w ich ewentualnym sprofilowaniu i utrudnia przeciwdziałanie dokonywaniu przez nie samobójczych ataktów, zwiększając tym samym ich powodzenie. Z jednej strony nic nie jest w stanie usprawiedliwić czynów szahidek; żadna idea czy religia nie dają bowiem podstawy do zabijania. Z drugiej jednak mit fanatyczek islamskich ginących w imię islamu i ojczyzny nie znajduje potwierdzenia. Gdyby nie zaszczepienie w umysłach zdesperowanych kobiet tego, że śmierć jest dla nich najlepszym rozwiązaniem, i wykorzystanie ich do nadrzędnych celów grupy, same prawdopodobnie nie miałyby wystarczającej motywacji i środków do przeprowadzenia zamachów. Obserwując problem z tej perspektywy, wydaje się, że stają się one jedynie narzędziem w walce i ofiarą konfliktu. Przyjmując pewne uogólnienie, można stwierdzić, że zamachowczynie są tylko ogniwem w łańcuchu działań terrorystycznych, a wysyłający je do przepropwadzenia ataku organizatorzy stoją w centrum całej sieci powiązań i pociągają za sznurki. Zanim „czarna wdowa" stanie się męczennicą, wcześniej przechodzi „trening emocjonalny", który pomaga jej neutralizować oceny moralne, usuwa poczucie winy związane z planowanym zamachem i dehumanizuje jego ewentualne ofiary. W następstwie tego ma przekonanie o tym, że winni wszystkich krzywd są Rosjanie, szczególnie żołnierze i służby bezpieczeństwa, co pozwala jej na takie, a nie inne działanie. W przekonaniu tych kobiet i organizatorów ataków społeczeństwo rosyjskie to nie cywile, gdyż całe jest w stanie wojny[34].

Patrząc na fenomen kobiet skrywających prawdę o motywacji popychającej je do ekstremalnych zachowań pod czarną burką, należy zaznaczyć, że czeczeńskim wahabitom udało się zradykalizować tylko niewielką część czeczeńskich kobiet. Czeczeni generalnie opowiadają się za zakończeniem konfliktu i przeciwko przemocy politycznej ze strony służb realizujących działania w ramach operacji antyterrorystycznej. Nie popierają także zamachów jako metody, dzięki której ich kraj może zdobyć niezależność.

Terroryzm samobójczy bez wątpienia nadal będzie służył za skuteczną metodę realizacji celów politycznych przez organizacje terrorystyczne i na stałe wpisze się w działania ekstremistów, przeprowadzane w różnych częściach świata pod szyldem

[33] S. Mc Cutcheon, *„Czarne wdowy"*, Gdańsk 2010, VM Group, s. 76

[34] A. Berko, *Droga do raju. Świat wewnętrzny zamachowców-samobójców,* Zakrzewo–Poznań 2010, Replika, s. 294.

globalnego dżihadu. Aktywnie zaczynają w nim uczestniczyć także Europejki. Przykładem jest Belgijka Muriel Degauque, która była sprawczynią zamachu w Iraku w listopadzie 2009 r., czy Samantha Lewthwaite, analogicznie do Czeczenek nazywana „białą wdową". Jej mąż był jednym z islamistów, którzy w lipcu 2005 r. przeprowadzili samobójcze zamachy w londyńskim metrze[35].

Z jednej strony zatem kobiety są traktowane przez organizacje terrorystyczne instrumentalnie, jako narzędzie wspierane manipulacją i obietnicami osiągnięcia statusu „jednostek wybranych". Z drugiej jednak świadomie decydują się na wyrażanie sprzeciwu wobec negatywnie przez nie ocenianych zdarzeń właśnie poprzez przeprowadzanie zamachów na życie innych ludzi, nie tylko tych bezpośrednio odpowiedzialnych za ich krzywdy.

Abstrakt

Artykuł dotyczy zjawiska ważnego dla bezpieczeństwa państw, choć nie do końca zbadanego, tj. samobójczych zamachów terrorystycznych przeprowadzanych przez kobiety, w tym przypadku przede wszystkim przez czeczeńskie „czarne wdowy", i psychologii tych zamachów. Udział kobiet w zbrojnym dżihadzie niewątpliwie wymusił nowe spojrzenie zarówno na zjawisko terroryzmu, jak i na jego zwalczanie. Analizie poddano tu kilka hipotez, które w jakimś stopniu mogą pomóc zrozumieć psychospołeczne aspekty zamachów dokonywanych przez muzułmanki i motywację działania tych kobiet. Biorąc pod uwagę specyfikę rejonów ogarniętych konfliktami, należy zaznaczyć, że nie zawsze znajdują potwierdzenie tezy, iż muzułmanki decydują się na męczeńską śmierć w imię Allaha, niepodległości czy suwerenności kraju oraz zemsty za cierpienia, jakich doświadczyły osobiście lub jakich doświadczyli ich bliscy. Zawężając ocenę zamachów przeprowadzanych przez kobiety do aktów dokonywanych przez czeczeńskie „czarne wdowy", niniejszy artykuł próbuje odpowiedzieć na pytanie, czy każda z nich działa z podobnych pobudek, które po uogólnieniu można sprowadzić do: osobistej traumy powiązanej z motywem społecznym, dania wyrazu ideologii religijnej, chęci zemsty oraz przypadków zmuszania do dokonywania zamachów, poprzez stosowanie środków odurzających lub szantażu moralnego. Dotarcie do informacji o większości ataków przeprowadzonych przez Czeczenki pozwoliło także na określenie ogólnej taktyki zamachów.

Fenomen czeczeńskich „czarnych wdów" jest zagadnieniem niezwykle interesującym z punktu widzenia badania terroryzmu, ale też niezmiernie trudnym do jednoznacznej oceny. Czy te kobiety to po prostu spragnione zemsty morderczynie, czy też są to poddawane psychomanipulacji ofiary konfliktu czeczeńsko-rosyjskiego, skutecznie wykorzystywane przez bojowników kaukaskich. Analiza problemu wykazuje, że na decyzję czeczeńskich kobiet dotyczącą podjęcia samobójczej misji ma wpływ złożona interakcja czynników socjopolitycznych i psychologicznych – mieszanka traumy, desperacji, manipulacji i indoktrynacji religijnej.

[35] *Rekrutuje kobiety do przeprowadzania samobójczych zamachów, ma powiązania z głównym jądrem al-Kaidy* [online], http://www.globaljihad.net/view_page.asp?id=2190 oraz *Czy Biała Wdowa znów uderzy?* [online], http://rokor1.pl//index.php/czytelnia/rozmaitoci/1692-czy-biala-wdowa-znow-uderzy [dostęp: 12 XII 2012].

Abstract

The article concerns suicide terrorist attacks carried out by women, in particular by the Chechen "black widows", and the psychology of these attacks. This topic is extremely important from the point of view of security, but has not yet been exhausted. The participation of women in the armed jihad undoubtedly requires a new approach to both terrorism and the combat against it. A few hypotheses have been analyzed, which to some extent might help to understand the psychosocial aspects of the attacks carried out by Muslim women and the motivation for their actions. Taking into consideration the special nature of the regions engulfed by conflicts, it has to pointed out that Muslim women not always decide to die a martyr's death in the name of Allah, for the independence or sovereignty of the country, or in order to revenge the suffering experienced by them personally or by their family and friends. The article focuses on the analysis of attacks conducted by the Chechen "black widows". It aims at answering the question, whether each of them had the same motives. Generally speaking, the motives include: a personal trauma connected with the social motive, expression of the religious ideology, desire to take revenge and being forced to carry out an attack using narcotic drugs or moral blackmail. Additionally, it was only possible to define the general tactics of the attacks, as we managed to obtain the information about the majority of the attacks conducted by the Chechen women.

The phenomenon of the Chechen "black widows" is a very interesting issue from the point of view of studies on terrorism, but also a very difficult one when it comes to providing unequivocal assessment. Are these women simply murderers craving for revenge, or are they subject to psychological manipulation, victims of the Chechen-Russian conflict, effectively used by the Caucasian fighters. The analysis of the problem shows that the decision of the Chechen women to die a suicidal death is influenced by a very complex combination of sociopolitical and psychological factors – trauma, desperation, manipulation and religious indoctrination.

Luiza Wojnicz

Europejska Służba Działań Zewnętrznych jako innowacyjny element bezpieczeństwa Unii Europejskiej *sensu largo*

Unia Europejska (UE) od początku swojego powstania, tj. od 1993 r., realizuje dualistyczną koncepcję bezpieczeństwa polegającą na dbałości o wewnętrzne bezpieczeństwo, podkreślając jednocześnie, że wymiar zewnętrzny tego obszaru jest szczególnie newralgiczny, w dużym bowiem stopniu wpływa na wewnętrzną sytuację. Zastanawiając się nad tą koncepcją, a także motywami budowania bezpieczeństwa dwutorowo, na pierwszy plan wysuwają się problemy związane z terroryzmem „napływowym", powiązania i implikacje połączone z tym zjawiskiem, a także regionalne konflikty poza granicami UE. Dlatego też w celu zapewnienia wysokiego poziomu bezpieczeństwa wewnątrz Unii Europejskiej konieczne są działania w wymiarze zewnętrznym, gdyż to właśnie one są gwarantem względnej stabilności wewnątrz danego obszaru, w tym przypadku wszystkich państw członkowskich UE. W związku z tym Unia Europejska podejmuje wiele działań obejmujących tereny poza jej granicami, do których należy zaliczyć: utrzymywanie i rozwijanie poprawnych stosunków dyplomatycznych, współpracę z ważnymi uczestnikami stosunków międzynarodowych czy budowanie układów i partnerstwa strategicznego w kluczowych z punktu widzenia Unii regionach. W ten sposób Unia buduje wokół siebie obszar bezpieczeństwa, starając się zapewnić pokój i stabilność swoim obywatelom[1]. Proces instytucjonalizacji zewnętrznych aspektów bezpieczeństwa stał się bardziej widoczny dzięki powstałej na mocy decyzji Rady z 26 lipca 2010 r.[2] Europejskiej Służbie Działań Zewnętrznych – ESDZ (European External Action Sernice – EEAS).

Utworzenie ESDZ uznaje się za jedną z najistotniejszych zmian wprowadzonych Traktatem z Lizbony[3], który wszedł w życie 1 grudnia 2009 r. (w Polsce obowiązuje od 2 grudnia 2009 r., czyli od ogłoszenia w Dzienniku Ustaw[4]). Europejska Służba Działań Zewnętrznych ma zapewnić większą spójność i skuteczność działań zewnętrznych UE, a tym samym doprowadzić do zwiększenia znaczenia Unii Europejskiej na arenie światowej, zwłaszcza że traktat dodatkowo wyposażył UE w całkowitą swobodę działania na poziomie międzynarodowym[5]. Służba funkcjonuje niezależnie od pozostałych organów UE, jednak ma prawny obowiązek działać w sposób spójny z pozostałymi podmiotami istniejącymi w ramach ESDZ. Podstawą

[1] Przykładami tego typu działań są: Partnerstwo Eurośródziemnomorskie (Euro-Mediterranean Partnership), Europejska Polityka Sąsiedztwa (European Neighbourhood Policy), partnerstwo z Federacją Rosyjską, ze Stanami Zjednoczonymi czy rozwój relacji z Chinami i wiele innych.

[2] *Decyzja Rady z dnia 26 lipca 2010 r. określająca organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych* (*2010/427/UE*), – Dz.Urz UE L 201 z 3 sierpnia 2010 r., s. 30, [online], www.eeas.eu [dostęp: 5 X 2012].

[3] Traktat z Lizbony zmieniający Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską, podpisany w Lizbonie dnia 13 grudnia 2007 r. (Dz.Urz. UE C 306 z 17 grudnia 2007, s. 1).

[4] Dz.U. z 2009 r. Nr 203, poz. 1569.

[5] *Decyzja Rady z dnia 26 lipca 2010 r. ...* Zob. *Taking Europe to the Word. 50 years of the European Commission's External Service*, EC 2004 Luxembourg, European Commission 2004.

prawną decyzji Rady z 26 lipca 2010 r. w sprawie organizacji i funkcjonowania Służby jest art. 27 ust. 3 Traktatu o Unii Europejskiej z Maastricht (TUE)[6]: *W wykonywaniu swojego mandatu, wysoki przedstawiciel jest wspomagany przez Europejską Służbę Działań Zewnętrznych. Służba ta współpracuje ze służbami dyplomatycznymi Państw Członkowskich i składa się z urzędników właściwych służb Sekretariatu Generalnego Rady i Komisji, jak również z personelu delegowanego przez krajowe służby dyplomatyczne. Organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych określa decyzja Rady. Rada stanowi na wniosek wysokiego przedstawiciela po konsultacji z Parlamentem Europejskim i po uzyskaniu zgody Komisji*. Zakres działalności Służby powinien umożliwić Wysokiemu Przedstawicielowi Unii do Spraw Polityki Zagranicznej i Bezpieczeństwa (High Representative of the Union for Foreign Affairs and Security Policy – HR) pełne wykonywanie mandatu określonego w Traktacie. Aby zapewnić spójność i lepszą koordynację działań zewnętrznych Unii, Służba powinna również wspierać Przewodniczącego Rady Europejskiej oraz Przewodniczącego i członków Komisji Europejskiej w zakresie ich funkcjonowania w dziedzinie stosunków zewnętrznych, a także powinna ściśle współpracować z państwami członkowskimi[7]. Po tym jak Parlament Europejski przyjął decyzję o utworzeniu ESDZ, Wysoka Przedstawiciel Unii do Spraw Polityki Zagranicznej i Bezpieczeństwa Catherine Ashton powiedziała: *Teraz możemy rozpocząć budowę nowoczesnej, efektywnej i wyraźnie europejskiej służby XXI wieku. Powód jest prosty – Europa musi się rozwijać, aby lepiej bronić swoich interesów i wartości w świecie coraz bardziej złożonych i znaczących zmian*[8].

Celem artykułu jest udowodnienie, że powstały organ wraz z licznymi instrumentami działającymi w jego obszarze stanowi innowacyjny komponent bezpieczeństwa sensu largo w Unii Europejskiej. Zadania ESDZ są bardzo wszechstronne i niejednokrotnie wykraczające poza zapewnienie bezpieczeństwa. Artykuł dotyczy wyłącznie obszaru bezpieczeństwa. Ponieważ jest to stosunkowo nowa sui generis służba, autorka, pisząc artykuł, oparła się w głównej mierze na dokumentach źródłowych oraz źródłach internetowych.

Funkcje ESDZ i UE

Głównym zadaniem Europejskiej Służby Działań Zewnętrznych jest wspieranie Catherine Ashton w wypełnianiu jego zadań. W tym miejscu należy nadmienić, iż zadania Wysokiej Przedstawiciel są skoncentrowane wokół kluczowych zagadnień, do których należą m.in:

– koordynacja wspólnej polityki zagranicznej i bezpieczeństwa UE,
– dbałość o spójność działań zewnętrznych,
– prowadzenie dialogów politycznych,
– występowanie na forach międzynarodowych,
– kontrola ESDZ.

---

[6] *Traktat o Unii Europejskiej* – wersja skonsolidowana (Dz.Urz. UE C 83 z 30 marca 2010 r., s. 13).

[7] *Sprawozdanie prezydencji skierowane do Rady Europejskiej dotyczące Europejskiej Służby Działań Zewnętrznych*, Bruksela, 23 października 2009, Dok. 14930/09, s. 2.

[8] *Catherine Ashton High Representative of the Union for Foreign Affairs and security Policy, Vice-President of the European Commission Introductory remarks at presentation of the proposal for the European External Action Service* (EEAS), Brussels, 25 March 2010, Council of the European Union. Por. *Speech by High Representative Catherine Ashton to the European Parliament on the creation of the European External Action Service*, Strasbourg, 7 July 2010, European Union, Doc. A 127/10.

Wart podkreślenia jest fakt, że działania samej ESDZ wymykają się spoza obszaru klasycznej polityki zagranicznej i bezpieczeństwa, obejmując bezpieczeństwo i obronę, do którego należy zaliczyć: cywilne zarządzanie kryzysowe oraz misje i operacje pokojowe przyczyniające się do budowania stabilności w danym regionie, a tym samym są czynnikiem zewnętrznym bezpieczeństwa wewnętrznego UE[9]. To szerokie spektrum funkcji w obszarze bezpieczeństwa wynika z celów i zadań, jakie realizuje Unia Europejska na zewnątrz (*external goals*) i jaką rolę przypisuje sobie w stosunkach zewnętrznych. Na uwagę zasługuje kilka najistotniejszych spraw. Najważniejszym celem jest dbałość o pokój. Unia Europejska jako jeden z najważniejszych partnerów handlowych na świecie, a jednocześnie darczyńca, realizuje zadania polegające na udzielaniu wsparcia politycznego, gospodarczego i czysto praktycznego (administrowanie i zarządzanie strukturami państwowymi) tym krajom, które potrzebują tego typu pomocy i które zwrócą się o taką pomoc. Dlatego fundamentalnym obszarem działania ESDZ jest promowanie integracji, wspieranie pokoju i zapobieganie konfliktom. Unia Europejska dość często podkreśla, że newralgicznym celem jej stosunków zewnętrznych jest polityczne zaangażowanie w zapobieganie konfliktom zbrojnym. Czynnikami ułatwiającymi wczesną prewencję: są: identyfikacja zagrożeń, analiza ryzyka oraz szybkie działanie. Skuteczne zapobieganie zagrożeniom, zarówno na krótki, jak i dłuższy czas, musi być oparte na rzetelnej informacji i analizie konkretnych możliwości działania. Wymaga to od podmiotów UE szerszego współdziałania oraz spójności, która musi być zapewniona w zakresie wczesnego ostrzegania, analizy, planowania, podejmowania decyzji oraz wdrożenia i oceny. Unia posiada bogaty zestaw instrumentów strukturalnych dotyczących bezpośrednich długoterminowych i krótkoterminowych działań zapobiegawczych. Do długoterminowych można zaliczyć współpracę rozwojową, handlową, kontrolę broni, ochronę praw człowieka i ochronę środowiska, a także dialog polityczny. Do krótkoterminowych działań zaliczono instrumenty dyplomatyczne i humanitarne. Jednym z nich jest mediacja będąca składnikiem unijnej dyplomacji prewencyjnej, pomagającej w zapobieganiu konfliktom i budowaniu pokoju w krajach ogarniętych konfliktami[10]. Według definicji unijnej mediacja to sposób wspomagania negocjacji pomiędzy stronami konfliktu, transformowania konfliktu, przy wsparciu akceptowanym przez strony trzecie. Mediacja jest istotnym elementem zarządzania kryzysowego na wszystkich szczeblach, zarówno pomiędzy państwami, jak i w państwach będących w stanie konfliktu. Ogólnym celem mediacji jest umożliwienie stronom osiągnięcie porozumienia. Szczegółowe cele zależą jednak od charakteru konfliktu i oczekiwań stron oraz samego mediatora. Podstawowym zadaniem jest zapobieżenie lub zakończenie przemocy poprzez zaprzestanie działań wojennych lub podpisanie zawieszenia broni. Aby zapewnić pokój i stabilność na dłuższy czas, mediacja powinna być świadoma i skupiona na przyczynach konfliktu. Dlatego za podstawowe narzędzie mediacji UE uznaje się dialog jako proces otwarty, prowadzący do poszukiwania wspólnej płaszczyzny, budowania zaufania, pojednania i budowania procesu pokojowego. Według UE udany dialog może doprowadzić do

[9] Zob. *Brussels European Council-29/30 October 2009, Presidency Conclusions*, Brussels, 1 December 2009, nr 15265/1/09 REV 1, Council of the European Union. Por. Ch. Hillion, M. Lefebvre, *The European External Action Service: towards a common diplomacy?, "*European Issue" 2010, nr 184.

[10] *Draft European Union Programme for the Prevention of Violent Conflict*, Brussels, 7 June 2001, 9537/1/01, REV 1, Council of the European Union.

deeskalacji konfliktu[11]. Unia jest zaangażowana w następujące typy dialogu: promowanie mediacji, jako skutecznego czynnika budowania pokoju, ochrony praw człowieka i rządów prawa. Z uwagi na polityczne znaczenie i zasoby finansowe Unii może ona wykorzystać mediacje, dokonując ekonomicznego lub dyplomatycznego nacisku (np. w ramach grupy przyjaciół). Unia Europejska wspomaga mediację za pomocą szkoleń, wsparcia logistycznego i wymiany doświadczeń pomiędzy ekspertami. Wspomaganie to powinno być dobrze skoordynowane ze wszystkimi podmiotami zaangażowanymi, aby uniknąć powielania działań. Drugim z narzędzi mediacji jest pośrednictwo finansowe, czyli wsparcie formalne, nieformalne i oddolne procesów mediacyjnych[12]. Tak szeroka gama narzędzi mediacyjnych pozwala dynamiczne wpływać na rozwój sytuacji.

Wraz z powołaniem ESDZ utworzono Dywizję Zapobiegania Konfliktom, Budowania Pokoju i Mediacji (Conflict Prevention, Peacebuilding and Mediation Division – CPPMD) oraz Zespół Wsparcia Mediacji (Mediation Support Team)[13], co ma wzmocnić zdolności UE w zakresie rozwiązywania sporów.

W ramach szeroko pojętego zarządzania kryzysowego pomocna jest również współpraca z organizacjami regionalnymi, takimi jak Rada Europy czy Organizacja Bezpieczeństwa i Współpracy w Europie (OBWE), z którymi UE zintensyfikowała wymianę informacji oraz nawiązała kooperację w ramach zarządzania kryzysowego i zapobiegania konfliktom. W tym miejscu warto wspomnieć, że Unia Europejska odegrała kluczową rolę w procesie budowania pokoju na Bałkanach Zachodnich. Od Bośni i Hercegowiny aż po Czarnogórę dyplomacja unijna wykorzystywała swoje wpływy, aby promować pokój i pojednanie. Niedawnym przykładem takich działań może być usprawnianie przez Unię Europejską dialogu pomiędzy Serbią a Kosowem – tzw. dialogu na osi Belgrad – Prisztina[14].

Jak wynika z unijnej strategii bezpieczeństwa (European Security Strategy – A Secure Europe in a betterworld), zaktualizowanej w 2008 r., głównymi zagrożeniami i jednocześnie wyzwaniami dla Unii są: terroryzm, rozprzestrzenianie broni masowego rażenia, konflikty regionalne oraz działalność organizacji przestępczych. Wszystkie z wymienionych zjawisk mają wymiar globalny, co oznacza, że wpływają w mniejszym lub większym stopniu na sytuację wewnętrzną Unii. Dotyczy to zwłaszcza terroryzmu i jego następstw. Nie sposób jest zwalczać i zapobiegać tym zjawiskom, działając w pojedynkę, mimo że Unia Europejska to związek 27 państw. Wobec zagrożeń globalnych należy odpowiadać globalnie, czyli wychodząc poza granice zewnętrzne Unii Europejskiej. Jako przykład takiego działania mogą posłużyć wspólne deklaracje, które Unia podpisuje z zewnętrznymi partnerami. Ich celem jest współpraca w ramach konkretnego zagadnienia lub grupy zagadnień, np. wspólna deklaracja UE

[11] *Concept on strengthening EU Mediation and Dialogue Capacities*, Brussels, 10 November 2009, Doc.15779/09, Council of the European Union.

[12] Tamże, s. 6.

[13] *Thematic Evaluation of European Commission Support to Conflict Prevention and Peace-Building*, Ref. 1277, [online], www.ec.europa.eu. Por. *Annual Activity Report* 2011. The European External Action Service, www.eas.europa.eu [dostęp: 25 XI 2012].

[14] Zob. www.eeas.ue [dostęp: 16 X 2012]. Por. *European Defence Capabilities: lessons from the past, signpost for the future,* European Union Committee, 31st Report of Session 2010-12, London, 4 May 2012, House of Lord; *European Union Commitee, European Security and Defence Policy, Development of European Military Capabilities*, London 2009, [online], www.publications.parliament.uk [dostęp: 25 XI 2012].

i ASEAN o zwalczaniu terroryzmu z 2003 r.[15] czy współpraca z wieloma innymi organizacjami regionalnymi (Radą Europy, Unią Afrykańską, NATO), regionami czy też poszczególnymi państwami (USA, Rosją), która obejmuje aspekty walki z terroryzmem i innymi przestępstwami międzynarodowymi. Unia Europejska bierze czynny udział w rozwoju regionalnym w Europie Południowo-Wschodniej i jej synergii z krajami basenu Morza Czarnego (Black Sea Synergy). Poprzez zachęcanie do współpracy pomiędzy krajami otaczającymi Morze Czarne stwarza się możliwość rozwiązywania wspólnych problemów, skłaniając jednocześnie te państwa do przeprowadzania reform politycznych i gospodarczych. Działania takie stymulują przede wszystkim demokratyczne i gospodarcze reformy w danym rejonie, wspierają jego stabilność i promują jego rozwój. Wprowadzają także udogodnienia w realizacji praktycznych projektów w dziedzinach będących przedmiotem wspólnego zainteresowania, otwarcia nowych możliwości i wyzwań, poprzez skoordynowane działania w ramach regionalnych zadań, zachęcania do pokojowego rozwiązywania konfliktów w regionie. W obszarze bezpieczeństwa kluczowy jest też rozwój kooperacji na takich płaszczyznach, jak: migracja, egzekwowanie prawa oraz zwalczanie przestępczości zorganizowanej[16].

Dbałość o bezpieczeństwo i stabilność jako interesów strategicznych dla UE są zauważalne również w relacjach z Azją Centralną. Współpraca ta obejmuje szczególnie: troskę o pokój, przestrzeganie praw człowieka i zasad demokracji, a także zwiększanie bezpieczeństwa energetycznego poprzez dywersyfikację dostaw i tranzytu energii, konwergencję rynków energetycznych, przejrzystość w sektorze energetycznym. Dodatkowo kooperacja obejmuje wspieranie i wzmacnianie współpracy technologicznej pomiędzy Unią Europejską i państwami Azji Środkowej w sektorze energetycznym, wspieranie zrównoważonego rozwoju energetycznego, w tym rozwój efektywności energetycznej, odnawialnych źródeł energii oraz zarządzanie popytem, a także przyciąganie inwestycji na rzecz realizacji projektów energetycznych dla tego regionu. W tym miejscu należy wspomnieć, iż podobne cele realizowane są przez UE w ramach współpracy z państwami wschodnimi, tzw. Wschodnie Partnerstwo (Estern Partnership)[17]. Wspólne forum UE i państw Azji Centralnej w 2008 r. zaowocowało podjęciem istotnych zagadnień dla bezpieczeństwa, którymi były: wzmocnienie stabilności regionalnej dzięki odpowiedniemu zarządzaniu granicami oraz intensyfikacja wymiany informacji.

Za szczególne zagrożenie dla pokoju i stabilności międzynarodowej uznano rozprzestrzenianie broni masowego rażenia i środków jej przenoszenia, dlatego wskazano na konieczność ustanawiania skutecznych systemów kontroli eksportu broni konwencjonalnej, wzmocnienie kontroli granicznych i zabezpieczanie wrażliwych urządzeń i źródeł jądrowych, promieniotwórczych, biologicznych i chemicznych materiałów, w celu uniknięcia ryzyka proliferacji i nabywania ich przez grupy terrorystyczne.

[15] *Joint Declaration on Co-operation to Combat Terrorism, 14th EU-ASEAN Ministerial Meeting Brussels 27–28 January*, [online], Brussels, 27 January 2003, 5811/03, www.aseansec.org [dostęp: 6 XI 2012], także na: www.consilium.europa.eu.

[16] *Joint Statement of the Ministers of Foreign Affairs of the countries of the European Union and of the wider Black Sea area*, [online], Kyiv, 14 February 2008. www.eeas.europa.eu/blacsea. Por. *Report on the first year of implementation of the Black Sea Synergy,* Brussels, 19.6.2008, COM (2008) 391 final, Commission of the European Communities, www.eeas.europa.eu/blacsea/doc/com08.

[17] Należą do niego: Armenia, Azerbejdżan, Białoruś, Gruzja, Mołdawia i Ukraina, Zob. *Eastern Partnership Roadmap 2012–13 the multilateral dimensio*n, SWD (2012) 108 final.

Ponadto potwierdzono zwalczanie terroryzmu we wszelkich formach[18]. W przyczynianiu się do budowania bezpieczeństwa na świecie, kluczową rolę odgrywa Wspólna Polityka Zagraniczna i Bezpieczeństwa (Common Foreign and Security Policy – CFSP) oraz Wspólna Polityka Bezpieczeństwa i Obrony (Common Security and Defence Policy – CSDP). Za pośrednictwem mechanizmów CFSP i CSDP Unia prowadzi cywilne i wojskowe misje na całym świecie. Misje te są prowadzone w celu realizowania różnych zadań, począwszy od operacji pokojowych i zapobieganiu konfliktom, poprzez misje humanitarne, ratunkowe, stabilizacyjne, po wspólne doradztwo i pomoc. Jako przykład można podać operację Atlanta prowadzoną przez EUNAVFOR[19] na wodach wzdłuż wybrzeży Somalii. Celem tej misji jest rozwiązanie problemu piractwa i ochrona statków z pomocą humanitarną dostarczaną w ramach Światowego Programu Żywnościowego i przeznaczoną dla ludności na obszarach zniszczonych z powodu suszy[20]. Mandat misji został przedłużony do 2014 r., a biorące w niej udział siły będą mogły interweniować na Wybrzeżu Somalii oraz na jej wodach terytorialnych i wewnętrznych. Zdynamizowanie działań wynika z chęci lepszej współpracy z tymczasowym rządem federalnym Somalii. Dodatkowo Rada Unii Europejskiej podjęła decyzję o aktywowaniu centrum operacyjnego UE dla usprawnienia synchronizacji unijnych misji w Rogu Afryki[21]. Maritime Security Centre – Horn of Africa MSCHOA monitoruje 24 godziny na dobę statki przepływające przez Zatokę Adeńską[22]. Polska nie wysłała jednostek w rejon operacji, a jedynie oddelegowała dwóch oficerów Wojska Polskiego do dowództwa operacji w Northwood[23].

Kolejnym przykładem budowania przez UE pokoju na świecie są misje na Bliskim Wschodzie. Dzięki powołanym przez siebie operacjom, UE stała się trzecim oprócz USA i Rosji graczem w regionie bliskowschodnim, który jednak wystrzega się środków militarnych na rzecz misji wspomagających rozwój porządku regionalnego, a zarazem pozwalających władzom poszczególnych państw na usamodzielnienie się od pomocy z zewnątrz. W tym miejscu należy wymienić EUBAM Rafah – Misję UE do spraw Szkolenia i Kontroli na przejściu granicznym w Rafah. Zadaniem jest tu przede wszystkim pomoc władzom Autonomii Palestyńskiej w efektywnym zarządzaniu granicą i w wykonywaniu operacji zaopatrzeniowych, ocena wypełniania przez Autonomię Palestyńską zobowiązań ustalonych w porozumieniu z 2005 r. (Agreement on Movement and Acces), budowa zaufania pomiędzy stronami traktatu, a także przygotowanie Autonomii Palestyńskiej do samodzielnego zarządzania przejściem granicznym w Rafah w przyszłości[24].

---

[18] *Joint Declaration of the Participants in the EU-Central Asia Forum on Security Issues in Paris*, September 2008., w: *The European Union and Central Asia: The New Partnership in Action*, DGF Communication/Publications, Brussels 2009, s. 51–53.

[19] European Union Naval Force, pierwsza operacja morska UE przeciwko somalijskim piratom rozpoczęta w grudniu 2008 r.

[20] Por. R. Targoński, *Międzynarodowe działania przeciw piratom somalijskim*, „Biuletyn PISM" 2009, nr 8. Por. Ch. Piening, *Global Europe, The European Union In World Affairs*, Colorado–London 1997, Lynne Rienner.

[21] K. Mazurek, *Unia poszerza mandat operacji Atalanta* [online], www.uniaeuropejska.org, [dostęp: 3 XII 2012].

[22] Zob. www.mschoa.org, [dostęp: 3 XII 2012]. Por. Newsletter-Sea Piracy 2010, nr 9.

[23] Zob. www.mon.gov.pl [dostęp: 3 XII 2012].

[24] E. Brzdąkiewicz, *Misje UE na Bliskim Wschodzie* [online], www.psz.pl [dostęp: 6 XI 2012]. Por. *Council Joint Action 2007/359/CFSP on establishing a European Union Border Assistance Mission for the Rafah Crossing Point (EU BAM Rafah) of 23 May 2007,* OJ L 133 z 25 maja 2007, s. 51.

Kluczową w budowaniu wzajemnych relacji w obszarze pokoju i bezpieczeństwa jest także misja EUPOL COPPS, czyli misja policyjna, której celem jest reforma policji na Zachodnim Brzegu i w Strefie Gazy, a w szerszym znaczeniu wsparcie Palestyńczyków we wzięciu odpowiedzialności za prawo i porządek na zarządzanych przez nich obszarach[25]. Na uwagę zasługuje również jedna z największych cywilnych misji CSDP, tj. misja w Kosowie (The European Union Rule of Law Mission – EULEX Kosowo), której celem jest pomoc w tworzeniu praworządności. Do jej zadań należy współpraca z wymiarem sprawiedliwości, władzami lokalnymi oraz monitorowanie newralgicznych obszarów związanych z bezpieczeństwem, tj. terroryzmu, przestępczości zorganizowanej i korupcji, przestępstw finansowych, a także zbrodni wojennych[26]. W misji aktywnie działa Polski Kontyngent Policyjny, którego celem jest rozwijanie i wzmacnianie wieloetnicznych służb policyjnych oraz wspomaganie lokalnych organów odpowiedzialnych za zapewnienie przestrzegania prawa, bezpieczeństwa i porządku publicznego w Kosowie. Polski Kontyngent Policyjny składa się z Jednostki Specjalnej Polskiej Policji (JSPP) oraz ośmiu ekspertów policyjnych. Policjanci wchodzący w skład jednostki są dobierani z jednostek policji z całego kraju, po uzyskaniu pozytywnej oceny w postępowaniu rekrutacyjnym prowadzonym dwukrotnie w ciągu roku[27]. Mandat misji EULEX Kosowo wygaśnie 14 czerwca 2014 r.

Istotą omówionych misji, czyli misji o pokojowym charakterze, gdzie wartością dodatnią są działania dyplomatyczne, jest wzmocnienie wizerunku Unii jako gracza-partnera oraz korzyści w wymiarze bezpieczeństwa, wszystkie bowiem misje prowadzone przez Unię mogą przyczyniać się do walki z terroryzmem, np. przez wspieranie państw trzecich w zwalczaniu tego zjawiska na ich terytoriach. Nie sposób w tym miejscu przytoczyć wszystkich misji, jednak ich liczba wskazuje na wysoki stopień zaangażowania zewnętrznego UE, promowania pokoju, bezpieczeństwa i stabilizacji.

Nie bez znaczenia jest promowanie kolejnego działania, dzięki któremu Unia staje się bezpieczniejsza. Jest to budowanie dobrego i odpowiedzialnego sąsiedztwa. Za wschodnimi i południowymi granicami UE leży wiele państw, które w ostatnich latach przeszły gwałtowne przemiany polityczne. Arabska Wiosna to tylko jeden z ostatnich przykładów takich przemian. Właśnie z ich powodu Europejska Polityka Sąsiedztwa (European Neighbourhood Policy – ENP) zakłada utrzymywanie stabilnych i przyjaznych stosunków z państwami sąsiadującymi z Unią Europejską. Promowanie demokracji, praw człowieka, otwieranie rynków, współpraca wizowa czy współpraca w obszarze bezpieczeństwa i zwalczania terroryzmu to tylko nieliczne przykłady aktywności w tym obszarze[28].

Podobnie jest z pomocą oferowaną przez Unię krajom będącym w potrzebie. Warto tutaj zwrócić uwagę, że prawie połowa międzynarodowej pomocy humanitarnej pochodzi właśnie od Unii Europejskiej i jej państw członkowskich. Dzięki tej pomocy udaje się ratować życie osób mieszkających na takich obszarach, jak Róg Afryki, gdzie głód dotyka całej ludności. Ponadto Unia Europejska jest gotowa do reagowania w sko-

---

[25] Tamże. Por. *Council Joint Action 2005/797/CFSP of 14 November 2005 on the European Union Police Mission for the Palestinian Territori*es, OJ L 300 z 17 listopada 2005, s. 65.

[26] EULEX Kosovo, www.consilium.europa.eu [dostęp: 3 XII 2012].

[27] Służba w JSPP trwa sześć miesięcy, natomiast eksperci policyjni wykonują swoje obowiązki na terenie Kosowa przez rok, zob. www.info.policja.pl [dostęp: 3 XII 2012].

[28] Zob. L. Wojnicz, *Europejska Polityka Sąsiedztwa w kontekście walki UE z terroryzmem na przykładzie synergii z obszarem Basenu Morza Śródziemnego*, w: *Polityka Sąsiedztwa Unii Europejskiej. Pomostowość czy buforowość,* J. Jartyś, A. Staszczyk (red.), Szczecin 2008, Instytut Politologii i Europeistyki US.

ordynowany sposób w każdej międzynarodowej sytuacji kryzysowej – bez względu na to, czy chodzi o trzęsienie ziemi na Haiti, tsunami w Japonii czy powódź w Pakistanie. W takich sytuacjach są wykorzystywane wszystkie dostępne w Unii Europejskiej narzędzia reagowania[29].

Struktura zarządzania kryzysowego i wczesnego ostrzegania w ramach ESDZ

Jak wynika z powyższej analizy zarządzanie kryzysowe jest jednym z najważniejszych wyzwań, jakie Unia Europejska stawia przed sobą. Zadania ESDZ dotyczące zarządzania kryzysowego są skupione wokół wspierania Wysokiego Przedstawiciela Unii do Spraw Polityki Zagranicznej i Bezpieczeństwa w zapewnieniu spójności koordynacji działań zewnętrznych, istnieje jednak możliwość samodzielnego podejmowania działań przez ESDZ w imieniu Wysokiego Przedstawiciela. Służba koordynuje prace Platformy Zarządzania Kryzysowego (EEAS Crisis Platform – CP) oraz śledzi rozwój wydarzeń na świecie w celu szybkiego reagowania na ewentualne zagrożenia[30]. Platforma Zarządzania Kryzysowego jest instrumentem pozwalającym na skuteczną koordynację działań dotyczących zarządzania kryzysowego, zarówno cywilnego, jak i wojskowego, dlatego jest niezbędnym elementem w funkcjonowaniu ESDZ. Dzięki kompleksowemu ujęciu różnorodnych działań CP przyczynia się do skuteczności funkcjonowania ESDZ. Ponadto łączy różne struktury zarządzania kryzysowego, do których zalicza się:

- Dyrektoriat Zarządzania i Planowania Kryzysowego (Crisis Management and Planning Directorate – CMPD) – ustanowiony w 2010 r., odpowiedzialny za opracowywanie dokumentów i koncepcji zarządzania kryzysowego,
- Departament Reagowania Kryzysowego Crisis Response Departament – CRD) – odgrywający kluczową rolę przy udzielaniu pierwszej politycznej oceny na terenach zagrożonych kryzysem i zapewniający szybką i skoordynowaną reakcję. Ma obowiązek uważnie obserwować rozwój sytuacji politycznej i bezpieczeństwa w świecie, aby umożliwić ESDZ odpowiednią reakcję na potencjalne kryzysy,
- Sztab Wojskowy UE (EU Military Staff – EUMS) – działający wcześniej przy Radzie Unii Europejskiej. Jego zadaniem jest koordynacja działań wywiadowczych, ściśle współpracuje z Centrum Analizy Wywiadowczej,
- Planowanie Cywilne i Zdolność Dowodzenia (Civilian Planning and Conduct Capability – PCC) – odpowiedzialne za planowanie i przeprowadzanie cywilnych operacji w ramach CSDP,
- Centrum Analizy Wywiadowczej (EU Intelligence Analysis Centre – INTCEN[31]) – podobnie jak EUMS zajmuje się dostarczaniem analiz wywiadowczych oraz wczesnym ostrzeganiem. Do jego zadań należy monitorowanie i ocena wydarzeń międzynarodowych,

[29] Crisis Response, www.eeas.eu [dostęp: 24 XI 2012].

[30] Od 2 grudnia 2010 r. Agostino Miozzo pełni funkcję dyrektora zarządzającego ds. reagowania kryzysowego i koordynacji działań w ramach ESDZ., tamże [dostęp: 16 X 2012]. Por. C. Gourlay, *European Union Procedures and Resources for Crisis management,* „International Peacekeeping" 2004, nr 3.

[31] Wcześniej znane jako SITCEN (Centrum Sytuacyjne), od 2005 r. zaczęto używać nazwy EU INTCEN. W 2012 r. oficjalnie dokonano zmiany nazwy z SITCEN na EU INTCEN.

- Przestrzeń Sytuacyjna (EU Situation Room) – powstała w 2011 r., ma za zadanie reagowanie w sytuacjach kryzysowych i koordynację operacji,
- Oficer Regionalny (Regional Crisis Response Planning Officers – RCRPOS) – odpowiedzialny za gromadzenie i analizowanie informacji na temat regionalnych kryzysów,
- Grupa Zapobiegania Konfliktom (Conflict Prevention Group – CPG) – utworzona w 2011 r., jest nieformalną grupą łączącą różne podmioty zajmujące się zapobieganiem konfliktów. Celem Grupy jest wspieranie spójnego podejścia do kwestii związanych z wczesnym ostrzeganiem i reagowaniem.
- wspomniana już Dywizja Zapobiegania Konfliktom, Budowania Pokoju i Mediacji (CPPMD) – zapewnia wsparcie operacyjne krajowym zespołom,
- Wywiadowcza Rada Sterująca (Intelligence Steering Board – ISB) i Robocza Grupa Wywiadowcza (Intelligence Working Group – IWG) – jedne z najnowszych organów ESDZ. Stanowią nieformalną inicjatywę wpierającą działania wywiadowcze poza Unią Europejską[32].

Do systemu instytucjonalnego ESDZ należy także zaliczyć: Komitet Wojskowy (EU Military Committee – EUMC), Komitet Polityczny i Bezpieczeństwa (Political and Security Committee – PSC) oraz służby działające przy Komisji Europejskiej, jak np.: Pomoc Humanitarna i Ochrona Cywilów (Humanitarian Aid and Civil Protection – ECHO), Współpraca i Rozwój (Development and Coordination – DEVCO), Instrument Polityki Zagranicznej (Foreign Policy Instrument – FPI).

W 2011 r. Platforma Zarządzania Kryzysowego aktywowała swoją działalność podczas kryzysu na Wybrzeżu Kości Słoniowej, w Libii oraz w Rogu Afryki. Na przełomie listopada i grudnia 2011 r. przeprowadzono pierwsze ćwiczenia w ramach ESDZ dotyczące zarządzania kryzysowego CME 11 (Crisis Management Exercise)[33]. Platforma Zarządzania Kryzysowego jest czynnie wspierana przez unijną przestrzeń sytuacyjną, określaną dosłownie jako Pokój Sytuacyjny[34], która jest częścią wydziału reagowania kryzysowego ESDZ. Praca przestrzeni sytuacyjnej odbywa się 24 godziny na dobę, siedem dni w tygodniu i polega na prowadzeniu monitoringu wszystkich zakątków świata, śledzeniu najnowszych sytuacji, a także obsłudze unijnych delegatur i specjalnych reprezentantów (European Union Special Representative – EUSR) oraz misji i operacji CSDP. Jest również odpowiedzialna za wymianę informacji z państwami członkowskimi, instytucjami i agencjami UE oraz niektórymi organizacjami i państwami trzecimi[35].

Warto podkreślić ciągłe podejmowanie wysiłków przez UE na rzecz usprawniania mechanizmów zarządzania kryzysowego. Doświadczenia instytucji europejskich i państw członkowskich wskazują, że mechanizm reagowania na kryzysy odwołujący się do możliwości jednego sektora się nie sprawdza. Unia potrzebuje całościowego

---

[32] T. Beswitch, *EU Early Warning and Early Response Capacity for Conflict Prevention In the Post-Lisbon Area*, IFP-NEW 2012, s. 7–15. Por. D. Čvnčec, *A New Intelligence Paradigm and the European Union* [online], www.fvv.uni-mb.si [dostęp: 3 XII 2012].

[33] EEAS Crisis Platform, www.consilium.europa.eu [dostęp: 23 XI 2012]. Zob. *EU Crisis Response Capability Revisited*, *Europe Report, No 160, 17 I 2005* [online], www.crisisgroup.org [dostęp: 23 XI 2012], K. Rintakoski, M. Setala, A. Ricci, *From Needs to Solutions: Enhancing the Civilian Crisis Management Capacity of the European Union*, Helsinki 2006, CMI.

[34] Działa w ramach ESDZ od 18 lipca 2011 r.

[35] Do osi współpracy należą m.in. NATO, Unia Afrykańska, ASEAN, organizacje wyspecjalizowane systemu ONZ, Międzynarodowa Organizacja Czerwonego Krzyża itp., www.consilium.europa.eu [dostęp: 16 X 2012].

i wielosektorowego podejścia opartego na dogłębnej analizie i kompleksowej znajomości sytuacji. W tym miejscu należy wskazać, iż zadania polskiego Rządowego Centrum Bezpieczeństwa (RCB) są ściśle powiązane z głównymi działaniami Unii Europejskiej w tej dziedzinie. Do zadań RCB należy m.in.:

- zapewnienie wymiany informacji między UE i narodowymi centrami zarządzania kryzysowego w państwach członkowskich tej organizacji. Rządowe Centrum Bezpieczeństwa jest jednym z krajowych punktów kontaktowych zapewniających szybki obieg informacji w sytuacjach kryzysowych, w ramach procedur koordynacji na poziomie politycznym (*Arrangements for Crisis Coordination at EU political level* – CCA). Na poziomie Sekretariatu Generalnego Rady UE koordynatorem, a zarazem punktem kontaktowym i administratorem systemów CCA, jest INTCEN (Intelligence Analysis Centre), które podejmuje działania związane z uruchomieniem tego mechanizmu,
- współpraca z UE i państwami członkowskimi w zakresie ochrony europejskiej infrastruktury krytycznej oraz wymiany doświadczeń i najlepszych praktyk dotyczących ochrony krajowej infrastruktury krytycznej,
- analizowanie zagrożeń bronią chemiczną, biologiczną, radiologiczną i nuklearną (Chemical, Biological, Radiological, Nuclear – CBRN) oraz współpraca w ramach realizacji Planu Działania UE ds. CBRN,
- udział w ćwiczeniach,
- współpraca z właściwymi podmiotami na poziomie narodowym,
- udział w badaniach, projektach, pracach grup roboczych (zespołów eksperckich). Przykładem jest tu uczestniczenie w pracach Grupy Roboczej ds. Planowania Reagowania (Disaster Response Planning Working Group – DRPWG)[36],
- udział w konferencjach, seminariach, warsztatach.

Ponadto RCB monitoruje prace:

- Grupy Roboczej UE ds. Terroryzmu (Terrorism Working Party – TWP) prowadzonej w Polsce przez Agencję Bezpieczeństwa Wewnętrznego,
- grupy roboczej Rady UE ds. ochrony ludności (Civil Protection – PROCIV), w której wiodącą rolę odgrywa Komenda Główna Państwowej Straży Pożarnej (zwłaszcza w zakresie prac nad projektem decyzji Parlamentu Europejskiego i Rady w sprawie Unijnego Mechanizmu Ochrony Ludności),
- grupy ad hoc ds. instrumentów finansowych (Justice and Home Affairs – JHA*)*, której przewodzi Ministerstwo Spraw Wewnętrznych,
- Komitetu Ochrony Ludności (Civil Protection Committee – CPC), gdzie wiodącą rolę odgrywa Komenda Główna Państwowej Straży Pożarnej,
- Komitetu ds. Cywilnych Aspektów Zarządzania Kryzysowego (Committee for Civilian Aspects of Crisis Management – CIVCOM), pod przewodnictwem Stałego Przedstawicielstwa RP przy UE[37].

---

[36] Disaster Response Planning Working Group jest grupą roboczą powołaną w celu usprawnienia zdolności planowania operacji ochrony ludności w Unii Europejskiej. Jednocześnie grupa prowadzi prace nad wspólną metodologią rozwoju planów na wypadek katastrof i innych zagrożeń. Po uzgodnieniu ogólnego podejścia prace są kontynuowane w podgrupach tematycznych dotyczących: powodzi, pożarów lasów, zdarzeń sejsmicznych i awarii jądrowych. Przykładem prac eksperckich są spotkania specjalistów zajmujących się oceną ryzyka zatytuowane Export Meetings on Risk Assessment and Mapping for Disaster Management. Głównym ich celem jest wymiana doświadczeń oraz dobrych praktyk w zakresie analizy oceny ryzyka w poszczególnych państwach członkowskich, Zob. www.rcb.gov.pl [dostęp: 3 XII 2012].

[37] Tamże, por. CIVCOM, www.cy2012.eu [dostęp: 3 XII 2012].

ESDZ w praktyce

Działalność ESDZ oraz osiągane przez nią wyniki są zawarte w corocznych raportach. Jak wynika z raportu za 2011 r. uwaga Unii Europejskiej, a tym samym ESDZ, była skierowana na zagrożenia terrorystyczne oraz zapobieganie temu zjawisku w ramach ONZ oraz w stosunkach z państwami trzecimi i organizacjami międzynarodowymi. Za priorytetowe uznano: zapobieganie terroryzmowi, zwalczanie radykalizacji i rekrutacji oraz zwalczanie finansowania terroryzmu w UE i poza nią. Pod względem geograficznym szczególnie przyglądano się Pakistanowi i Afganistanowi, Azji Południowo-Wschodniej, Jemenowi, Somalii i Azji Środkowej, czyli obszarom wyjątkowo podatnym na działania terrorystyczne. Głównym mechanizmem finansowym wspierającym państwa trzecie w ich wysiłkach zmierzających do zapobiegania aktom terroryzmu pozostaje unijny Instrument na rzecz Stabilności (Instrument of Stability – IfS), ustanowiony 15 listopada 2006 r. jako uzupełnienie mechanizmu szybkiego reagowania (Rapid Reaction Mechanism – RRM) utworzonego w 2001 r.[38] Warto zwrócić uwagę na fakt, że dzięki koordynacji tych dwóch instrumentów zdecydowanie zintensyfikowano prace dotyczące zapobiegania konfliktom, zarządzania kryzysowego i budowania pokoju. Projekty z zakresu reagowania kryzysowego w ramach Instrumentu na rzecz Stabilności obejmują takie zagadnienia, jak wsparcie dla mediacji, budowanie zaufania, tymczasowe administrowanie, wzmocnienie praworządności, sprawiedliwości oraz rola zasobów naturalnych w konflikcie. W ramach IfS tego typu działania mogą być wspierane w sytuacjach kryzysu bądź też na początku kryzysu, gdy pomoc finansowa nie może być dostarczona z innych unijnych źródeł. Do tej pory z IfS sfinansowano wiele projektów dotyczących reagowania kryzysowego na całym świecie. Największa część funduszy została przyznana na projekty w Afryce, Azji i Pacyfiku i na Bałkanach, a następnie na Bliskim Wschodzie, w Ameryce Łacińskiej i na Karaibach. Na przykład podczas arabskiej wiosny oprócz bezpośredniego wsparcia dla pokojowych wyborów położono nacisk na wzmocnienie uczestnictwa społeczeństwa obywatelskiego w procesach transformacji (Tunezja, Egipt i Libia), ze szczególnym wsparciem roli kobiet. W zarządzanie kryzysowe w ramach IfS są zaangażowane m.in. społeczeństwa obywatelskie, administracja publiczna, państwa członkowskie UE, unijne instytucje, państwa trzecie. Kluczową rolę odgrywają jednak w tym procesie unijne delegacje, na nich to bowiem spoczywa wczesne ostrzeganie i opracowywanie koncepcji, strategii. Przykładowymi programami finansowanymi z IfS w 2011 r. są:

- walka z zorganizowaną przestępczością (przemyt kokainy) – koszt 6 mln euro,
- ochrona krytycznych szlaków morskich – koszt 4,5 mln euro,
- zapobieganie terroryzmowi – koszt 6,7 mln euro,
- cyberprzestępczość – koszt 4,5 mln euro.

Nie sposób wymienić wszystkich projektów, gdyż ich liczba jest imponująca, co tylko potwierdza determinację UE, jeśli chodzi o zapewnienie pokoju na świecie. Partnerskie budowanie pokoju w ramach IfS jest projektem innowacyjnym, łączy społe-

[38] W myśl art. 3. mechanizm szybkiego reagowania może zostać uruchomiony, gdy w zainteresowanych państwach beneficjentach wystąpią sytuacje kryzysowe lub grożące kryzysem, sytuacje stanowiące zagrożenie dla prawa i porządku publicznego, bezpieczeństwa jednostek, sytuacje grożące przeistoczeniem się w konflikt zbrojny lub destabilizacją danego państwa i w przypadku gdy sytuacje takie mogą być zagrożeniem dla dobroczynnych efektów polityki i programów pomocy i współpracy, ich efektywności i (lub) warunków ich właściwego wykonania. Zob. *Coucil Regulation (EC) No 381/2001 of 26 February 2001 creating a rapid-reaction mechanizm,* OJ L 57 z 27 lutego 2001, s. 5.

czeństwa obywatelskie z instytucjami UE oraz pozwala Unii na działanie, ułatwiając jej tym samym budowanie zdolności w zakresie zarządzania kryzysowego, co w szerszym ujęciu stanowi wartość dodatnią dla systemu bezpieczeństwa wewnętrznego Unii[39].

Unia Europejska aktywnie uczestniczyła w działaniach uruchomionego we wrześniu 2011 r. Globalnego Forum Antyterrorystycznego (Global Counterterrorism Forum – GCTF), skupiającego 29 państw oraz Unię Europejską. Forum ma na celu promowanie wielostronnej, cywilnej współpracy w zwalczaniu terroryzmu oraz budowanie potencjału w państwach zagrożonych terroryzmem. Ponieważ UE jest nadal jednym z najsilniejszych zwolenników Globalnej Strategii Zwalczania Terroryzmu ogłoszonej przez ONZ (UN Globar Strategy to Combat Terrorism – GCTS), podjęte wspólne wysiłki UE i ONZ w Azji Środkowej doprowadziły do wzmocnienia regionalnej współpracy w walce z terroryzmem. Przyjęto także plan działania dotyczący globalnego podejścia do terroryzmu w ramach ONZ[40]. Stanowi to zwrot w polityce antyterrorystycznej, gdyż dotychczas społeczność międzynarodowa walczyła ze zjawiskiem terroryzmu opierając się na sektorowych konwencjach ONZ, regionalnych porozumieniach oraz wewnętrznych regulacjach. Globalne podejście do zapobiegania i zwalczania terroryzmu stanowiłoby przełom oraz stworzyłoby podstawy do spójnego działania. Byłoby też sukcesem państw opowiadających się za takim podejściem.

Europejska Służba Działań Zewnętrznych jest instytucją skupiającą wszystkie instrumenty, jakimi dysponuje Unia Europejska w zakresie działań zewnętrznych, co wskazuje na tzw. efekt synergiczny. Należy zauważyć, że ESDZ poza wymienionymi instrumentami mediacji i zarządzania kryzysowego współpracuje ze służbami dyplomatycznymi państw członkowskich, w których skład wchodzą urzędnicy z odpowiednich departamentów Sekretariatu Generalnego Rady Unii Europejskiej i Komisji Europejskiej oraz pracownicy oddelegowani z krajowych służb dyplomatycznych państw członkowskich[41]. Kluczową rolę w ESDZ odgrywają właśnie delegacje UE, stąd często określa się ją mianem korpusu dyplomatycznego, także z racji posiadania swojego przedstawicielstwa w prawie każdym zakątku świata. Globalny zasięg działania ESDZ nie objawia się tylko poprzez zaistnienie UE w danym regionie, ale także poprzez liczne kontakty i ścisłą współpracę ESDZ z takimi uczestnikami, jak: organizacje międzynarodowe, centra zarządzania oraz państwa nienależące do UE. Służba bez wątpienia jest innowacyjnym komponentem bezpieczeństwa sensu largo w Unii Europejskiej. Przede wszystkim dlatego, że łączy w sobie trzy części składowe, tj. szeroko pojętą globalną politykę zagraniczną, bezpieczeństwo i obronę w ujęciu melioratywnym. Podział na trzy części wraz z narzędziami, jakimi dysponuje, powoduje zharmonizowane w całość działania. Ponadto ESDZ łączy w całość szeroką gamę narzędzi dyplomatycznych i zarazem praktycznych, jak np. prowadzenie dialogu wspartego pomocą techniczną i (lub) finansową. Za prekursorski mechanizm istniejący w ramach ESDZ należy uznać wspomnianą już Platformę Zarządzania Kryzysowego, dzięki której możliwa jest skuteczna koordynacja instrumentów zarządzania kryzysowego, zarówno cywilnego, jak i wojskowego, działająca 24 godziny na dobę. Za pomocą wspomnianych instrumentów ESDZ wpływa na poprawę

[39] Zob. *Regulation (EC) No 1717/2006 of the European Parliament and of the Council of 15 November 2006 establishing an Instrument for Stability*, OJ L 327 z 24 listopada 2006, s. 1. Por. *2012 Annual Action Programme for the Instrument for Stability – Crisis Preparedness Component (Peace-building Partnership)*, Brussels 20.3.2012, C(2012) 1791 final. *Annual Report on the Instrument for Stability* 2011, Brussels, Brussels 24.7.2012, COM(2012) 405 final.

[40] *Annual Activity Report*..., s. 29.

[41] www.eeas.eu [dostęp: 25 XI 2012].

sytuacji oraz zjawisk, które mogłyby zagrozić wewnętrznym procesom zachodzącym w UE, w tym naruszeniu jej bezpieczeństwa, bądź też wpływać na nie pejoratywnie.

Bibliografia

1. *Annual Action Programme for the Instrument for Stability – Crisis Preparedness Component (Peace-building Partnership)*, Brussels 20.3.2012, C(2012) 1791 final.
2. *Annual Activity Report* 2011, The European External Action Service. www.eeas.europa.eu.
3. *Annual Report on the Instrument for Stability* 2011, COM (2012) 405 final.
4. Beswitch T., *EU Early Warning and Early Response Capacity for Conflict Prevention In the Post-Lisbon Area*, IFP-EW 2012.
5. *Brussels European Council-29/30 October 2009, Presidency Conclusions*, Brussels, 1 December 2009, nr 15265/1/09 REV 1, Council of the European Union.
6. Brzdąkiewicz E., *Misje UE na Bliskim Wschodzie*, www.psz.pl.
7. *Catherine Ashton High Representative of the Union for Foreign Affairs and security Policy, Vice-President of the European Commission Introductory remarks at presentation of the proposal for the European External Action Service* (EEAS), Brussels, 25 March 2010, Council of the European Union.
8. *CIVCOM,* www.cy2012.eu.
9. *Concept on strengthening EU Mediation and Dialogue Capacities*, Brussels, 10 November 2009, Doc.15779/09, Council of the European Union.
10. Crisis Response, www.eeas.eu.
11. *Council Joint Action 2007/359/CFSP on establishing a European Union Border Assistance Mission for the Rafah Crossing Point (EU BAM Rafah) of 23 May 2007,* OJ L 133 z 25 maja 2007.
12. *Council Joint Action 2005/797/CFSP of 14 November 2005 on the European Union Police Mission for the Palestinian Territori*es, OJ L 300 z 17 listopada 2005, s. 65.
13. *Council Decision of 26 July 2010 establishing the organization and functioning of the European External Action Service (2010/427/UE),*OJ L 210 z 3 sierpnia 2010, s. 30.
14. *Coucil Regulation (EC) No 381/2001 of 26 February 2001 creating a rapid-reaction mechanizm*, OJ L 57 z 27 lutego 2001, s. 5.
15. Čvnčec D., *A New Intelligence Paradigm and the European Union*, www.fvv.uni-mb.si
16. *Decyzja Rady z dnia 26 lipca 2010 r. określająca organizację i zasady funkcjonowania Europejskiej Służby Działań Zewnętrznych* (*2010/427/UE*), Dz.Urz UE L 201 z 3 sierpnia 2010 r., s. 30.
17. *Draft European Union Programme for the Prevention of Violent Conflict*, Brussels, 7 June 2001, 9537/1/01, REV 1, Council of the European Union.
18. *Eastern Partnership Roadmap 2012-13 the multilateral dimensio*n, SWD (2012) 108 final.
19. EEAS Crisis Platform, www.consilium.europa.eu.
20. *EU Crisis Response Capability Revisited*, *Europe Report, No 160, 17 I 2005*, www.crisisgroup.org.
21. EULEX Kosovo, www.consilium.europa.eu.

22. *European Defence Capabilities: lessons from the past, signpost for the future,* European Union Committee, 31st Report of Session 2010–12, London, 4 May 2012, House of Lord.
23. *Evaluation of European Commission suport to Conflict Prevention and Peace-Building*, www.europa.eu.
24. Gourlay C., *European Union Procedures and Resources for Crisis management,* „International Peacekeeping" 2004, nr 3.
25. Hillion Ch, Lefebvre M., *The European External Action Service: towards a common diplomacy?,* „European Issue" 2010, nr 184.
26. *Joint Declaration of the Participants in the EU-Central Asia Forum on Security Issues in Paris*, September 2008., w: *The European Union and Central Asia: The New Partnership in Action*, DGF Communication/Publications, Brussels 2009, s. 51–53.
27. *Joint Declaration on Co-operation to Combat Terrorism, 14th EU-ASEAN Ministerial Meeting Brussels 27-28 January.*, Brussels, 27 January 2003, 5811/03, www.aseansec.org.
28. *Joint Statement of the Ministers of Foreign Affairs of the countries of the European Union and of the wider Black Sea area*, Kyiv, 14 II 2008, www.eeas.europa.eu/blacsea.
29. Mazurek K., *Unia poszerza mandat operacji Atalanta*, www.uniaeuropejska.org.
30. MSCHOA, www.mschoa.org.
31. Newsletter-Sea Piracy, 2010, nr 9.
32. Piening Ch, *Global Europe, The European Union In World Affairs*, Colorado-London 1997, Lynne Rienner.
33. *Polityka Sąsiedztwa Unii Europejskiej. Pomostowość czy buforowość,* Jartyś J., Staszczyk A. (red.), Szczecin 2008, Instytut Politologii i Europeistyki US.
34. *Regulation (EC) No 1717/2006 of the European Parliament and of the Council of 15 November 2006 establishing an Instrument for Stability*, OJ L 327 z 24 listopada 2006.
35. *Report on the first year of implementation of the Black Sea Synergy,* Brussels, 19.6.2008, COM (2008) 391 final, Commission of the European Communities.
36. Rintakoski K., Setala M., Ricci A., *From Needs to Solutions: Enhancing the Civilian Crisis Management Capacity of the European Union*, Helsinki, 2006, CMI.
37. *Speech by High Representative Catherine Ashton to the European Parliament on the creation of the European External Action Service*, Strasbourg, 7 July 2010, European Union Doc. A 127/10.
38. *Sprawozdanie prezydencji skierowane do Rady Europejskiej dotyczące Europejskiej Służby Działań Zewnętrznych*, Bruksela, 23 października 2009, Dok. 14930/09.
39. *Taking Europe to the Word. 50 years of the European Commission's External Service*, EC 2004 Luxembourg, European Commission 2004.
40. Targoński R., *Międzynarodowe działania przeciw piratom somalijskim*, „Biuletyn PISM" 2009, nr 8.
41. *The European Union and Central Asia: The New Partnership in Action*, DGF Communication/Publications, Brussels 2009.
42. www.mon.gov.pl.
43. www.info.policja.pl.
44. www.rcb.pl.

Abstrakt

Unia Europejska od początku swojego powstania realizuje dualistyczną koncepcję bezpieczeństwa polegającą na dbałości o wewnętrzne bezpieczeństwo, podkreślając jednocześnie, że wymiar zewnętrzny jest szczególnie newralgiczny, w dużym bowiem stopniu wpływa na sytuację wewnętrzną.

Od kilku lat nastąpił zauważalny wzrost instytucji, które odpowiadają za szeroko pojęte bezpieczeństwo. Proces instytucjonalizacji zewnętrznych aspektów bezpieczeństwa stał się bardziej widoczny szczególnie dzięki powstałej na mocy decyzji Rady z 26 lipca 2010 r. Europejskiej Służbie Działań Zewnętrznych (European External Action Sernice – EEAS), której cele i zadania są bardzo wszechstronne i w dużym stopniu dotyczą zagadnień bezpieczeństwa sensu largo.

Celem, jaki autorka postawiła sobie w niniejszej publikacji, jest próba udowodnienia, że powstały organ wraz z licznymi instrumentami, działającymi w jej obszarze, to innowacyjny komponent bezpieczeństwa sensu largo w Unii Europejskiej.

Abstract

Since its establishment, the European Union has been pushing forward the dualistic idea of security consisting in caring for its internal aspects, underlining, the particularly sensitive nature of its external dimension, as it affects the internal situation greatly.

Therefore, for several years there has been a noticeable increase in the number of institutions, which are responsible for a broad area of security. The institutionalization process of the external security has become more visible, especially since the European External Action Service (EEAS) was established based on decision of the Council of 26 July 2010. Its aims and responsibilities are comprehensive and concern mostly a broad area of security.

The goal that the author has set herself in this publication is an attempt to prove that the established body together with a number of instruments available, are innovative components of a broad area of security in the European Union.

Arkadiusz Dymowski

Agentes in rebus. Antyczny rodowód współczesnych służb specjalnych

Kiedy w 2002 r. likwidowano Urząd Ochrony Państwa (UOP), zamiast tej służby specjalnej powołano dwie inne: Agencję Bezpieczeństwa Wewnętrznego (ABW) i Agencję Wywiadu (AW)[1]. Co prawda oficjalnie nie podano, dlaczego twórcy tej reformy nazwali nowo utworzone instytucje agencjami, jednak, jak można się domyślać, wzorowano się na nazwach amerykańskich agencji wywiadowczych – przede wszystkim Agencji Bezpieczeństwa Narodowego (National Security Agency – NSA) oraz Centralnej Agencji Wywiadowczej (Central Intelligence Agency – CIA). Podobnie zresztą jak nazwa Centralne Biuro Śledcze (CBŚ), potocznie określanego jako „polskie FBI"[2], jest kalką językową z nazwy Federalnego Biura Śledczego (Federal Bureau of Investigation – FBI). Analogicznych inspiracji można się doszukiwać w nazwie utworzonego w 2006 r. Centralnego Biura Antykorupcyjnego (CBA)[3]. Owe zapożyczenia nomenklaturowe, jak można domniemywać, uboczny efekt fascynacji rozwiązaniami amerykańskimi w zakresie organizacji i funkcjonowania policji oraz służb specjalnych, nie do końca były zgodne z polską tradycją nazewniczą. W dotychczasowej polskiej praktyce termin „agencja" oznaczał raczej przedstawicielstwo lub wyspecjalizowaną organizację reprezentującą czyjeś interesy w określonym zakresie. Na przykład głównym zadaniem Agencji Nieruchomości Rolnych jest gospodarowanie państwowymi nieruchomościami rolnymi w imieniu i na rzecz Skarbu Państwa. Z kolei agencja celna załatwia na zlecenie importera lub eksportera formalności związane z międzynarodowym obrotem towarowym, agencja ubezpieczeniowa zaś reprezentuje towarzystwo ubezpieczeniowe, a niejednokrotnie również kilka towarzystw równocześnie, w kontaktach z klientami. Niemniej jednak twórcy Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, zapewne w sposób niezamierzony nawiązali do sięgającej kilkunastu stuleci tradycji „służb" cesarstwa rzymskiego.

---

[1] Artykuły 1, 2 i 221 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. z 2010 Nr 29, poz. 154). Zob. również K. Mordaszewski, *Proces kształtowania służb specjalnych w systemie prawnym Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1, s. 21–22; A. Barcikowski, *UOP i ABW w latach 2000–2005*, „Przegląd Bezpieczeństwa Wewnętrznego", Wydanie specjalne. 20-lecie UOP/ABW, 6 kwietnia 2010 r., s. 80–81; A. Misiuk, *Ewolucja cywilnych służb specjalnych w Polsce*, „Przegląd Bezpieczeństwa Wewnętrznego", Wydanie specjalne. 20-lecie UOP/ABW, 6 kwietnia 2010 r., s. 90–91.

[2] Zob. P. Pytlakowski, *Urodziny CBŚ. 10 lat polskiego FBI* [online], „Polityka", 8 kwietnia 2010 r., http://www.polityka.pl/kraj/opinie/1504946,1,10-lat-polskiego-fbi.read [dostęp: 13 V 2012].

[3] Ponadto wzorem amerykańskiego FBI jedno ze stanowisk służbowych w CBA nazwano „agentem specjalnym" (odpowiednik angielskiego *special agent*). Wcześniej w oficjalnej nomenklaturze polskiej nigdy nie stosowano nazwy „agent", a tym bardziej „agent specjalny" w stosunku do urzędników i funkcjonariuszy państwowych. Zob. *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U. z 2012 poz. 621) oraz *Rozporządzenie Prezesa Rady Ministrów z dnia 6 października 2010 r. w sprawie stanowisk służbowych w Centralnym Biurze Antykorupcyjnym oraz wymagań w zakresie wykształcenia i kwalifikacji zawodowych, jakie powinni spełniać funkcjonariusze na poszczególnych stanowiskach służbowych* (Dz.U. Nr 189, poz. 1265).

Źródłosłowu pokrewnych pojęć „agencja" i „agent", mających swoje podobnie brzmiące odpowiedniki prawie we wszystkich współczesnych językach europejskich, należy szukać w łacińskim czasowniku *agere*, tłumaczonym na język polski m.in. jako: działać, prowadzić, przedsiębrać[4]. Jedną z form imiesłowowych[5] tego czasownika jest słowo *agens* (w dopełniaczu liczby pojedynczej *agentis*, w mianowniku liczby mnogiej *agentes*), które można tłumaczyć jako: działający, prowadzący. Z typowego dla polszczyzny przekształcenia formy dopełniaczowej owego imiesłowu powstało polskie słowo „agent"[6]. Cały ten wywód etymologiczny ma na celu doprowadzenie do łacińskiego wyrażenia *agentes in rebus*, które można dosłownie przetłumaczyć jako eufemizm „działający w sprawach". W jakich sprawach? Otóż właśnie w sprawach na tyle ważnych i na tyle poufnych, że nie należy ich doprecyzowywać. Jako *agentes in rebus* byli bowiem określani funkcjonariusze tajnej służby państwowej późnego cesarstwa rzymskiego.

Agentes in rebus, niejednokrotnie określani po prostu jako *agentes*[7], pojawili się prawdopodobnie za rządów cesarza Dioklecjana (284–305)[8]. Pierwotnie była to służba o charakterze kurierskim powołana zamiast korpusu żołnierzy nazywanych *frumentarii,* którzy wcześniej występowali w podobnej roli[9]. Owe przekształcenia instytucjonalne należy rozpatrywać w kontekście przemian w strukturach zarządzania państwem wprowadzanych przez wspomnianego cesarza-reformatora. Dzięki nim podczas swoich ponad dwudziestoletnich rządów Dioklecjan zdołał wyprowadzić cesarstwo z głębokiego kryzysu polityczno-ekonomicznego, w jakim znajdowało się ono w III wieku. Formalnie *agentes* podlegali szefowi administracji cesarskiej (*magister officiorum*)[10], wchodzili w skład gwardii pałacowej (*scholae palatinae*) i używali pięciu rang kawaleryjskich: *equites*, *circitores*, *biarchi*, *centenarii* i *ducenarii*[11]. Mimo to *agentes in rebus* należy rozpatrywać jako służbę cywilną, urzędniczą, w przeciwieństwie do *frumentarii*, którzy wywodzili się z armii i do końca istnienia funkcjonowali w struktu-

---

[4] *Słownik łacińsko-polski,* K. Kumaniecki (opr.), Warszawa 1990, PWN, s. 25–26; L. Winniczuk (red.), *Mały słownik polsko-łaciński*, Warszawa 1994, Wydawnictwo Naukowe PWN, s. 126.

[5] *Participium praesentis activi*, tj. imiesłów czynny czasu teraźniejszego.

[6] W. Doroszewski, *O kulturę słowa. Poradnik językowy*, t. II, Warszawa 1962, PIW, s. 308.

[7] W. Blum, *Curiosi und Regendarii. Untersuchungen zur Geheimen Staatspolizei der Spätantike*, München 1969, Uni-Druck, s. 4.

[8] Niewykluczone, że powstanie korpusu *agentes in rebus* należy datować na okres nieco późniejszy, tj. rządy Konstantyna I (306–337), za którego panowania pojawiają się oni w źródłach pisanych (w tym w konstytucjach cesarskich regulujących zadania i uprawnienia *agentes* pod kątem prawnym); pierwsze wzmianki na ten temat. F. Dvornik, *Origins of intelligence services. The ancient Near East, Persia, Greece, Rome. Byzantium, the Arab Muslim Empires, the Mongol Empire, China, Muscovy*, New Brunswick 1974, Rutgers University Press, s. 129; A. Pikulska-Robaszkiewicz, *Funkcjonariusze służb specjalnych w późnym Cesarstwie – agentes in rebus*, „Prawo Kanoniczne" 1994, nr 3/4, s. 148–149;

[9] Tamże, s. 147; N.J.E. Austin , N.B. Rankov, *Exploratio. Military and Political Intelligence in the Roman World from the Second Punic War to the Battle of Adrianople,* London 1998, Routledge, s. 219; T. Crowdy, *Historia szpiegostwa i agentury*, Warszawa 2006, Bellona, s. 47.

[10] Bezpośredni wpływ na funkcjonowanie korpusu *agentes in rebus* w niektórych aspektach rezerwowali sobie sami cesarze. Na przykład w 399 r. cesarze Arkadiusz i Honoriusz zastrzegli dla siebie ostateczne decyzje odnośnie zatrudniania konkretnych osób jako *agentes*. A. Pikulska-Robaszkiewicz, *Funkcjonariusze*..., s. 154.

[11] Tamże, s. 148–149; C. Kelly, *Ruling the Later Roman Empire,* Cambridge, MA 2004, Harvard University Press, s. 20.

rach wojskowych[12]. Początkowo w liczbie kilkuset[13], w drugiej połowie V wieku korpus *agentes in rebus* liczył ponad 1200 osób w samej tylko części wschodniej podzielonego już wówczas imperium[14]. Służba ta przetrwała w cesarstwie bizantyjskim, będącym, jak wiadomo, kontynuacją wschodniej części cesarstwa rzymskiego, wciąż ewoluując pod względem organizacyjnym i kompetencyjnym, do początków VIII wieku pod greckimi nazwami *aggeliaforoi* (αγγελιαφοροι) lub *magistrianoi* (μαγιστριανοι)[15]. Mamy więc do czynienia z późnoantyczną[16] instytucją, która funkcjonowała nieprzerwanie przez około 400 lat.

Agentes in rebus przede wszystkim przewozili urzędową korespondencję, w tym rozkazy wojskowe, oraz sprawowali kontrolę nad pocztą publiczną (*cursus publicus*)[17]. Ponadto w pewnym okresie nadzorowali również statki przewożące ładunki państwowe[18]. Innym aspektem ich aktywności była funkcja dość tajemniczo i eufemistycznie określana jako *cura agendarum*, czyli: nadzór nad sprawami[19]. Funkcja ta związana była z informowaniem cesarza i jego najbliższych współpracowników przede wszystkim o działalności urzędników cywilnych i wojskowych oraz osób prywatnych mogącej stanowić zagrożenie dla władzy cesarskiej. *Agentes* sprawowali swego rodzaju sekretny nadzór nad prawidłowym funkcjonowaniem administracji prowincjonalnej[20]. W ramach swoich kompetencji mieli również zadania ujawniania przypadków przestępstw obrazy majestatu cesarskiego (*crimen laesae maiestatis*)[21], co w świetle konstytucji cesarskich obejmowało zamachy czy spiski, czyli przygotowania do zamachów na życie władcy, członków jego rodziny i najwyższych urzędników państwowych[22]. Ponadto jako jedno z zadań *agentes* wymienia

---

[12] *Agens in rebus*, w: *Late Antiquity: A Guide to the Postclassical World*, G.W. Bowersock, P. Brown, O. Grabar (red.), Cambridge, MA 1999, Harvard University Press, s. 278; T. Crowdy, *Historia* ..., s. 47; C.J. Fuhrmann, *Policing the Roman Empire. Soldiers, administration and public order*, Oxford–New York 2011, Oxford University Press, s. 244.

[13] N.J.E. Austin , N.B. Rankov, *Exploratio* ..., s. 219.

[14] C. Kelly, *Ruling*..., s. 207.

[15] *Agentes in rebus*, w: *The Oxford Dictionary of Byzantium*, A. Kahzdan (red.), t. 1, Oxford 1991, Oxford University Press, s. 37.

[16] Obecnie w naukach historycznych coraz wyraźniej zaznacza się tendencja do wyróżnienia swego rodzaju okresu przejściowego między tradycyjnie pojmowanymi starożytnością a średniowieczem, nazywanego właśnie późnym antykiem. Nie wchodząc w szczegóły, początek epoki późnego antyku wyznacza się zazwyczaj na panowanie cesarza Dioklecjana (przełom III i IV wieku), a koniec – w zależności od zakresu terytorialnego i przedmiotu badań – od VII wieku do przełomu VIII i IX wieku. Późniejsze daty odnoszą się zazwyczaj do terenów bizantyjskich, gdzie tradycja antyczna przetrwała zdecydowanie dłużej niż na zachodzie Europy. Zob. E. Wipszycka, *Przedmowa*, w: *Vademecum historyka starożytnej Grecji i Rzymu*. T. III. *Źródłoznawstwo czasów późnego Antyku*, tejże (red.), Warszawa 1999, Wydawnictwo Naukowe PWN, s. 6.

[17] A. Kolb, *Transport und Nachrichtentransfer im Römischen Reich*, „Klio". Beiträge zur alter Geschichte, Bd. 2, Berlin 2000, Akademie, s. 282–284; A. Świętoń, *Rola agentes in rebus w wykrywaniu i zwalczaniu spisków przeciwko władzy cesarskiej w okresie rządów Konstancjusza II (337-361 r. n.e.),* w: *Ochrona bezpieczeństwa i porządku publicznego w prawie rzymskim*, K. Amielańczyk, A. Dębiński, D. Słapka (red.), Lublin 2010, Wydawnictwo UMCS, s. 263–264 i 273. Tam wskazano dalszą literaturę i źródła pisane.

[18] A. Pikulska-Robaszkiewicz, *Funkcjonariusze*..., s. 150; A. Świętoń, *Rola*..., s. 263–264.

[19] Tamże, s. 264; por. również A. Pikulska-Robaszkiewicz, *Funkcjonariusze*..., s. 151.

[20] W. Blum, *Curiosi*…, s. 70; A. Świętoń, *Rola*..., s. 264.

[21] A. Świętoń, *Rola*..., s. 264.

[22] Por. M. Dyjakowska, *Ochrona bezpieczeństwa i porządku publicznego a rzymskie ustawy o obrazie majestatu,* w: *Ochrona bezpieczeństwa i porządku*..., s. 69–78.

się również chwytanie szpiegów[23]. Jeśli przyjmiemy taką interpretację źródeł za właściwą, to korpus *agentes in rebus* można uznać za swego rodzaju służbę „kontrwywiadowczą"[24]. Wypełniający swoje obowiązki *agentes in rebus* byli uprawnieni do dokonywania aresztowań i przeprowadzania przesłuchań[25]. W niektórych wypadkach, niejednokrotnie z polecenia samego cesarza, zlecano im również realizowanie „misji specjalnych", jak wykonywanie wyroków śmierci na wysoko postawionych osobistościach[26].

Jeśli we współczesnej Polsce można wskazać instytucję, której kompetencje obejmują coś, co w dzisiejszych realiach można nazwać *cura agendarum*, to niewątpliwie będzie to Agencja Bezpieczeństwa Wewnętrznego. Po pierwsze z tego powodu, że funkcja ta odnosiła się najwyraźniej do sfery, którą według dzisiejszej terminologii należałoby nazwać bezpieczeństwem wewnętrznym państwa[27]. Po drugie funkcję tę można przyrównać, nie zapominając jednak o zasadniczych różnicach wynikających z odrębnych kontekstów historycznych, do kompetencji Agencji Bezpieczeństwa Wewnętrznego[28] odnoszących się do rozpoznawania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, szczególnie w zakresie uzyskiwania i przekazywania właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego. Po trzecie funkcja *cura agendarum* obejmowała najprawdopodobniej również działania, które we współczesnych realiach nazywamy kontrwywiadowczymi, realizowane obecnie w głównej mierze przez ABW[29]. Po czwarte *agentes in rebus* ścigali w późnym cesarstwie rzymskim i we wczesnym cesarstwie bizantyjskim sprawców najcięższych przestępstw skierowanych przeciwko państwu, silnie identyfikowanym z cesarzem i jego najbliższym otoczeniem, co aktualnie również leży w kompetencjach ABW.

---

[23] F. Dvornik, *Origins* ..., s. 131; E.S. Danilov, *Kontrrazwiedywatel'nyje funkcyi agentes in rebus*, w: *Aktual'nyje probliemy istoriczieskoj nauki: Miežđunarodnyj sbornik naucznyh trudow mołodych uczionych*,. O. W. Jagow (red.), t. 6 (Е.С. Данилов, *Контрразведывательные функции agentes in rebus*, в: О. В. Ягов (ред.), *Актуальные проблемы истической науки: международный сборник научных трудов молодых ученых*. Вып. 6, Jarosławl' (Ярославль) 2009, s. 11–12.

[24] E.S. Danilov, *Kontrrazwiedywatel'nyje*..., s. 11–14.

[25] A. Pikulska-Robaszkiewicz, *Funkcjonariusze*..., s. 152–153. Owe funkcje „policyjne" *agentes in rebus* były zapewne główną przyczyną złej opinii, jaką cieszyli się wśród ogółu obywateli. Zarzucano im łapówkarstwo i liczne nadużycia m.in. w związku z aresztowaniami na podstawie fałszywych oskarżeń lub spreparowanych dowodów. Tamże, s. 152–154; A. Świętoń, *Rola*..., s. 264 i 273.

[26] A. Pikulska-Robaszkiewicz, *Funkcjonariusze*..., s. 151. Na przykład w 354 r. *agens* o imieniu Apodemiusz uczestniczył w egzekucji oskarżonego o zdradę i nadużycia Konstancjusza Gallusa, kuzyna współwładcy cesarza Konstancjusza II (337–361); zob. A. Świętoń, *Rola*..., s. 265–266.

[27] W taki właśnie sposób zadania *agentes in rebus* opisuje Francis Dvornik; zob. F. Dvornik, *Origins*..., s. 129–132. Por. również S. Sulowski, *W poszukiwaniu definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1(1), s. 10–13; K.A. Wojtaszczyk, *Istota i dylematy bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1(1), s. 14–15; P. Majer, *W poszukiwaniu uniwersalnej definicji bezpieczeństwa wewnętrznego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 7(4), s. 11–18.

[28] Artykuł 5 ustawy o Agencji Bezpieczeństwa Wewnętrznego. Zob. również Ł. Skoneczny, *Rola Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa Rzeczypospolitej Polskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2009, nr 1, s. 24 i in.

[29] Obecnie w Polsce funkcję kontrwywiadowczą realizuje również Służba Kontrwywiadu Wojskowego (SKW), w odniesieniu do sfery militarnej. Kompetencje te wynikają z artykułu 5 *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz.U. Nr 104, poz. 709 z późn. zm.).

Podobieństw między *agentes in rebus* a Agencją Bezpieczeństwa Wewnętrznego można się doszukiwać również w aspektach innych niż zakres wykonywanych zadań czy kompetencje wynikające z opisanych w przepisach prawnych[30] rozwiązań instytucjonalnych. Sekretny sposób działania *agentes* w dość oczywisty sposób przywodzi na myśl niejawne czynności operacyjno-rozpoznawcze prowadzone przez funkcjonariuszy współczesnych służb specjalnych, w tym ABW[31]. Wskazując na dalsze analogie, *agentes in rebus*, jak wspomniano, niezmiennie funkcjonowali w ramach struktury administracji cywilnej (tj. niewojskowej), używając jednocześnie „stopni wojskowych". Zadania *agentes* również dotyczyły raczej sfery cywilnej niż wojskowej. W tym sensie korpus *agentes in rebus* można uznać za pierwszą „cywilną służbę specjalną" w historii państw europejskich.

Gwoli ścisłości trzeba w tym miejscu zaznaczyć, że niektórzy badacze uznają określanie *agentes in rebus* tajną służbą, policją polityczną lub agencją szpiegowską[32] za nadinterpretację źródeł wynikającą z przenoszenia współczesnych doświadczeń na grunt starożytny[33]. Z pewnością można znaleźć wiele mocnych argumentów na poparcie tego stanowiska, jednak podobne zarzuty można wysuwać także w stosunku do innych porównań współczesnych instytucji do ich antycznych odpowiedników. Na przykład trudno stawiać znak równości między rzymskimi *vigiles* a obecną strażą pożarną, jednak z racji wykonywanych funkcji można uznać te służby za wypełniające analogiczne zadania publiczne w określonych, specyficznych warunkach historycznych. Z całą jednak pewnością za zbyt daleko idące należy uznać próby wtłoczenia zadań „służb" państw antycznych i sposobu wykonywania tych zadań w ramy czynności operacyjno-rozpoznawczych i dochodzeniowo-śledczych[34] opisanych współczesnymi przepisami prawnymi, także polskimi.

Wracając do *agentes in rebus* i Agencji Bezpieczeństwa Wewnętrznego, wywodzenie współczesnych polskich instytucji odpowiedzialnych za bezpieczeństwo państwa z antycznej tradycji rzymskiej nie jest wcale przedsięwzięciem tak karkołomnym, jak mogłoby się na pierwszy rzut oka wydawać. Samo pojęcie i idea Rzeczypospolitej, *Rei Publicae*, są przecież zapożyczone ze starożytnego Rzymu. Ochrona interesów państwa, w rozumieniu zaskakująco podobnym do współczesnego, również była Rzymianom nieobca[35]. Ponadto, a może przede wszystkim, skoro obecnie obowiązująca konstytucja w preambule[36] odwołuje się do *najlepszych tradycji Pierwszej i Drugiej Rzeczypospolitej,* to należy mieć świadomość, że Pierwsza Rzeczpospolita była oparta w dużej mierze na wzorach rzymskich. Jak to zwięźle ujął Jerzy Axer, *w dawnej Rzeczypospolitej*

---

[30] Dla *agentes in rebus*, biorąc pod uwagę zachowane do czasów współczesnych źródła, będzie to przede wszystkim Kodeks Teodozjański (*Codex Theodosianus*), a konkretnie zamieszczone w księdze 6 konstytucje *De agentibus in rebus* oraz *De principibus agentum in rebus.*

[31] Artykuły 21 i następne ustawy o Agencji Bezpieczeństwa Wewnętrznego. Zob. również Ł. Skoneczny, *Rola* ..., s. 29.

[32] Wszystkich tych określeń w stosunku do *agentes in rebus* użył m.in. William B. Sinnigen, zob. W.B. Sinnigen, *Two Branches of the Late Roman Secret Service*, „The American Journal of Philology" 1959, nr 3, s. 238.

[33] A. Świętoń, *Rola*..., s. 264; tam dalsza literatura.

[34] Por. A. Pikulska-Robaszkiewicz, *Funkcjonariusze*..., s. 152.

[35] Zob. np. referaty opublikowane w: *Salus rei publicae suprema lex. Ochrona interesów państwa w prawie karnym starożytnej Grecji i Rzymu*, A. Dębiński, H. Kowalski, M. Kuryłowicz (red.), Lublin 2007, Wydawnictwo KUL.

[36] Preambuła *Konstytucji Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. Nr 78 poz. 483, z późn. zm.).

– jeśli myślimy o zachowaniu narodu politycznego, czyli narodu szlacheckiego – niepodzielnie rządziła łacińska kultura i rzymska semiotyka zachowań, łacińskie słowo i rzymska poza[37]. Rzeczpospolita Obojga Narodów była postrzegana przez szlachtę jako bezpośrednia kontynuacja republiki rzymskiej[38], a łacina została podniesiona do rangi swego rodzaju języka narodowego panującego stanu[39]. Z punktu widzenia współczesnego historyka republika rzymska pod koniec I wieku przed Chrystusem została zastąpiona przez cesarstwo[40], jednak państwo to przez jego władze i obywateli w ciągu następnych kilku stuleci wciąż było nazywane *Res Publica*. Świadczą o tym chociażby emitowane w IV i V wieku po Chrystusie, nota bene stosunkowo często znajdowane na ziemiach polskich[41], monety rzymskie opatrzone legendą Securitas Rei Publicae[42], co oznacza: Bezpieczeństwo Rzeczypospolitej. Nie trzeba chyba nikogo przekonywać, że hasło to po kilkunastu stuleciach nie utraciło nic ze swojej aktualności i mogłoby z powodzeniem służyć za dewizę zarówno *agentes in rebus*, jak i polskich służb specjalnych, w tym także ABW. Oczywiście stwierdzenia tego nie można pozostawić bez komentarza odnośnie uwarunkowań historycznych. Trudno wprost porównywać XXI-wieczną demokrację europejską do reżimu późnoantycznej monarchii, a sposób i zakres działania *agentes in rebus* z pewnością byłyby nie do przyjęcia we współczesnych służbach demokratycznego i praworządnego państwa. Niemniej jednak w realiach schyłku antyku, kiedy alternatywą dla silnej władzy cesarskiej były dokuczliwe najazdy barbarzyńców lub chaos wywołany częstymi wówczas wojnami domowymi, hasło *Securitas Rei Publicae* było z całą pewnością równie dobrze odbierane przez ogół obywateli rzymskich, jak dewiza „Bezpieczeństwo Rzeczypospolitej" przez współczesnych obywateli polskich.

---

[37] J. Axer, *Orka na ugorze. Filhellenizm wobec tradycyjnie łacińskiej orientacji kultury polskiej,* w: *Filhellenizm w Polsce. Rekonesans*, M. Borowska, M. Kalinowska, J. Ławski, K. Tomaszuk (red. nauk.), Warszawa 2007, Wydawnictwo UW, s. 40.

[38] Tenże, *„Latinitas" jako składnik polskiej tożsamości kulturowej,* w: *Tradycje antyczne w kulturze polskiej – perspektywa polska,* tenże (red.), Ośrodek Badań nad Tradycją Antyczną w Polsce i w Europie Środkowo-Wschodniej UW. Eseje i Studia, t. I, Warszawa 1995, s. 74.

[39] Por. tamże, s. 76–81.

[40] Obiektywnie rzecz biorąc, ten sam punkt widzenia podzielał zapewne przeciętny polski szlachcic z XVI–XVIII wieku, który utożsamiał się przede wszystkim ze spuścizną Rzymu republikańskiego, a nie późnoantycznego cesarstwa. Wynikało to z m.in. faktu, że studiowanie tekstów łacińskich z okresu republiki, w pewnym zakresie również z wczesnego, ale już nie z późnego cesarstwa, było podstawowym elementem wykształcenia ogólnohumanistycznego w Polsce w XVI wieku, co utrzymała XVII- i XVIII-wieczna szkoła jezuicka. Por. tamże. s 109; W. Sawrycki, *Kultura antyczna w szkolnej edukacji romantyków,* w: *Filhellenizm w Polsce*..., s. 182.

[41] Zob. np. A. Bursche, *Later Roman-Barbarian Contacts in Central Europe. Numismatic Evidence*, seria: Studien zu Fundmünzen der Antike 11, Berlin 1996, Gebr. Mann, s. 147–220; J. Bodzek, *Remarks on the Inflow of Roman Coins into Southern Poland in the Second Half of the 4th and in the 5th Centuries A.D.*, w: M. Wołoszyn (red.), *Byzantine Coins in Central Europe between the 5th and 10th century*, seria: Moravia Magna, Seria Polona, t. III., Kraków 2009, PAU, s. 186 i 191.

[42] P.V. Hill, J.P.C. Kent, R.A.G. Carson, *Late Roman Bronze Coinage,* t. I–II, London 1976, Spink & Son (reprint), w różnych miejscach.

Abstrakt

W artykuł opisano z zarysie tajną służbę późnego cesarstwa rzymskiego i wczesnego cesarstwa bizantyjskiego (koniec III–początek VIII wieku) jako prekursorkę współczesnej polskiej służby specjalnej – Agencji Bezpieczeństwa Wewnętrznego. Funkcjonariusze owej późnoantycznej służby byli nazywani *agentes in rebus*, tj. „działający w sprawach".

Jednym z obszarów aktywności *agentes in rebus* było informowanie cesarza i jego najbliższych współpracowników m.in. o działalności urzędników cywilnych i wojskowych oraz osób prywatnych mogącej stanowić zagrożenie dla władzy cesarskiej. Jeśli można wskazać we współczesnej Polsce instytucję, której kompetencje obejmują coś, co w dzisiejszych realiach można nazwać *cura agendarum*, niewątpliwie będzie to Agencja Bezpieczeństwa Wewnętrznego. Po pierwsze z tego powodu, że funkcja *cura agendarum* odnosiła się najwyraźniej do sfery, którą według dzisiejszej terminologii należałoby nazwać bezpieczeństwem wewnętrznym państwa. Po drugie funkcję tę można przyrównać, nie zapominając o różnicach wynikających z kontekstów historycznych, do kompetencji ABW odnoszących się do rozpoznawania zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny. Po trzecie funkcja *cura agendarum* obejmowała najprawdopodobniej też działania, nazywane obecnie kontrwywiadowczymi, realizowane w głównej mierze przez ABW. Po czwarte *agentes in rebus* ścigali sprawców najcięższych przestępstw skierowanych przeciwko państwu, co również leży w kompetencjach ABW.

Podobieństw między *agentes in rebus* a Agencją Bezpieczeństwa Wewnętrznego można się doszukiwać również w „sekretnym" sposobie działania *agentes*, co kojarzy się z niejawnymi czynnościami operacyjno-rozpoznawczymi prowadzonymi przez funkcjonariuszy ABW. Ponadto *agentes in rebus* funkcjonowali w ramach struktury administracji cywilnej (tj. niewojskowej), używając jednocześnie „stopni wojskowych", a wykonywane przez nich zadania dotyczyły raczej sfery cywilnej niż wojskowej. W tym sensie *agentes in rebus* można uznać za pierwszą „cywilną służbę specjalną" w historii państw europejskich.

Abstract

The article outlines the secret service of the late Roman empire and the early Byzantine empire (from the end of the 3rd until the beginning of the 8th century) as the precursor of the contemporary Polish special service – the Internal Security Agency. Officers of this late-ancient service were called *agentes in rebus*, i.e. "working on cases".

One of the areas of activities of *agentes in rebus* was informing the emperor and his closest collaborators, among other things, about activities of the civil and military officials and of private persons that could pose a threat to the emperor's power. If it is possible to name an institution in contemporary Poland, whose powers include something that in today's reality might be called *cura agendarum,* it is, undoubtedly, the Internal Security Agency. Firstly, because the area of operation of *cura agendarum,* according to the present terminology should be called the internal security of the state. Secondly, bearing in mind the differences resulting from the historical contexts, this function can be compared to the powers of the ABW in the area of recognizing threats to the internal security of the country and its constitutional order. Thirdly, the function

of *cura agendarum* most probably included the activities that are today referred to as counterintelligence, carried out mostly by the ABW. Fourthly, *agentes in rebus* prosecuted perpetrators of the most serious crimes, which also lies within the scope of the ABW powers.

The similarities between *agentes in rebus* and the Internal Security Agency can also be found in the secrecy of operation of agents, which seems similar to the secret operational and investigative activities conducted by ABW officers. Moreover, *agentes in rebus* operated within civil administration (and not in the military), using at the same time military ranks. They concerned civil affairs rather than the military. In this sense, *agentes in rebus* can be regarded as the first "civil special service" in the history of the European countries.

II
STUDIA I ANALIZY

Anna Kańciak

Problematyka cyberprzestępczości w Unii Europejskiej

Kwoty utraconych pieniędzy z powodu przestępstw popełnianych w cyberprzestrzeni, o czym dowiadujemy się, analizując statystyki, na każdym robią ogromne wrażenie, niezależnie czy odbiorcą tych danych jest ekspert, czy zwykły obywatel. Nie trudno się więc dziwić, że z powodu straconych rocznie miliardów dolarów kwestia bezpieczeństwa w cyberprzestrzeni staje się centralnym punktem zainteresowania decydentów, służb ochrony porządku publicznego oraz przedstawicieli sektora prywatnego. Tak szerokie zainteresowanie powoduje, że wymiar cyberprzestępczości nie jest wyłącznie prawno-karny czy informatyczny, ale również społeczny i gospodarczy[1].

Ponadto uwagę opinii społecznej zwracają również tzw. cyberataki na obiekty należące do infrastruktury krytycznej czy na strony internetowe organów administracji państwowej, które w połączeniu z ponadnarodowym sporem o ACTA[2] powodują że społeczność międzynarodowa stanęła wobec nowego niebezpieczeństwa, jakim jest cyberprzestępczość.

Już po kilkuzdaniowym wstępie można mieć wyobrażenie, jakie trudności pojawiają się podczas analizowania przestępstw popełnianych w cyberprzestrzeni. Od kwestii terminologicznych przez zakres przedmiotowy i podmiotowy cyberprzestępstw po kluczowe pytanie o istotę i powszechnie przypisywaną cechę nowości temu zjawisku.

Z uwagi na zakres artykułu nie jest możliwe udzielenia odpowiedzi na wszystkie pytania i rozstrzygnięcie wątpliwości. Dlatego też, po krótkim wyjaśnieniu istoty przestępstw w cyberprzestrzeni, zostanie przedstawiony zarys podejmowanych obecnie działań w Unii Europejskiej zapobiegających tego rodzaju przestępczości i ją zwalczających.

Międzynarodowy wymiar prac nad cyberprzestępczością

„Cyberprzestępczość" jest pojęciem, które dość szybko zostało włączone do powszechnego użycia. Nie stanowi również większej trudności intuicyjne zdefiniowanie go. Jednak z uwagi na swoją wieloaspektowość, zarówno po stronie doktryny, jak i praktyki, pojawiło się wiele sporów i niejasności terminologicznych.

Na poziomie krajowym wyjaśnienie tego pojęcia zostało zawarte w kluczowym dla tej problematyki dokumencie – Rządowym Programie Ochrony Cyberprzestrzeni

---

[1] R Lusawa., *Ekonomiczno-społeczne uwarunkowania cyberprzestępczości, wersja elektroniczna* [online], http://wbs.ks.net.pl/pliki/Lusowa9.pdf., s. 2 [dostęp: 2 VI 2012].

[2] Umowa handlowa dotycząca zwalczania obrotu towarami podrabianymi (*Anti-Counterfeiting Trade Agreement* – ACTA) – umowa międzynarodowa mająca ustalić międzynarodowe standardy w walce z naruszeniami własności intelektualnej. Szerzej: *Wniosek. Decyzja Rady w sprawie zawarcia umowy handlowej dotyczącej zwalczania obrotu towarami podrobionymi między Unią Europejską i jej Państwami Członkowskimi, Australią, Kanadą, Japonią, Republiką Korei, Meksykańskimi Stanami Zjednoczonymi, Królestwem Marokańskim, Nową Zelandią, Republiką Singapuru, Konfederacją Szwajcarską i Stanami Zjednoczonymi Ameryki*, Bruksela, dnia 24.06.2011 r., KOM(2011) 380 wersja ostateczna.

RP – i oznacza *czyn zabroniony popełniony w obszarze cyberprzestrzeni*[3]. Z kolei „cyberprzestrzeń" określono jako cyfrową przestrzeń przetwarzania i wymiany informacji tworzoną przez systemy i sieci teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami[4]. Dodatkowo program wprowadza, na potrzeby realizacji jego założeń, definicję „cyberprzestrzeni RP"[5].

Sama problematyka cyberprzestępczości nie jest zjawiskiem zupełnie nowym. Zainteresowanie tym tematem pojawiło się już na początku XX wieku, jednak dowodem podjęcia faktycznych prac w przedmiotowym zakresie jest ogłoszona w 2001 r. Konwencja Rady Europy o cyberprzestępczości[6]. Co prawda w konwencji nie zdefiniowano wprost pojęcia cyberprzestępczości, ale wskazano na zagrożenia wymagające wspólnego działania w ramach ochrony sieci informatycznych i informacji elektronicznych przed ich wykorzystaniem w celu popełniania przestępstw[7]. Poza środkami, jakie należy podjąć na szczeblu krajowym, zwrócono w niej uwagę na trzy rodzaje przestępstw[8]:

1) komputerowe:
   – fałszerstwo komputerowe,
   – oszustwo komputerowe,
2) ze względu na charakter zawartych informacji:
   – przestępstwa związane z pornografią dziecięcą,
3) związane z naruszeniem praw autorskich i praw pokrewnych.

Przedmiotowa konwencja, która z perspektywy kilkunastu lat od momentu jej przyjęcia i zdobytych doświadczeń może wydawać się bardzo ogólna i nieprecyzyjna, jest solidną podstawą do tworzenia wspólnej polityki krajów członkowskich[9] Rady Europy w zakresie zwalczania cyberprzestępczości. Ponadto wciąż jest punktem odniesienia wielu rozwiązań prawnych w pracach nad przeciwdziałaniem zagrożeniom cyberbezpieczeństwa i zwalczaniem tych zagrożeń. Dowodem na to są dokumenty i programy pojawiające się na forum Unii Europejskiej. Najnowszym dokumentem jest komunikat Komisji Europejskiej z 28 marca 2012 r. wprowadzający definicję „cyberprzestępczości" rozumianej jako *wysokodochodowa, niskiego ryzyka forma przestępczej działalności, która coraz bardziej staje się powszechna i szkodliwa*[10].

Jednak wyjaśnienie terminu cyberprzestępczości pojawiło się już wcześniej w *Europejskiej agendzie cyfrowej*, dokumencie Komisji Europejskiej, w którym okre-

---

[3] *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016*, MSWiA, Warszawa 2010, s. 6,. http://bip.msw.gov.pl/portal/bip/6/19057, s. 6 [dostęp: 24 VI 2012].

[4] Tamże.

[5] Cyberprzestrzeń RP to cyberprzestrzeń w obrębie terytorium państwa Polskiego i w lokalizacjach poza terytorium, gdzie funkcjonują przedstawiciele RP (placówki dyplomatyczne, kontyngenty wojskowe), tamże, s. 6.

[6] *Konwencja o cyberprzestępczości* (*Convention on cybercrime*), Budapeszt, 23 listopada 2001 r., ETS nr 185.

[7] Tamże, s. 1.

[8] Tamże, s. 3–6.

[9] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożeń cyberterroryzmem*, Warszawa 2010, Wolters Kluwer, s. 81.

[10] *Komunikat Komisji do Rady i Parlamentu Europejskiego. Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością*, Bruksela, dnia 28.03.2012, KOM(2012) 140 wersja ostateczna, s. 2.

ślono ją jako *nową formę przestępczości obejmującą między innymi wykorzystywanie dzieci, kradzież tożsamości i ataki cybernetyczne*[11].

Analizując przytoczone sposoby definiowania pojęcia cyberprzestępczości, można zuważyć nie tylko niejednolity stopień szczegółowości tych definicji, ale również – z uwagi na okoliczności powstawania dokumentów, w których są zawarte – różny ich zakres przedmiotowy. Dodatkowo należy również przywołać charakterystykę cyberprzestępczości przedstawioną w obszernym materiale Parlamentu Europejskiego, która została opracowana na podstawie doświadczeń państw członkowskich UE. Parlament Europejski dokonując analizy zebranych materiałów oraz korzystając z dorobku całej Unii w zakresie cyberprzestępczości, wskazał, że jako jedna z największcyh obaw i zagrożeń dla zinformatyzowanego współczesnego świata, charakteryzuje się ona:

- ogromną skalą,
- niejednoznaczną naturą podmiotów w cyberprzestrzeni,
- używaniem w dużej mierze podobnych technik ataków,
- zaawansowaniem i wysokim poziomem dochodowości,
- dużym zróżnicowaniem i trudnością w przeciwdziałaniu i zwalczaniu[12].

Rozpatrując działania Unii Europejskiej w zakresie ochrony cyberprzestrzeni, przede wszystkim należy zwrócić uwagę na dwutorowość podejmowanych prac, w czym również jest upatrywana słabność wszelkich inicjatyw. Podział prac UE został dokonany na dwa obszary ze względu na krytetium przedmiotu:

1) zwalczanie cyberataków (włączając w to cyberprzestępczość i cyberterroryzm),
2) utrzymanie ochrony:
   – infrastruktury krytycznej (Critical Infrastructure Security – CIS),
   – bezpieczeństwa sieci i informacji (Network and Information Security – NIS),
   – krytycznej infrastruktury informatycznej (Critical Information Infrastructure Protection – CIIP)[13].

Zgodnie podziałem na kwestie ochrony z jednej strony, a zwalczanie cyberataków z drugiej, są przygotowywane kluczowe unijne programy i strategie. Jednak z uwagi na pewien wspólny zakres odnoszący się chociażby do definiowania podstawowych pojęć, wielokrotnie dochodzi do powielania prac i braku jednolitości instytucji unijnych w podejściu do tej problematyki.

Zanim jednak podda się krytyce wysiłki UE podejmowane w celu przeciwdziałania cyberprzestępczości, należy zwrócić uwagę na bardzo istotną kwestię. Zauważona powyższej rozbieżność w podejściu i próbach uregulowania zagadnienia ochrony cyberprzestrzeni wynika z traktatowego[14] podziału obszarów, w ramach których odpowiednie podmioty wypracowują nowe narzędzia i mechanizmy działania.

W zakresie pierwszego kierunku zmierzającego do zwalczania cyberprzestępstw jako czynów prawnie zabronionych, niosących za sobą konkretny wymiar karny

---

[11] *Komunikat Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska agenda cyfrowa*, Bruksela, dnia 26.08.2010, KOM(2010) 245 wersja ostateczna/2, s. 6.

[12] *Cybersecurity and cyberpower: concepts, conditions and capabilities for cooperation for action within the EU*, Policy Department Directorate-General for External policies of the Union, EXPO/B/SEDE/FWC/2009-01/LOT6/09, April 2009 r., s. 7.

[13] Tamże, s. 27.

[14] Stan prawny wprowadzony *Traktatem z Lizbony zmieniającym Traktat o Unii Europejskiej i Traktat ustanawiający Wspólnotę Europejską*", Dz.Urz. UE C 306 z 17 grudnia 2007, s. 1.

i społeczny, wszelkie działania podlegają przepisom Tytułu V (*Przestrzeń wolności, bezpieczeństwa i sprawiedliwości*) *Traktatu o funkcjonowaniu Unii Europejskiej* (TFUE)[15]. Dlatego też, zgodnie z przedmiotowym i kompetencyjnym podziałem struktur unijnych, problematyka ta jest podejmowana przez Dyrekcję Generalną do Spraw Wewnętrznych. Z kolei ochrona infrastruktury krytycznej i teleinformatycznej, należąca do kompetencji Dyrekcji Generalnej ds. Społeczeństwa Informatycznego (DG INFOSO)[16], jest uregulowana w Tytule VIII (*Polityka gospodarcza i pieniężna*) TFUE[17].

Każdy z tych dwóch tematów doczekał się szczegółowych regulacji i planów działania. Jednak z uwagi na zakres artykułu zostanie w nim przedstawiona problematyka cyberprzestępczości w kontekście przeciwdziałania temu zjawisku i jego zwalczania, czyli pierwszemu z przedstawionych obszarowi.

W ramach kierunku zajmującego się cyberprzestępczością, realizowanego zgodnie z przepisami *Przestrzeni wolności, bezpieczeństwa i sprawiedliwości,* przede wszystkim należy zwrócić uwagę na *Decyzję Ramową Rady w sprawie ataków na systemy informatyczne* przyjętą w 2005 r.[18] stanowiącą kamień milowy w zwalczaniu tego procederu. Wymaga ona od państw członkowskich wprowadzenia do krajowych systemów prawnych regulacji dotyczących skutecznego działania przeciwko podstawowym typom cyberataków. Ponadto, co ważniejsze, wprowadza wspólną definicję takich ataków. Przyjmując tę decyzję, państwa zgodziły się na wspólne wyjaśnienia takich czynów zabronionych, jak:

- nielegalny dostęp do systemów informatycznych,
- nielegalna ingerencja w system,
- nielegalna ingerencja w dane[19].

Kolejne kroki podjęto w następstwie ataków terrorystycznych w Londynie i Madrycie. Wtedy to cała uwaga instytucji i agencji unijnych oraz organizacji międzynarodowych zajmujących się zapewnianiem bezpieczeństwa skupiła się wokół problematyki zagrożenia atakami terrorystycznymi. Po analizach tamtych wydarzeń zaczęto identyfikować słabe punkty całego systemu bezpieczeństwa oraz rozważać możliwości ograniczania zakresu praw i obowiązków na rzecz *porządku publicznego, tj. zachowania bezpieczeństwa narodowego (tj. bezpieczeństwa państwa), obronności, bezpieczeństwa publicznego czy też zapobiegania, dochodzenia, wykrywania i ścigania przestępstw lub nielegalnego wykorzystania systemów łączności elektronicznej*[20]. Zwrócono uwagę na stopień dostępności do danych i przygotowano – jak się później okazało, kontrowersyjny – dokument w sprawie retencji danych[21], zwany w skrócie Europejską Dyrektywą. Konieczność wprowadzenia takich regulacji wynikała z dąże-

---

[15] Wersja skonsolidowana *Traktatu o funkcjonowaniu Unii Europejskiej* (TFUE), Dz.Urz. UE C 83 z 30 marca 2010 r., s. 73–85.

[16] Od 1 lipca 2012 r. zmienione na DG CONNECT – *Directorate General for Communications Networks, Content and Technology.*

[17] *Traktat o funkcjonowaniu Unii Europejskiej*…, s. 78–79.

[18] *Decyzja Ramowa Rady 2005/222/WSiSW z dnia 24 lutego 2005 r. w sprawie ataków na systemy informatyczne*, Dz.Urz. UE L 69 z 16 marca 2005 r.

[19] Tamże, s. 69.

[20] *Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności oraz zmieniająca dyrektywę 2002/58/WE*, Dz.Urz. UE L 105 z 15 marca 2006 r., s. 54.

[21] Tamże.

nia do nałożenia na dostawców ogólnie dostępnych usług łączności elektronicznej lub publicznych sieci łączności obowiązków w zakresie przechowywania pewnych danych przez nich generowanych lub przetwarzanych, aby zapewnić dostępność tych danych w razie dochodzenia, wykrywania i ścigania poważnych przestępstw, określonych w ustawodawstwie każdego państwa członkowskiego[22]. Drugim celem, który pośrednio przyświecał pomysłodawcom tego dokumentu, było zwiększenie efektywności środków służących zwalczaniu cyberprzestępczości oraz innych form przestępczej aktywności.

Z kolei w 2007 r. Komisja Europejska przygotowała Komunikat pod nazwą *W kierunku ogólnej strategii zwalczania cyberprzestępczości*[23], obecnie dość rzadko przytaczany z uwagi na niepodjęcie dalszych prac na forum unijnym nad przedmiotową strategią. Warto jednak poświęcić mu chwilę uwagi ze względu na poruszone w nim zagadnienia mające istotne znaczenie w działaniach w zakresie przeciwdziałania cyberprzestępczości.

W komunikacie, poza ogólnym celem, jakim jest zwalczanie cyberprzestępczości na poziomie krajowym, unijnym i międzynarodowym oraz próbą zdefiniowania cyberprzestępczości i określeniem jej wymiaru i tendencji, za najważniejsze inicjatywy Komisja i państwa członkowskie uznały:

- koncentrację działań na ściganiu przestępstw oraz na aspektach prawnokarnych zwalczania przestępczości,
- uzupełnienie innych działań UE poprawiających ogólne bezpieczeństwo w przestrzeni wirtualnej o elementy przyszłej strategii zwalczania cyberprzestępczości,
- lepszą współpracę operacyjną organów ścigania; lepszą współpracę i koordynację polityczną między państwami członkowskimi,
- współpracę polityczną i prawną z krajami trzecimi, podnoszenie świadomości; szkolenia, badania; ściślejszy dialog z sektorem przemysłu i ewentualne działania legislacyjne[24].

Tego rodzaju założenia w zestawieniu z praktyczną ich realizacją mogą spotkać się z pewną krytyką. Należy jednak mieć na uwadze nie tylko procedury obowiązujące w instytucjach unijnych, ich traktatowy zakres kompetencyjny, lecz także skutki tego rodzaju dokumentów i ich przełożenie w późniejszych działaniach na poziomie UE.

Wynikiem podjętych prac zmierzających do zidentyfikowania kluczowych obszarów wymagających wspólnych działań na poziomie międzynarodowym, w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości, było przyjęcie w 2009 r. *Programu sztokholmskiego*[25] będącego najnowszym programem pięcioletnim (na lata 2010–2014[26]), w którym przez wyznaczanie obszarów priorytetowych sprecyzowano postanowienia Traktatu z Lizbony dotyczące tego zagadnienia. Należy podkreślić, że

---

[22] Tamże, art. 1.

[23] *Komunikat Komisji do Parlamentu Europejskiego, Rady i Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości,* Bruksela, dnia 22.05.2007, KOM (2007) 267 wersja ostateczna.

[24] Tamże, s. 4.

[25] *Informacje instytucji, organów i jednostek organizacyjnych Unii Europejskiej, Rada Europejska Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli*, Dz.Urz. UE C 115 z 4 maja 2010 r., s. 1.

[26] Przyjęty przez Radę Europejską na posiedzeniu 10–11 grudnia 2009 r., zaczął obowiązywać od 1 stycznia 2010 r. Jest to trzeci z kolei program obejmujący szeroki zakres tematyczny bezpieczeństwa, począwszy od zarządzania zewnętrznymi granicami UE do sądowej współpracy w sprawach karnych i cywilnych. Pierwszy powstał w Tempere (1999–2004), kolejny to Program haski (2005–2009). Więcej: *Unia Europejska. System prawny, porządek instytucjonalny, proces decyzyjny*, J. Barcz (red. nauk.), Warszawa 2009, KSAP & EuroPres. s. 657.

dokument ten to olbrzymi krok w zwiększaniu bezpieczeństwa wewnętrznego UE, gdyż zawiera wiele odwołań do ochrony cyberprzestrzeni. Nie tylko zalicza cyberprzestępczość do sześciu głównych priorytetów dla całej UE, lecz także wzywa do:

- propagowania prawodawstwa, które zapewnia bardzo wysoki poziom bezpieczeństwa sieci i umożliwia szybsze reagowanie w przypadku ataków cybernetycznych,
- przyspieszenia procesu ratyfikacyjnego *Konwencji o cyberprzestępczości*[27],
- udzielenia pełnego poparcia krajowym podmiotom powiadamiania o zagrożeniach, odpowiedzialnym za walkę z cyberprzestępczością,
- współpracy z państwami spoza Unii,
- wzmocnienia (usprawnienia) partnerstwa publiczno-prywatnego,
- poprawy współpracy sądowej w sprawach dotyczących cyberprzestępczości[28].

Kolejnym krokiem Komisji Europejskiej było przygotowanie wniosku Dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne[29], który był związany z wdrożeniem i zastosowaniem postanowień wspomnianej już Decyzji Ramowej z 2005 r. w sprawie ataków na systemy informatyczne. W wyniku przeprowadzonego przeglądu okazało się, że *ataki, jakie miały miejsce w całej Europie od czasu przyjęcia decyzji ramowej, uświadamiają wiele rodzących się zagrożeń, a w szczególności pojawienie się zjawiska masowych jednoczesnych ataków na systemy informatyczne oraz wzrost przestępczego wykorzystania tzw. botnetów*[30]. Wniosek został, co prawda z pewnymi poprawkami, pozytywnie przyjęty przez Parlament Europejski[31]. Obecnie trwają prace w Komisji Europejskiej nad jego zaktualizowaniem, uzupełnieniem o opinię Parlamentu oraz rozpoczęciem i przeprowadzeniem procedury legislacyjnej tak, aby akt wszedł w życie najpóźniej na początku 2013 r.

Z kolei drugim dokumentem o dość dużym poziomie ogólności, choć kluczowym z punktu widzenia ochrony bezpieczeństwa wewnętrznego, jest Strategia Bezpieczeństwa Wewnętrznego[32]. Odnosi się ona wprost do cyberprzestępczości, którą zaliczono

---

[27] Polska podpisała Konwencję 23 listopada 2001 r., jednak nie została ona dotychczas ratyfikowana. [podkreślenie aut. art.]. Prace legislacyjne podjęte w Polsce po podpisaniu konwencji doprowadziły do zgodności prawa krajowego z większością jej przepisów. Podobna sytuacja jest z *Protokołem dodatkowym do Konwencji o cyberprzestępczości dotyczącym kryminalizacji działań o charakterze rasistowskim i ksenofobicznym popełnianych przy użyciu systemów komputerowych*, który Polska podpisała 21 lipca 2003 r. Więcej: http://bip.ms.gov.pl/pl/ministerstwo/wspolpraca-miedzynarodowa/rada-europy/konwencje-rady-europy-z-obszaru-sprawiedliwosc-i-sprawy-wewnetrzne-podpisaneratyfikowane-przez-polske/ [dostęp: 17 VI 2012].

[28] *Informacje instytucji, organów i jednostek organizacyjnych*…, s. 15–23.

[29] *Wniosek. Dyrektywa Parlamentu Europejskiego i Rady dotycząca ataków na systemy informatyczne i uchylająca decyzję ramową Rady 2005/222/WSiSW*, Bruksela, dnia 30.09.2010 r., KOM(2010)517 wersja ostateczna, 2010/0273 (COD).

[30] Tamże, s. 1. Pojęcie „botnetu" oznacza *sieć komputerów zarażonych złośliwym oprogramowaniem (wirusami komputerowymi). Taka sieć zainfekowanych komputerów (tzw. zombie) może zostać aktywowana do wykonywania szczególnych zadań, takich jak ataki na systemy informatyczne (cyberataki). Owe komputery „zombie" można kontrolować – często bez wiedzy użytkowników zainfekowanych komputerów – z innego komputera* […] nazywanego również „centrum dowodzenia i kontroli" (*command-and-control centre*). Szerzej: tamże, s. 2 (*Uzasadnienie pkt 1.*).

[31] *Opinia Komisji Spraw Zagranicznych dla Komisji Wolności Obywatelskich, Sprawiedliwości i Spraw Wewnętrznych w sprawie wniosku dotyczącego dyrektywy Parlamentu Europejskiego i Rady dotyczącej ataków na systemy informatyczne i uchylającej decyzję ramową Rady 2005/222/WSiSW, z 28.11.2011 r.*, [COM(2010)0517 – C7-0293/2010 – 2010/0273(COD)] [online], http://www.europarl.europa.eu/meetdocs/2009_2014/documents/afet/ad/883/883545/883545pl.pdf, 2010/0273(COD).

[32] *Komunikat Komisji do Parlamentu Europejskiego i Rady. Strategia bezpieczeństwa wewnętrznego UE w działaniu: pięć kroków w kierunku bezpieczniejszej Europy*, Bruksela, dnia 22.11.2010 r., KOM(2010) 673 wersja ostateczna (dok. 16797/10 JAI 990 z 23.11.2010 r.). Zgodnie z założeniem Programu

do pięciu strategicznych celów dla bezpieczeństwa wewnętrznego UE z uwagi na fakt, że Europa ze względu na zaawansowaną infrastrukturę Internetu, wysoką liczbę jego użytkowników oraz przekazywane przez Internet oszczędności i system płatności jest kluczowym celem dla cyberprzestępców. Wymaga to jeszcze lepszej ochrony zarówno obywateli, przedsiębiorców czy rządów, jak i infrastruktury krytycznej[33]. Mając na uwadze zadania stawiane Strategii przez *Program sztokholmski*[34], zakłada się w niej podjęcie następujących kroków[35]:

1) do 2013 r. ustanowienie centrum ds. cyberprzestępczości w UE, które pomoże wzmocnić analityczne i operacyjne zdolności dochodzeniowo-śledcze oraz przyczyni się do zwiększenia współpracy z państwami trzecimi,
2) zapewnienie, w toku postępowań dochodzeniowo-śledczych, wspólnych standardów dla policji, sądów, prokuratorów,
3) w zakresie współpracy z sektorem przemysłowym, w celu ochrony i wzmocnienia pozycji obywateli, zapewnienie systemu raportowania o incydentach w cyberprzestrzeni,
4) w celu poprawy zdolności zwalczania przestępstw w cyberprzestrzeni:
   – utworzenie do 2012 r. sprawnego Centrum Reagowania na Incydenty Komputerowe UE (EU CERT)[36],
   – połączenie do 2012 r. krajowych (rządowych) zespołów CERT działających w państwach członkowskich; będzie to ważnym instrumentem w utworzeniu do 2013 r. Europejskiego System Wymiany Informacji i Powiadamiania (*European Information Sharing and Alert System* – EISAS) dla szerszej rzeszy odbiorców,
   – rozwój krajowych programów reagowania i przeprowadzenie regularnych ćwiczeń na poziomie krajowym i europejskim z zakresu reagowania na incydenty i naprawy szkód.

Ostatnim dokumentem, co prawda dość ogólnie odnoszącym się do problematyki cyberprzestępczości, ale bezpośrednio wiążącym się z wcześniejszym dokumentem określającym wstępną strategię pracy służącą zwalczaniu cyberprzestępczości[37], jest projekt konkluzji Rady na temat planu wdrażania zorganizowanej strategii walki z cyber-

---

sztokholmskiego nowa strategia powinna uwzględniać postanowienia Europejskiej Strategii Bezpieczeństwa przyjętej przez Radę Europejską 12 grudnia 2003 r., która dotyczy bezpieczeństwa Europy w wymiarze zewnętrznym, często nazywaną Europejską Strategią Bezpieczeństwa (European Security Strategy).

[33] Tamże, s. 4.

[34] *W celu zwiększenia bezpieczeństwa w Europie strategia powinna mieć na celu zacieśnienie współpracy w dziedzinie egzekwowania prawa, zarządzania granicami, ochrony ludności, zarządzania katastrofami, jak również współpracy wymiarów sprawiedliwości w sprawach karnych*, szerzej: *Informacje instytucji, organów i jednostek organizacyjnych Unii Europejskiej, Rada Europejska Program sztokholmski – otwarta i bezpieczna Europa dla dobra i ochrony obywateli*, Dz.Urz. UE C 115 z 4 maja 2010 r., s. 5.

[35] *Komunikat Komisji do Parlamentu Europejskiego i Rady. Strategia bezpieczeństwa wewnętrznego...,* s. 9–10.

[36] Testowa wersja Centrum Reagowania na Incydenty Komputerowe (*Computer Emergency Response Pre-configuration Team* – CERT-EU) powstała 1 czerwca 2011 r. Centrum składa się z ekspertów ds. bezpieczeństwa IT z głównych instytucji unijnych: Komisji Europejskiej, Parlamentu Europejskiego, Sekretariatu Generalnego Rady UE, Komitetu Regionów, Komitetu Ekonomiczno-Społecznego. Po roku od jego utworzenia, po pozytywnej opinii wydanej po przeprowadzeniu przeglądu, została wydana decyzja o ustanowieniu od 11 września 2012 r. w pełni funkcjonującego CERT-u UE. Szerzej: http://www.enisa.europa.eu/activities/cert/background/inv/cert-eu [dostęp: 17 XII 2012].

[37] *Projekt konkluzji Rady w sprawie uzgodnionej strategii pracy i konkretnych środków służących zwalczaniu cyberprzestępczości*, dok. 15569/08 ENFOPOL 224 CRIMORG 190. W konkluzjach zwrócono się do państw członkowskich i Komisji, aby wprowadziły środki opracowane na podstawie analizy zaist-

przestępczością[38]. Wskazano w nim, jakie działania należy podjąć, aby zrealizować postanowienia strategii, której celem jest dostosowanie sposobów eliminowania cyberprzestępczości w zależności od rodzaju przestępstw popełnianych drogą elektroniczną: pornografii dziecięcej, działalności terrorystycznej, ataków na sieci elektroniczne, oszustw, kradzieży tożsamości itd.[39] W perspektywie krótkoterminowej, zgodnie z dokumentem, należy zwrócić uwagę na działania zmierzające do zweryfikowania i zintensyfikowania prac Europejskiej Platformy ds. Walki z Cyberprzestępczością[40] tak, aby ułatwić gromadzenie, wymianę i analizowanie informacji[41].

Z kolei w perspektywie średnioterminowej przede wszystkim zwrócono uwagę na konieczność ratyfikacji Konwencji o cyberprzestępczości z 2001 r., a następnie na podniesienie standardów procedur szkolenia policji, sędziów, prokuratorów i służb kryminalistycznych ułatwiającego prowadzenie czynności procesowych w dziedzinie cyberprzestępczości. Konieczne jest również propagowanie procesu zharmonizowania różnych całodobowych sieci oraz punktów kontaktowych dla organów ochrony porządku publicznego, eliminując nakładanie się działań podejmowanych na forach współpracy międzynarodowej takich, jak np. G8 i Interpol[42].

Europejskie Centrum ds. Walki z Cyberprzestępczością (*European Cybercrime Centre* – EC3)

Wspomniane postulaty, w myśl których chodziło nie tylko o zbieranie danych na temat cyberprzestępstw, przyjmowanie wspólnych standardów szkolenia i działania, lecz także o unikanie powielania działań, miały na celu stworzenie właściwej podstawy powołania centrum ds. cyberprzestępczości, zapowiadanego już od 2007 r.[43] Idea stworzenia w Unii Europejskiej jednego ośrodka, który w sposób kompleksowy zająłby się problematyką cyberprzestępczości, była wielokrotnie przywoływana we wszystkich wspomnianych dokumentach: od aktów wypracowywanych na poziomie eksperckim przez komunikaty Komisji po kluczowe programy i strategie w ramach przestrzeni wolności, bezpieczeństwa i sprawiedliwości. Po niemalże pięcioletnich wysiłkach, po wcześniejszym przeprowadzeniu przez Komisję Europejską studium wykonalności oraz po osiągnięciu wstępnego

niałych przypadków, uwzględniające postęp techniczny i umożliwiające przygotowanie – w krótkiej lub średniej perspektywie – narzędzi operacyjnych.

[38] *Projekt konkluzji Rady na temat planu wdrażania zorganizowanej strategii walki z cyberprzestępczością*, dok. 5957/2/10 z 25 marca 2010 r.

[39] *Projekt konkluzji Rady na temat planu wdrażania…*, s. 1.

[40] Platforma (*European Cybercrime Platform* – ECCP) została utworzona zgodnie z postanowieniami *Komunikatu Komisji do Parlamentu Europejskiego, Rady, Europejskiego Komitetu Ekonomiczno-Społecznego i Komitetu Regionów. Europejska agenda cyfrowa,* Bruksela, dnia 26.08.2010 r., KOM(2010) 245 wersja ostateczna/2.

[41] Europejski Urząd Policji (Europol) wraz z Komisją został poproszony o połączenie wszystkich właściwych krajowych platform w UE w jedną platformę ostrzegania o cyberprzestępczości. Europejska platforma ostrzegania funkcjonowałaby jako centrum, które zbierałoby i przechowywało informacje na temat przestępstw związanych z Internetem w celu dokonywania regularnych raportów statystycznych poświęconych cyberprzestępczości. W dalszych działaniach ECCP będzie znaczącym elementem mającego powstać do 2013 r. Centrum ds. Cyberprzestępczości.

[42] *Projekt konkluzji Rady na temat planu wdrażania…*, s. 6–7.

[43] W ramach ogólnych perspektyw zwalczania cyberprzestępczości wskazano na możliwość stworzenia, w ramach współpracy, centralnego unijnego punkt kontaktowego ds. cyberprzestępczości, *Komunikat Komisji do Parlamentu Europejskiego, Rady oraz Komitetu Regionów. W kierunku ogólnej strategii zwalczania cyberprzestępczości*, Bruksela, dnia 22.05.2007 r., KOM(2007) 267 wersja ostateczna, s. 11.

kompromisu co do siedziby i zadań, społeczność unijna doczekała się oficjalnej informacji zawartej w Komunikacie Komisji Europejskiej[44] o sformalizowaniu prac nad utworzeniem Europejskiego Centrum ds. Walki z Cyberprzestępczością (*European Cybercrime Centre* – EC3). W dokumencie tym Komisja zaleca utworzenie takiego centrum, które będąc częścią struktur Europolu, będzie spełniać funkcję punktu koordynującego działania w zakresie walki z cyberprzestępczością w UE[45]. Nie tylko sprecyzowano w nim przedmiot[46] prac EC3, lecz także wskazano na jego zadania, do których należy:

- służenie jako europejski punkt kontaktowy w zakresie informacji dotyczących cyberprzestępczości,
- gromadzenie dostępnej w Europie wiedzy specjalistycznej na temat cyberprzestępczości potrzebnej do budowania potencjału państw członkowskich w zakresie walki z tym zjawiskiem,
- wspieranie krajowych dochodzeń dotyczących cyberprzestępstw,
- zapewnienie wspólnego głosu służbom ścigania i służbom sądowniczym zaangażowanym w europejskie dochodzenia w zakresie cyberprzestępczości[47].

Kierując się zasadą racjonalnego gospodarowania środkami w dobie światowego kryzysu finansowego, wskazano, że Centrum EC3 powinno zostać umieszczone w ramach struktur Europolu. Z perspektywy rachunku zysków i strat, powszechnie wiadomo, że tworzenie jakiegokolwiek nowego podmiotu, w krajowym czy miedzynarodowym systemie organizacyjnym, zawsze pociąga za sobą znaczne koszty.

Centrum ze względu na spodziewane korzyści[48] oraz potrzebę reagowania na rozwijające się zjawisko cyberprzestępczości powinno współdziałać z czterema grupami podmiotów. Poza państwami członkowskimi, sektorem prywatnym oraz parnterami międzynarodowymi[49] na uwagę zasługuje grupa podmiotów unijnych takich, jak: Europejskie Kolegium Policyjne – CEPOL, Europejska Jednostka Współpracy Sądowej – EUROJUST czy unijny CERT-EU, z którymi Centrum powinno intensywnie współpracować. Dość długa lista podmiotów, które od momentu utworzenia EC3 będą zaangażowane w problematykę walki z cyberprzestępczością, jest wyrazem aktywnej odpowiedzi UE na wzrost

---

[44] *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej: ustanowienie Europejskiego Centrum ds. Walki z Cyberprzestępczością*, Bruksela, dnia 28.03.2012 r., KOM(2012) 140 wersja ostateczna.

[45] Tamże, s. 2.

[46] Główne formy cyberprzestępczości objęte zakresem działania prac Centrum:

– cyberprzestępstwa popełniane przez zorganizowane grupy przestępcze, szczególnie przestępstwa przynoszące duże zyski, takie jak oszustwa internetowe,
– cyberprzestępstwa wyrządzające poważne szkody ofiarom, np. przemoc seksualna wobec dzieci w internecie,
– cyberprzestępstwa (m.in. ataki cybernetyczne) w odniesieniu do infrastruktury kluczowej i najważniejszych systemów informacyjnych na terenie Unii.

Szerzej: *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej…*, s. 4.

[47] Tamże, s. 5–7.

[48] *Niesie to ze sobą różnorodne korzyści. Europol cieszy się uznaniem państw członkowskich i innych zainteresowanych stron, m.in. Interpolu i międzynarodowych organów ścigania. Posiada również uprawnienia w zakresie działań dotyczących przestępstw komputerowych* [...]. *Podstawowym zadaniem Europolu jest pomoc w osiągnięciu celu, jakim jest bezpieczniejsza Europa, z korzyścią dla wszystkich obywateli, i wspieranie organów ścigania UE dzięki wymianie i analizie danych wywiadu kryminalnego*, cyt. za: *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej…*, s. 7.

[49] Poza Interpolem wskazano na innych strategicznych partnerów na całym świecie, tamże, s. 8.

tego zjawiska. Wśród tych instytucji została także wskazana Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA), wzbudzająca najwiecej pytań i wątpliwości.

Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji została utworzona w 2004 r.[50] w celu zapewnienia wysokiego poziomu bezpieczeństwa sieci i informacji na rzecz: obywateli, konsumentów, przedsiębiorstw oraz organizacji sektora publicznego Unii Europejskiej[51]. Mając to na uwadze, można postawić pytanie, czy prace Agencji nie będą w pewnym zakresie powielały działań podejmowanych przez Centrum, co więcej, czy ENISA nie jest odpowiednim miejscem do jego umiejscowienia i stworzenia szeroko pojętej kompleksowej ochrony: od bezpieczeństwa sieci i informacji w sensie technicznym po ochronę prawno-karną w cyberprzestrzeni.

W tym miejscu należy wyjaśnić kwestie formalne i jednocześnie przywołać wspomniany na początku artykułu traktatowy podział problematyki odnoszącej się do cyberprzestrzeni, mający decydujący wpływ na działania całej UE w tym zakresie. Zgodnie z artykułem ust. 3 art. 1 Rozporządzenia[52] cele i zadania Agencji dotyczą:

- prac z dziedziny bezpieczeństwa sieci i informacji, które nie należą do działań objętych, po zmianach wprowadzonych Traktatem z Lizbony, Tytułem V (*Przestrzeń wolności, bezpieczeństwa i sprawiedliwości*) i VI (*Transport*) TFUE,
- wszystkich działań związanych z bezpieczeństwem publicznym, obroną, bezpieczeństwem państwa, w tym dobrem państwa, w odniesieniu do zagadnień dotyczących bezpieczeństwa, a także działań państwa w obszarze prawa karnego[53].

Wprowadzony rozporządzeniem zakres działania Agencji pozwala zrozumieć istniejącą dwutorowość w podejściu do cyberbezpieczeństwa, która uniemożliwia przekazanie jej nowych zadań w postaci zwalczania cyberprzestępczości.

Z punktu widzenia zasadności wyboru Europolu na siedzibę EC3 należy zwrócić uwagę na okres działania ENISY, która początkowo została utworzona na pięć lat[54]. Od tego momentu dwukrotnie, w 2008 r.[55] i 2011 r.[56], przedłużano mandat tej Agencji odpowiednio: o kolejne cztery lata, a następnie o rok – obecnie jest on ważny do 13 września 2013 r., co z pewnością nie stanowi dobrej podstawy do zmiany zakresu jej funkcjonowania oraz rozszerzania jej struktury.

Biorąc więc pod uwagę dokonywane co jakiś czas rewizje prac i działań ENISY oraz jej znacznie szerszy zakres kompetencyjny, wybór Europolu jako siedziby nowego Centrum ds. Walki z Cyberprzestępczością wydaje się być zasadny.

Na koniec należy zwrócić uwagę na wymiar merytoryczny i praktyczny utworzenia oraz umiejscowienia Centrum EC3 w ramach Europolu, czyli na to, co Komisja w swoim komunikacie nazwała *wpływem ustanowienia Europejskiego Centrum*

---

[50] *Rozporządzenie (WE) nr 460/2004 Parlamentu Europejskiego i Rady z dnia 10 marca 2004 r. ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji*, Dz.Urz. UE L 77 z 13.03.2004 r., s. 1.

[51] Tamże, art. 1, s. 38.

[52] Tamże.

[53] Tamże.

[54] Zgodnie z art. 27 rozporządzenia (WE) nr 460/2004 Agencja została utworzona na pięć lat, od 14 marca 2004 r.

[55] *Rozporządzenie Parlamentu Europejskiego i Rady (WE) nr 1007/2008 z dnia 24 września 2008 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania*, Dz.Urz. UE L 293 z 31.10.2008 r., s. 1–2.

[56] *Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 580/2011 z dnia 8 czerwca 2011 r. zmieniające rozporządzenie (WE) nr 460/2004 ustanawiające Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji w zakresie okresu jej działania*, Dz. Urz. UE L 165 z 24.06.2011 r., s. 3.

ds. Walki z Cyberprzestępczością na zasoby[57]. Biorąc pod uwagę uprawnienia Europolu w zakresie działań dotyczących przestępstw komputerowych[58], funckjonującą w jego ramach europejską platformę do walki z cyberprzestępczością (*European Cyber Crime Platform* – ECCP), Centrum ds. Przestępczości Zaawansowanej Technologicznie (*Hight Tech Crime Centre*)[59] oraz Europejską Grupę Zadaniową ds. Cyberprzestępczości (*European Cybercrime Task Force* – EUCTF)[60], szerokie zaangażowanie państw członkowskich, mające wpływ na posiadany zasób informacji, i jednocześnie możliwości analityczne Europolu, umiejscowienie Centrum w sprawnie funkcjonującym i dobrze znanym urzędzie wydaje się być uzasadnione. Z jednej strony rozwijanie kompetencji i możliwości zwalczania cyberprzestępczości, a z drugiej przesunięcie środków finansowych na rzecz Centrum, zostało wskazane jako kluczowe działanie nie tylko w *Ocenie zagrożenia wykorzystania Internetu przez zorganizowane grupy przestępcze* (tzw. iOCTA)[61], lecz także we wstępnym Programie Prac Europolu na 2013 r.[62]

Abstrakt

Pomimo pojawiających się sprzeciwów, nierzadko słusznych, niegodne z prawem działania w Internecie określono mianem cyberprzestępczości. Należy zauważyć, że zagrożenia w cyberprzestrzeni, z uwagi na daleko idące i dotkliwe konsekwencje, stały się jednym z priorytetowych tematów na arenach krajowej i międzynarodowej. Wyraźnym tego przejawem są pojawiające się programy walki z tym zjawiskiem, wspólne przedsięwzięcia sektora prywatnego i publicznego. Z uwagi na transgraniczny wymiar cyberprzestępczości czy ogólniej, działalności w Internecie, temat ten stał się również głównym zagadnieniem w polityce bezpieczeństwa wewnętrznego Unii Europejskiej, która podjęła działania w kierunku wypracowania mechanizmów przeciwdziałania i zwalczania przestępczości w cyberprzestrzeni.

W imię ochrony interesów państw członkowskich oraz samej Unii zostały podjęte działania legislacyjne i instytucjonale. Choć pierwszych inicjatyw z zakresu bezpieczeństwa w sieci na poziomie wspólnotowym można doszukiwać się już pod koniec lat 90., Unia weszła w fazę bardziej intensywnych prac z momentem przyjęcia kluczowego aktu, jakim jest Europejska Agenda Cyfrowa. Agenda stanowi odpowiedź i pierwszą na taką skalę reakcję Unii na widoczną zmianę punktu ciężkości w obszarach ludzkiej działalności – z form tradycyjnych na aktywność

[57] *Komunikat Komisji do Rady i Parlamentu Europejskiego, Zwalczanie przestępczości w erze cyfrowej…*, s. 7.

[58] Art. 4 ust. 1 (w związku z załącznikiem odnoszącym się do tego artykułu) *Decyzji Rady z dnia 6 kwietnia 2009 r. ustanawiająca Europejski Urząd Policji* (Europol) (2009/371/WSiSW, Dz.Urz. UE L 121 z 15.05.2009 r., s. 37.

[59] Centrum ds. Przestępczości Zaawansowanej Technologicznie w Europolu zapewnia państwom członkowskim wsparcie w ogólnym zwalczaniu cyberprzestępczości. W centrum tym powstaje europejska platforma służąca zaspokajaniu potrzeb państw członkowskich w tym ważnym i rozwijającym się obszarze działalności przestępczej. Szerzej: *Przegląd Europolu. Sprawozdanie ogólne z działalności Europolu*, Europejski Urząd Policji, 2011, s. 47.

[60] Utworzona przez szefów jednostek ds. cyberprzestępczości w UE, Komisję Europejską i Eurojust, powstała w Europolu w 2010 r. w celu stworzenia platformy dla osób zarządzających dochodzeniami i sprawami dotyczącymi cyberprzestępczości.

[61] *Threat Assessment (Abridged) Internet Facilitated Organised Crime – iOCTA*, Europol Public Information, Haga 7 stycznia 2011 r., File nr 2530–264, s. 3.

[62] *Europol Preliminary Work Programme*, Haga, 2 lutego 2012 r., File nr 1422–110r5.

w cyberprzestrzeni, co zostało zauważone zarówno w wymiarze gospodarczym (np. handel elektroniczny), jak i przestępczym (niezgodna z prawem działalność w sieci). Po trzech latach od jej przyjęcia, pomimo opóźnień terminowych i trudności finansowych, Agenda stała się punktem odniesienia do kolejnych działań Unii, które przejawiły się nie tylko w formie planów, projektów aktów pozalegislacyjnych czy komunikatów Komisji Europejskiej, ale również przyczyniły się do utworzenia nowego podmiotu na forum unijnym – Europejskiego Centrum ds. Cyberprzestępczości. Centrum, z uwagi na usytuowanie w Europolu oraz zakres zadań, stało się przedmiotem krytyki i fali wątpliwości.

Pamiętając jednak o traktatowych zdaniach Unii i ich zakresie oraz uwzględniając fakt, że Centrum rozpoczęło swoje funkcjonowanie z początkiem stycznia 2013 r., z oceną zasadności decyzji oraz prac unijnego ustawodawcy w zakresie cyberprzestępczości należy się jednak wstrzymać.

Abstract

Although some objections have been made, frequently justified ones, the unlawful acts committed online are called cybercrimes. Except for the technical imprecision, it must be noted that threats in the cyberspace, because of the far-reaching and severe consequences, have become a priority both in the national and international arena. A visible sign of that are new programmes designed to fight with this phenomenon, as well as joint initiatives launched jointly by the private and public sectors. Due to the trans-border dimension of cybercrime, or generally, of the activities in the Internet, it has become the main problem of the EU internal security policy. The European Union, often criticized for its ineffective and expensive actions, like other international organizations, has taken actions aiming to develop mechanisms of preventing and countering crime in the cyberspace.

In order to protect the interests of Member States and the EU, particularly at a time of crisis, legislative and institutional actions have been taken. Though the first initiatives regarding the Web were launched at the Community level in late 90s, the EU has intensified its work on this issue once the key act - the European Digital Agenda was adopted. In view of its scope, the Agenda is the EU's answer and its first wide range reaction to the shift of its focus in the area of human activity - from traditional behaviors to the activity in cyberspace, which has affected the economic (e.g. electronic commerce) and criminal areas (online illegal activity). Three years after its adoption, despite delays and financial difficulties, the Agenda has become a point of reference for any subsequent actions taken in the EU. They included plans, drafts of non-binding acts or the European Commission Communications. Moreover, those actions also contributed to the establishment of a new EU body, i.e. European Cyber Crime Centre. Due to its location in Europol's infrastructure as well as its scope of actions the Centre met with a lot of criticism and raised many doubts.

However, bearing in mind the EU treaty commitments and their scope and also the fact that the Centre was launched in January 2013, we should refrain from any premature judgment of the decisions and legitimacy as well as the EU law making as regards cybercrime.

Maciej Aleksander Kędzierski

Cybernetyczne ujęcie funkcjonowania związku przestępczego przy wykorzystaniu teorii układów autonomicznych (samodzielnych) Mariana Mazura. Zarys problematyki[1]

Marian Mazur jest twórcą teorii układów samodzielnych, opublikowanej w 1966 r.[2] Jednym z podstawowych pojęć tej teorii jest pojęcie „układu samodzielnego" (autonomicznego) jako układu *zdolnego do sterowania się oraz który potrafi przeciwdziałać utracie tej swojej zdolności*[3]. Założeniem powstania takiego układu jest możliwość jego istnienia w danym czasie i miejscu w celu realizowania funkcji układu oraz jego zdolność (umiejętność) do funkcjonowania w czasie. Podobne założenia dotyczą związku przestępczego (czasami grupy przestępczej). Powstaje wiec pytanie, na ile i w jakim zakresie będzie można wykorzystać teorię układów samodzielnych, ale także teorię informacji, do oceny funkcjonowania zorganizowanych grup przestępczych, które zyskały już określoną trwałość funkcjonowania w czasie. Na ile układ przestępczy będzie można uznać za układ samodzielny w rozumieniu teorii M. Mazura oraz jakie relacje mogą w nim zachodzić (wewnętrzne – między elementami układu i zewnętrzne – z elementami otoczenia) będzie omówione w dalszej części artykułu.

Organizowanie się obywateli w celu pozyskiwania środków (lub zdobycia władzy) poprzez działania kryminalne znane jest w Polsce od wielu lat. Uważa się, że jest to jeden z negatywnych wyników przemian społeczno-ekonomicznych po 1989 r. Zjawisko to zostało określone mianem przestępczości zorganizowanej. Abstrahując od społecznych uwarunkowań, dodatkowym elementem wpływającym na powstanie tego rodzaju przestępczości jest kierowanie się potrzebą „organizowania", wyrażającą się w przygotowywaniu się do dokonania przestępstwa, a także chęcią uzyskania większych efektów negatywnych zachowań. Powodem aktywności przestępczej była i jest więc chęć wyboru takiego sposobu popełniania przestępstw, który pozwoliłby sprostać stawianym celom organizacyjnym, tj. generowaniu zysku finansowego[4].

Przedstawienie struktury i działania organizacji przestępczej jako układu cybernetycznego ma na celu głównie charakter poznawczy. Pozwala na przybliżenie

---

[1] Ze względu na ograniczenie tematyczne, artykuł nie prezentuje kompleksowego wykorzystania teorii reprezentowanych przez M. Mazura. Dotyczy to między innymi zastosowania jakościowej teorii informacji prezentowanej również przez tego autora. Przedstawienie tej teorii w odniesieniu do sterowania układami – związkami przestępczymi – ze strony organów ścigania powinno być przedmiotem odrębnej pracy. Dlatego też na potrzeby niniejszej publikacji ograniczono się wyłącznie do niezbędnego minimum.

[2] M. Mazur stworzył teorię systemów autonomicznych „autosomów" (wcześniej posługiwał się pojęciem „układów samodzielnych"). Jego teoria została opublikowana w opracowaniu *Cybernetyczna teoria układów samodzielnych* (Warszawa 1966, PWN) i rozwinięta w publikacji pt. *Cybernetyka i charakter* (Warszawa 1976, PWN). Jako przykład skonkretyzowanego układu autonomicznego uznano człowieka, którego charakterowi została poświęcona znaczna część publikacji M. Mazura.

[3] M. Mazur, *Cybernetyczna teoria*..., s. 51–55.

[4] Celem działań przestępczych może być także zdobycie i utrzymanie władzy, które koreluje z posiadaniem środków finansowych i stosowaniem pozaprawnych metod postępowania zarówno wobec członków własnej organizacji (elementów układu), jak i podmiotów pozaorganizacyjnych (elementów otoczenia).

i ocenę rozwiązań uzyskanych w innych dziedzinach nauki (w tym cybernetyki[5]) do kryminalistycznej oceny i analizy zachowań organizacyjnych występujących w obszarze przestępczości zorganizowanej. Rozwiązania te mogą być przydatne do oceny i rozpoznawania struktur zorganizowanych grup przestępczych oraz organizacji terrorystycznych, szczególnie mających bardziej tradycyjny, zhierarchizowany charakter. Przyjęte w cybernetyce oceny zachowań organizacyjnych powinny przyczynić się także do ustalania taktyki kryminalistycznej organów ścigania wobec podmiotów funkcjonujących w strukturach przestępczości zorganizowanej i strukturach terrorystycznych.

Cybernetyka określa system jako układ elementów wzajemnie ze sobą współdziałających dla osiągnięcia określonego celu. W ujęciu cybernetycznym również organizację przestępczą można potraktować jako system (układ) otwarty i wyodrębniony z otoczenia[6]. Otoczenie zakłóca działanie systemu, starając się doprowadzić do maksymalnej entropii, czyli do jego zniszczenia. Celem systemu w sensie cybernetycznym jest utrzymywanie stanu równowagi podczas wymiany z otoczeniem czynników materialnych, informacyjnych i energetycznych[7]. Systemy zamknięte w związku z brakiem wymiany wyżej wymienionych czynników z otoczeniem są bardziej narażone na zjawisko entropii i zanik. Związki przestępcze, nawet najbardziej hermetyczne, pozostają układami otwartymi, żywymi, wchodzącymi w relacje z otoczeniem. Wynika to z istoty funkcjonowania związku, który działa kosztem otoczenia, czerpiąc z niego zasilanie informacyjne i energetyczne. *W rozpatrywanym układzie – związku przestępczym (układzie przestępczym) – zachodzą procesy wymiany informacji i energii, co pozwala na jego utrzymanie w równowadze funkcjonalnej, a w konsekwencji umożliwia utrzymywanie się układowi w równowadze homeostatycznej*[8].

W społeczeństwie można wyróżnić co najmniej dwa rodzaje homeostazy – homeostazę całego społeczeństwa oraz homeostazę poszczególnych jej członków. Równowaga utrzymywana przez homeostazę społeczną może różnić się od równowagi utrzymywanej przez homeostazy poszczególnych ludzi. Inaczej mówiąc, może zachodzić sprzeczność między interesem społeczeństwa a interesem jego członków. Najbardziej istotne jest jednak rozróżnienie między homeostazą społeczną a organizacją. Aby uniknąć nieporozumień, przez organizację (przestępczą) należy tu rozumieć strukturę społeczną opartą na wydawaniu rozkazów i wymuszaniu ich wykonywania. Strukturę taką mają np. rozmaite instytucje[9], a także związki przestępcze.

---

[5] Cybernetyka jako dziedzina nauki powstała pod wpływem koncepcji związanych z konstrukcją samosterownych pocisków rakietowych, rozwoju automatyzacji i elektronicznej techniki obliczeniowej oraz prac N. Wienera. Najważniejsza w zakresie opisania zjawisk stała się analiza matematyczna, z czasem jednak zaczęto kreować tzw. niematematyczne podejście cybernetyczne i przekładać budowę systemów na zachowania społeczne. Wynikiem tego było zastosowanie cybernetyki jako myśli porządkującej w socjologii, naukach politycznych (decydowanie polityczne), psychologii i prawie (w zakresie teorii znaków i norm prawnych).

[6] Układ powiązany z otoczeniem za pomocą wejść i wyjść nazywa się układem względnie odosobnionym.

[7] Z. Biniek, *Elementy teorii systemów modelowania i symulacji*, skrypt akademicki, wyd. III internetowe, Infoplan Internet 2002, s. 6.

[8] Pojęcie homeostazy wprowadził w 1939 r. Walter Cannon, żyjący na przełomie XIX i XX stulecia amerykański psycholog i neurolog, na podstawie założeń Claude Bernarda z 1857 r. dotyczących stabilności środowiska wewnętrznego. Homeostaza jest podstawowym pojęciem w fizjologii, ale jest również stosowane w psychologii zdrowia dla określenia mechanizmu adaptacyjnego.

[9] M. Mazur, *Homeostaza społeczna*, w: *Procesy samoregulacji w oświacie. Problemy homeostazy społecznej*, M. Pęcherski, J. Tudrej (red.), Warszawa 1983, PWN, s. 107–115. Przedstawioną strukturę posiadają również organizacje zwalczające przestępczość (np. Policja, Straż Graniczna). W takim przy-

Warto także wspomnieć o konfliktach między homeostazą społeczną a organizacją, wynikających z przeciwstawności interesów. W sytuacjach konfliktowych przewaga homeostazy społecznej nad organizacją ma źródło w tym, że społeczeństwo może istnieć bez organizacji, organizacja natomiast nie może istnieć bez społeczeństwa, zawsze jest tylko dodatkiem do niej[10]. Przedmiotowe rozważania mogą się równie dobrze odnosić do związku przestępczego jako alternatywnego funkcjonowania społecznego, nie zawsze skierowanego przeciwko społeczności[11]. To stwierdzenie ma swoje uzasadnienie przede wszystkim w tym, że niejednokrotnie organizacja przestępcza działa w swoistej symbiozie ze społeczeństwem, upatrując wroga raczej w przedstawicielach władzy niż w samym społeczeństwie[12]. Homeostaza społeczna odnosi się do społeczeństwa jako całości, które ma przyjęte, określone, wzorce postępowania oraz określone (definiowalne) odchylenia od przyjętych norm postępowania. Tym odchyleniem będzie na przykład działalność zorganizowanych grup przestępczych, która ingeruje w porządek prawny dotyczący określonej społeczności jako całości[13]. Nie ma przy tym różnicy, czy działalność grup przestępczych ma charakter narodowy (krajowy, etniczny), czy międzynarodowy (ponadgraniczny). Ważne jest natomiast to, że ich działanie burzy wzorzec homeostatycznego funkcjonowania ustalony w danej społeczności. W rzeczywistości układ społeczny tak kształtuje swoje relacje, aby mieć przewagę nad taką organizacją. Wielokrotnie stwierdza się, że organizacje przestępcze istnieją dzięki społeczeństwu, czasami na jego rzecz, ale bez społeczeństwa nie mogą istnieć, gdyż funkcjonują w sposób pasożytniczy. Społeczeństwa mogłyby funkcjonować bez tego typu organizacji, ale biorąc pod uwagę obecnie występujące zagrożenia, taki społeczny wzorzec chyba długo jeszcze będzie nieosiągalny.

W zależności od różnic, do jakich może dochodzić między homeostazą społeczną a homeostazą danej organizacji można wyodrębnić pięć następujących możliwości[14]:

1) homeostaza społeczeństwa i homeostaza grupy są zgodne i ze sobą i z prawem. Oznacza to, że interes grupy jest taki sam, jak interes całego społeczeństwa, i pozostaje w granicach prawa. Jest to stan określany jako **praworządność**,
2) homeostaza społeczeństwa i homeostaza grupy są zgodne ze sobą, ale niezgodne z prawem. Oznacza to, że prawo nie odpowiada niczyim interesom (np. jest przestarzałe) i jest określane jako **prawo nieżyciowe**,
3) **homeostaza społeczeństwa jest zgodna z prawem, ale niezgodna z homeostazą grupy. Oznacza to, że grupa dąży do osiągnięcia korzyści własnych, ze szkodą dla społeczeństwa. W tym obszarze została uplasowana także grupa przestępcza**[15],

padku różnica między grupami dyspozycyjnymi a zorganizowanymi grupami przestępczymi tkwi w celu organizacyjnym, formalizowaniu zachowań, a także w samym rodzaju i usytuowaniu organizatora systemu.

[10] Tamże, s. 107–115.

[11] Zob. E.W. Pływaczewski, *Przestępczość zorganizowana*, Warszawa 2011, C.H. Beck, s. 43.

[12] Założenie to legło u podstaw między innymi powstania i funkcjonowania mafii włoskiej (sycylijskiej) w jej początkowej fazie działania.

[13] Tego typu zachowania można prześledzić na podstawie przedsięwzięć podejmowanych przez prezydenta Meksyku F. Calderona w stosunku do gangów narkotykowych.

[14] M. Mazur, *Homeostaza społeczna*…, s. 107–115.

[15] Powstanie niektórych związków o charakterze mafijnym było pozytywnie traktowane przez społeczeństwo. Przykładem może być włoska mafia czy japońska yakuza. Generalnie rzecz biorąc, powstanie takiego układu stoi jednak w sprzeczności z potrzebami społeczeństwa. Państwo jako układ społeczny w znacznie większym stopniu zapewnia i zabezpiecza potrzeby społeczne i jest odpowiedzialne za społeczeństwo jako całość niż organizacja przestępcza, która zabezpiecza jedynie potrzeby doraźne, tj. zyski finansowe.

4) homeostaza grupy jest zgodna z prawem, ale niezgodna z homeostazą społeczeństwa. Oznacza to, że grupa podporządkowała sobie prawo dla własnych korzyści. Taka grupa jest określana jako **klika rządząca**,
5) homeostaza społeczeństwa i homeostaza grupy są niezgodne ze sobą, a ponadto każda z nich jest również niezgodna z prawem. Oznacza to, że interesy grupy są niezgodne z interesem społeczeństwa, a prawo nie jest respektowane przez żadną ze stron. Taki stan jest określany jako **anarchia**.

Do przeprowadzenia dalszych rozważań należy przyjąć następujące założenia:

1) związek przestępczy będzie traktowany jako układ niezależnie od tego, jaki jest jego cel działania – popełnianie przestępstw kryminalnych, skarbowych (cel finansowy) czy przestępstw o charakterze terrorystycznym (cel ideologiczny, narodowościowy, separatystyczny czy inny)[16],
2) związek przestępczy będzie traktowany jako układ samodzielny (autonomiczny), zgodnie z teorią układów samodzielnych opracowaną przez M. Mazura.

Pod względem cybernetycznym nie wydaje się zasadne rozpatrywanie organizacji przestępczych działających przez krótki okres i o słabo zorganizowanych strukturach. Wydaje się, że każdy związek (grupę) zorganizowany (spełniający wymogi określone dla tego typu formy organizacyjnej[17]) można ocenić pod tym kątem. Działalność organizacji, niezależnie od okresu jej funkcjonowania, może świadczyć o jej zdolnościach homeostatycznych. Im dłużej jest ona zdolna przetrwać, tym zdolności te będą większe.

Cybernetyczne spojrzenie na organizacyjne formy popełniania przestępstw

Zorganizowane grupy przestępcze określane są jako: komplot, mafia, grupa, związek, gang itp. Podobnie rzecz się ma w przypadku organizacji terrorystycznych; tu stosuje się takie nazwy, jak: organizacja, związek, grupa, ugrupowanie, sieć itp. Niezależnie od przedstawionego nazewnictwa punktem wyjścia będzie to, co będzie świadczyć o zorganizowanej formie popełniania przestępstw (sposobie postępowania) i jej formy funkcjonowania (zdolności organizatorskiej budowy struktury). Drugorzędną, ale także ważną sprawą, jest w tym przypadku to, czy zachowania przestępcze są ukierunkowane na jednakowy cel działania, czy też cele zachowań przestępczych są różne (z punktu widzenia cybernetycznego istotne jest to, aby podmiot traktowany jako układ posiadł określony funkcjonalny cel działania). Cel działania zorganizowanej grupy przestępczej może rzutować na wewnętrzny układ organizacyjny (strukturę, w której kładzie się nacisk na inne obszary niż wyznaczony cel działania) i relacje z otoczeniem (poszukiwanie elementów otoczenia, z którymi układ będzie współdziałał, oddziaływał na nie czy rywalizował z nimi przy realizacji ustalonego celu działania).

Pierwszym pytaniem, jakie należałoby zadać, jest: czy zorganizowana grupa przestępcza może być traktowana jako układ samodzielny (zorganizowany)? Odpowiedź na nie wymaga jednak wcześniejszego doprecyzowania pewnych pojęć. Przede wszystkim zorganizowanej grupy przestępczej (lub związku) z punktu widzenia społecznego nie należy oceniać w kategoriach prawnych, zgodnie z art. 258 kk

[16] Zorganizowane grupy przestępcze dążą raczej do zapewnienia autonomii swoich działań w ramach homeostazy społecznej, w działaniach organizacji terrorystycznych natomiast należałoby się dopatrywać celu w postaci naruszenia funkcjonującej homeostazy społecznej.

[17] Pomocna będzie ocena zgodności odpowiednika cybernetycznego pojęcia (wzorca) układu i zachodzących relacji z udziałem elementów układu, z kwalifikacją działań członków zgodnie z art. 258 kk aktywnych przestępczo w ramach organizacyjnej struktury grupy/związku przestępczego.

penalizującym działalność tego typu struktur. Niemniej przy ścisłym traktowaniu tych pojęć zgodnie z przepisami prawa karnego, dalsza interpretacja zorganizowanej grupy przestępczej (lub związku) pozwoli na posłużenie się systematyką cybernetyczną zarówno w celu dokonania oceny zachowań tego typu struktur przestępnych, jak i przeciwdziałania ich aktywności[18].

Obecnie brakuje jednolitej definicji zorganizowanej grupy przestępczej. Może to wynikać z różnorodności tego typu grup w poszczególnych państwach oraz ich oceny przez przedstawicieli organów odpowiedzialnych za tworzenie prawa. Można jednak doszukać się cech wspólnych takich struktur w definicjach, które są już powszechnie prezentowane w literaturze przedmiotu[19]. Ponadto ważne jest takie samo rozumienie tego rodzaju form przestępczych i mechanizmów ich zwalczania przez całą społeczność międzynarodową. Cybernetyka pozwala na ogólne spojrzenie na to zjawisko, systematyzując je i porządkując na potrzeby organów ścigania uprawnionych do przeciwdziałania i zwalczania zorganizowanej przestępczości.

W polskim ustawodawstwie funkcjonują dwa pojęcia: „grupa przestępcza" i „związek przestępczy". Powszechnie uważa się, że zorganizowaną grupę przestępczą tworzą co najmniej trzy osoby, których celem jest popełnienie określonych przestępstw lub przestępstw o luźnym związku, między innymi bez określenia stałych ról poszczególnych członków, jednak z większym określeniem tych ról niż przy współsprawstwie[20]. Związek przestępczy natomiast cechuje wyższy stopień organizacji niż w przypadku zorganizowanej grupy przestępczej. Związek ten cechuje się trwałą formą organizacyjną, na jego czele stoi kierownictwo oraz narzuca określoną dyscyplinę. *Dla przyjęcia, że pewna grupa ludzi stanowi „związek", nie jest istotne, czy zachodziła w niej potrzeba stosowania rygorów organizacyjnych, lecz to, czy były one w ogóle przewidziane. Nie można stawiać znaku równości pomiędzy dobrowolnym podporządkowaniem się autorytetowi innej osoby a wynikającym z porozumienia zobowiązaniem do wypełniania jej poleceń z ustalonymi konsekwencjami odmowy ich wykonania*[21].

Ponadto samo określenie przestępstwa zawarte w art. 258 kk wskazuje na cechy charakteryzujące ten sposób popełniania przestępstw, a mianowicie:

1) *Kto bierze udział w zorganizowanej grupie albo związku* – oznacza wykreowanie i określenie podmiotów organizacyjnych przynależnych do określonej struktury, co wskazuje na utożsamianie się z nią i bycie dla niej elementem składowym,
2) (…) *mających na celu popełnienie przestępstwa lub przestępstwa skarbowego* – w tym zakresie ustalono cel powołania takiego podmiotu organizacyjnego,
3) (…) *jeżeli grupa albo związek mają charakter zbrojny albo mają na celu popełnienie przestępstwa o charakterze terrorystycznym* – w tej części przepisu wskazano na określone atrybuty, jakie mogą być przynależne podmiotowi organizacyjnemu oraz poszczególnym elementom układu,

---

[18] Właściwe wyodrębnienie układu – związków przestępczych – powinno stanowić stały proces realizacyjny w ramach działań podejmowanych przez uprawnione podmioty państwowe, głównie w obszarze czynności operacyjno-rozpoznawczych.

[19] Zob. więcej: E.W. Pływaczewski, *Przestępczość zorganizowana...*

[20] Por. wyrok Sądu Apelacyjnego w Poznaniu z 25 marca 1999 r., sygn. akt II Aka 45/99, OSA 2000, z. 2, poz. 15, *Komentarz do art. 258 kodeksu karnego* (Dz.U. z 1997 r. Nr 88, poz. 553), w: M. Budyn-Kulik, P. Kozłowska-Kalisz, M. Kulik, *Kodeks karny. Komentarz praktyczny*, Warszawa 2007, Oficyna.

[21] Wyrok Sądu Najwyższego z 27 października 1995 r., sygn. akt III KRN 122/95, „Orzecznictwo Prokuratury i Prawa" 1996, nr 5, poz. 5, wyrok Sądu Nawyższego z 23 marca 1992 r., sygn. akt II KRN 433/91, OSNKW 1992, nr 7–8, poz. 48.

4) *Kto grupę albo związek, w tym mający charakter zbrojny, zakłada lub taką grupą albo związkiem kieruje* – ustawodawca wskazał na wewnętrzną budowę, relacje zachodzące pomiędzy osobami przynależnymi do tego podmiotu organizacyjnego oraz na homeostatyczną rolę kierownictwa grupy (związku).

Przedstawione definicje przestępczości zorganizowanej (jako zjawiska społecznego) i przepisy penalizujące zachowania przestępcze, stworzone na podstawie analizy funkcjonowania zorganizowanej grupy przestępczej, pozwalają na stwierdzenie, że taką grupę będzie można traktować jako układ (system) z punktu widzenia cybernetycznego. Ponadto należy sobie zdać sprawę z tego, że penalizowanie opisanych zachowań powinno być na tyle uniwersalne, aby mogło objąć negatywne zachowania organizatorskie, niezależnie od tego, jaki wzorzec postępowania (struktury, taktyki) przyjmą członkowie związku (grupy). W takiej sytuacji wzorzec związku przestępczego pozostaje systemem abstrakcyjnym, ponieważ ma charakter nieformalny. Jego istnienie jest zależne od spełnienia wielu warunków wewnętrznych (np. świadomość członków, rytuał wejścia do związku) oraz zewnętrznych (np. postrzeganie grupy przez osoby z otoczenia, wyróżnienie przez ocenę faktyczno-prawną organów ścigania, pozostawianie charakterystycznych śladów działalności). Ponadto wyróżnienie to może być mentalne (intelektualna więź z organizacją i chęć przynależności do niej) oraz fizyczne (charakterystyczny strój, okaleczenie, tatuaż itp.), co będzie się odnosiło do zachowań członków grupy (związku). Związek taki będzie spełniał funkcje układu, kiedy będzie on, ze względu na realizowany cel, wyodrębniony spośród innych układów i z samego otoczenia. Wydaje się, że wyodrębnienie nie będzie dotyczyło wyłącznie kwestii istnienia jako struktura przestępcza (można wskazać wiele takich bytów w kraju i poza jego granicami). O wyodrębnieniu układu – związku przestępczego – będzie decydowało wykreowanie się tej, a nie innej grupy członków, zbudowanie pomiędzy nimi relacji oraz pomnażanie zdobytych w sposób przestępny środków finansowych i przeznaczanie ich dla konkretnych członków grupy. Trudno określić, która z tych cech powinna być dominująca w odniesieniu do utrzymania układu w równowadze homeostatycznej. Niekoniecznie także w związkach przestępczych wystąpi potrzeba budowania wyższej formy organizatorskiej dla realizacji przyjętego celu. W rozumieniu homeostatu zgodne z równowagą całości związku może być dojście do określonego poziomu zamożności elementów i zaprzestanie działania w określonym momencie, co może doprowadzić do świadomego ustania „życia" układu i wchłonięcia go przez otoczenie.

Aby mówić o systemie, należy wcześniej podać określenie „układu". Otaczający nas świat składa się z niezliczonej liczby wpływających na siebie elementów. Do oddziaływania, zwanego inaczej interakcją, dochodzi na różnych płaszczyznach, w różnym czasie i różnej przestrzeni. Dlatego też można wyróżnić takie związki, które wzajemnie oddziałują na siebie bardziej niż na inne elementy spoza grupy (pozostałe to elementy otoczenia)[22]. Oprócz pojęcia „układu" istnieje także pojęcie „systemu", również definiowane w różny sposób. System to celowo określony zbiór elementów oraz relacji zachodzących między tymi elementami i między ich właściwościami[23]. Za właściwości systemu uznaje się cechy poszczególnych obiektów, relacje natomiast to stosunki wiążące poszczególne części z całością. System rozpatruje się według właściwości. System w przeciwieństwie do układów może być nie tylko obiektem konkretnym (realnym, rzeczywistym), ale także

[22] S. Mynarski, *Elementy teorii systemów i cybernetyki*, Warszawa 1979, PWN, s. 7–8.

[23] Tamże, s. 12.

abstrakcyjnym[24]. Tak jak system składa się z elementów i ich właściwości, tak otoczenie takiego systemu jest zbiorem elementów i właściwości, na których zachowanie będzie można oddziaływać poprzez wysyłanie bodźców oraz podejmowanie reakcji. W rzeczywistości układ – związek przestępczy – jest bytem abstrakcyjnym, skonkretyzowanym w świadomości jego członków zarówno w sensie mentalnym, jak i wykonywanych działań (mechanizmów postępowania). Oczekuje się od niego skuteczniejszego postępowania, zapewnienia instrumentów potrzebnych do działań przestępczych.

Przy takim rozumowaniu należy ocenić, co będzie stanowiło system (nadsystem) w odniesieniu do poszczególnego układu przestępczego. Jeśli chodzi o przestępczość, to raczej trudno mówić o nadsystemie. Bardziej prawidłowe jest wskazanie, że poszczególny związek przestępczy jest systemem przestępczym, składającym się z poszczególnych układów i pojedynczych elementów. W strukturze organizacji terrorystycznych można doszukiwać się pewnego nadsystemu wobec pomniejszych systemów walki islamistycznej, działających niezależnie, jednak w ramach dżihadu ogólnoświatowego. Właściwością układu jako związku przestępczego jest zdolność do grupowego organizowania czynów penalizowanych w celu osiągania zysków finansowych (bądź uzyskania władzy). Tym samym, jeżeli dokonywanie przestępstw będzie realizowane indywidualnie, w sposób niezorganizowany, przy luźnych więzach pomiędzy poszczególnymi sprawcami, to nie będzie można mówić o zorganizowaniu układu. Grupa, o której mowa w art. 258 § 1 kk, nie wymaga „specjalnej wewnętrznej struktury". Nie ulega wątpliwości, że „zorganizowanie" oznacza w języku polskim ułożenie czegoś w pewne formy, podporządkowanie regułom, normom, wprowadzenie do czegoś ładu i organizacji[25].

Przy posługiwaniu się pojęciem „system" w przypadku funkcjonowania omawianych struktur, pomocna staje się tzw. metoda systemowa. Metoda ta jest użyteczna, niemniej jednak wymaga przestrzegania następujących rygorów (reguł):

- **Ścisłość**. System powinien być ściśle określony, żeby było wiadomo, co do niego należy. Określenie systemu może być dość ogólne, ale nie może być ogólnikowe.
- **Niezmienność**. Określenie systemu powinno być niezmienne w całym toku rozważań. Jest niedopuszczalne, żeby jakieś elementy systemu były czasem traktowane jako należące do systemu, a czasem jako będące poza nim.
- **Rozłączność**. Systemy powinny być rozłączne, tj. nie może być elementów należących do kilku systemów na raz. Przynależność elementów do jednego systemu musi więc być równoznaczna z tym, że na pewno nie należą one do żadnego innego systemu.
- **Zupełność**. Ujęcie systemu powinno być zupełne, tj. powinno obejmować wszystkie elementy systemu, a nie jedynie niektóre z nich. Podział systemu na podsystemy powinien być zupełny, to znaczy system nie może zawierać elementów nienależących do żadnego z jego podsystemów.
- **Funkcjonalność**. Systemy powinny być wyodrębniane ze względu na pełnione funkcje, a nie ze względu na oddzielność przestrzenną[26].

---

[24] Wydaje się, że możliwe jest także występowanie związku przestępczego jako abstrakcji. Do takich sytuacji może dochodzić, gdy władza, motywując potrzebę utrzymania homeostazy społecznej, przedstawia wzmocnienie w tym zakresie swoich działań jako walkę z nieistniejącym, a „sztucznie" wykreowanym wrogiem, którym mogą być np. związki przestępcze.

[25] Wyrok Sądu Apelacyjnego w Katowicach z dnia 16 lipca 2009 r., sygn. akt II AKa 150/09.

[26] M. Mazur, *Pojęcie systemu i rygory jego stosowania,* w: Materiały Szkoły Podstaw Inżynierii Systemów nr 2, przedruk w „Postępach Cybernetyki" 1987, z. 2, s. 21–29 – numer w całości poświęcony

Przykładem wyodrębnienia stosowanego w związkach przestępczych mogą być chińskie triady. Człowiek o białym kolorze skóry nie może zostać członkiem tej organizacji. Ponadto kandydat na członka triady musi mieć odpowiednie rekomendacje. Zanim zostanie szeregowym członkiem mafii, musi przejść trzyletni okres próbny jako tzw. czeladnik. W przypadku popełnienia przez niego błędu – zostaje zgładzony. W celu zwiększenia kamuflażu członkowie triad używają liczb, które są szyframi. Każda liczba oznacza inny poziom organizacji i zaczyna się od cyfry 4, uważanej za szczęśliwą[27]. W takim przypadku jest zapewniona niezmienność i rozłączność każdej struktury. Można zauważyć, że w przypadku prezentowanej metody systemowej ścisłość odnosi się do opisania układu jako całości, co może nastąpić przez zastosowanie wielu kryteriów: oceny zachowań elementów, zewnętrznych znaków, inicjacji, kierunków aktywności organizatora w opisaniu układu itp. Przynależność do grupy przestępczej nie może być decyzją jednostronną. Żeby danej osobie przypisać czyn z art. 258 kk, niezbędne jest wykazanie nie tylko tego, że miała ona świadomość istnienia grupy przestępczej i zamiar działania w jej ramach, lecz także, że jako jej członek została zaakceptowana przez pozostałe osoby tworzące tę grupę, a co najmniej te, które mogły decydować o jej składzie osobowym[28].

Pewnym utrudnieniem może być to, że związki przestępcze są organizacjami nieformalnymi (nierejestrowanymi). Stąd też reguły wyodrębnienia układu (systemu) z otoczenia są określane przez samego organizatora (występującego jako pojedynczy element lub zespół elementów)[29].

Wskazuje się, że granica między systemem a otoczeniem jest granicą sztuczną[30]. Zewnętrzny obserwator może ewentualnie ocenić, co należy do systemu, a co pozostaje w jego otoczeniu. Z punktu widzenia związku przestępczego wyznaczniki go klasyfikujące definiowane przez organizatora znajdują się w samym systemie (wewnętrzne) i w założeniu mają zmierzać do uzyskania optymalnej efektywności systemu. Związane z tym jest to, „kogo chce widzieć" organizator w systemie i kto z wybranych zapewni sprawność funkcjonalną tego systemu. Oprócz wyznaczników wewnętrznych wyróżnia się wyznaczniki zewnętrzne, którymi są organy ścigania, otoczenie członków związku przestępczego, media itp.

Z punktu widzenia związku przestępczego ważne jest spełnienie wymogów niezmienności, rozłączności i zupełności. Niezmienność pozwala na zachowanie bezpieczeństwa, kontrolę wewnętrzną elementów systemu, kreowanie lojalności w działalności przestępczej. Wymóg ten jest również związany z zadaniowaniem członków czy podziałem zysku przestępczego wewnątrz organizacji. Podobnie rzecz się ma z wymogiem rozłączności, której należałoby się dopatrywać głównie

Marianowi Mazurowi, Orzysz, Komitet Budowy Maszyn PAN.

[27] R. Radzik, *Syndykaty zbrodni*, „Tygodnik Solidarność" 1998, nr 34, s. 7, w: K. Laskowska, *Azjatyckie zorganizowane grupy przestępcze*, „Prokuratura i Prawo" 2004, nr 7/8, s. 161.

[28] Wyrok Sądu Apelacyjnego w Lublinie z dnia 13 listopada 2008 r., sygn. akt II AKa 166/08.

[29] Szef klanu w terminologii triad nosi również nazwę Głowa Smoka lub funkcjonuje jako liczba 489. Zob. K. Laskowska, *Azjatyckie zorganizowane grupy…*, s. 161. Przykładem innego rodzaju kierowania jest „grupa pruszkowska", aktywna w latach 90. na terenie Polski. Członkowie gangu nazywali tę grupę „spółdzielnią", ponieważ mafia pruszkowska nigdy nie miała jednego szefa. Działaniami grupy kierował tzw. zarząd, nazywany czasem kolegium. Każdy z członków zarządu miał własną grupę, własne wojsko, prowadził własne interesy, ale poważniejsze decyzje wszyscy członkowie „zarządu" podejmowali wspólnie. Zdaniem jednego z funkcjonariuszy CBŚ KGP *kasa też szła do jednego worka*. Zob. W. Krasnowska, *Holding Pruszków*, „Wprost" 2000, nr 36.

[30] Z. Biniek, *Elementy teorii systemów…*, s. 7– 8.

w lojalności członków nie tylko wobec przywództwa, ale także wobec samego układu (jako organizacji) i identyfikowaniu się z nim[31]. Jego spełnienie pozwala na zapewnienie „szczelności" związku przestępczego. Spełnienie wymogu zupełności wyzwala u kierownictwa grupy pragmatyzm, zwłaszcza potrzebę odpowiedniego doboru jej członków, ale i odpowiedzialność organizatora za działania członków grupy. Należy jednak zauważyć, że obecnie funkcjonujące systemy, zwłaszcza sieci terrorystyczne, działają mimo nie zawsze spełnionego wymogu zupełności. Wydaje się, że utrzymanie reguły zupełności ogranicza organizacyjnie aktywność grup przestępczych. Bardziej więc ten wymóg odnosi się do tradycyjnego ujęcia związku przestępczego niż do jego współczesnych odpowiedników.

Wymóg funkcjonalności jest związany z aktywnością samego układu i sprawdzalnością cechy funkcjonalności przyjętego wzorca organizacyjnego. Wiąże się z nim także rodzaj konstrukcji wprowadzony dla związku przestępczego. W jego założeniu tkwi głównie element sprawdzalności realizacji celu, zapewnienie sterowalności systemu (głównie przy dużej jego rozpiętości) oraz uzyskanie ciągłości funkcjonowania układu. Tym samym niezapewnienie funkcjonalności systemu, może być powodem zmiany schematu wewnętrznego związku przestępczego przez organizatora (np. zmiany przywództwa średniego szczebla zarządzania).

Pracownicy organów ścigania mogą przy zastosowaniu metody systemowej porównywać zachowania organizacji, typować między nimi związki, podobieństwa, budować schematy decyzyjności wśród wewnętrznych elementów układu (np. w ramach wstępnego porządkowania materiałów przed przygotowaniem ich do profesjonalnej analizy kryminalnej bądź obrania sposobu prowadzenia sprawy operacyjnej czy procesowej).

Podsumowując, wyodrębniona w układ struktura przestępcza powinna charakteryzować się następującymi cechami:

– powinna działać w zespole trzech lub więcej elementów (liczbowe wyodrębnienie elementów układu),
– każdy z elementów układu powinien mieć świadomość przynależności do organizacji (wyodrębnienie mentalne elementów układu),
– relacje między elementami organizacji powinny służyć osiągnięciu ustalonego celu działania, któremu powinna być podporządkowana aktywność poszczególnych elementów (ustalone relacje wewnątrzukładowe i samosprzężenia, a także zapewnienie sprawności przepływów informacyjnych i energetycznych),
– oddziaływanie na elementy otoczenia powinno służyć realizacji celu układu, a w ostateczności jego przetrwaniu (sprzężenie z elementami otoczenia),
– świadomość członków układu powinna dotyczyć także tego, że w organizacji można zrobić więcej razem niż pojedynczo (całość to więcej niż suma wszystkich części[32]),
– w świadomości członków powinna być zdolność do przetrwania (homeostazy).

Tym samym przedstawione założenia prezentują określony i przyjęty wzorzec złożonego układu przestępczego podlegającego dalszej analizie. Z pewnością można także przyjmować jakieś pozostające na dwóch biegunach skrajne odwzorowania (z jednej – model struktury hierarchicznej, z drugiej – model struktury przestępczej) oraz wzorzec pośredni (model multistrukturalny) mający cechy dwóch skrajnych

[31] Szczególnie ważne może być spełnienie tego warunku w przypadku rywalizacji układów przestępczych na danym terytorium czy na danym obszarze przestępczym.

[32] Autorem tego stwierdzenia jest Arystoteles (384–322 p.n.e.).

odwzorowań[33]. Ponadto uniwersalizm w kształtowaniu wzorców modeli związków przestępczych pozwala na przyjęcie podstawowych założeń dotyczących ich budowy. Są to występujące łącznie wyznaczniki:

1) zorganizowana, wielopodmiotowa i wyodrębniona (intelektualnie i fizycznie), abstrakcyjna struktura podmiotowa,
2) struktura powiązana relacjami dostosowanymi do optymalnego funkcjonalnego utrzymania się w czasie[34],
3) struktura przyjmująca, poprzez przepływy energetyczne i informacyjne, realizację celu w sposób przestępny.

Tym samym poszczególne modele związków stają się odwzorowaniem dotychczas istniejących bądź też są nowym bytem przestępczym o nieznanej poprzednio strukturze. Na tworzenie nowych modeli decydujący wpływ będzie miała szczególnie zmiana struktury społecznej i aktywności społeczeństwa, na której dany model będzie się odwzorowywał. Biorąc pod uwagę popełnianie przestępstw, możemy wyróżnić układy samodzielne i niesamodzielne.

Mając wyodrębnione konstytutywne cechy układu przestępczego jako systemu, będzie można podjąć działania analityczne, przyjmując za punkt wyjścia strukturę systemu lub jego zachowanie (poprzez ocenę relacji wewnątrzukładowych i z elementami otoczenia). Postępowanie polegające na poszukiwaniu zachowania się systemu na podstawie znajomości jego struktury nosi nazwę analizy systemu. Postępowanie polegające na znajdowaniu struktury systemu na podstawie znajomości jego zachowania natomiast nosi nazwę syntezy systemu.

ANALIZA

badanie **struktury** systemu → uzyskanie informacji o **zachowaniu** się systemu

W wyniku analizy powinno się uzyskać rozwiązanie jednoznaczne, ponieważ bada się dany, określony, system, a badanie powinno dać informacje o zachowaniu występującym i przynależnym temu danemu systemowi.

[33] Stąd też można mówić raczej o odwzorowaniu w związku przestępczym modelu struktury przedsiębiorstwa niż o „przedsiębiorstwie przestępczym". Pojęcie to występuje u D.C. Smitha, *Some Things That May Be Important To Understand About Organized Crime Than Cosa Nostra*, „University of Florida Law Review" 1971, nr 1, s. 6 oraz u M. Leviego, w: *The Organisation of Serious Crimes*, Oxford 2002, Oxford University Press, s. 880–881, za: W. Filipkowski, *Przestępczość zorganizowana – ujęcie prawne i kryminologiczne*, „Prokuratura i Prawo" 2006, nr 12, s. 61.

[34] Uwzględnia zbudowanie związku przestępczego „od początku", na podstawie już funkcjonującej struktury przestępczej lub formalnie działających podmiotów (np. banku, fundacji czy firmy).

SYNTEZA

badanie **zachowań** sytemu → uzyskanie informacji o **strukturze** systemu[35]

W rozważaniach na temat struktury przestępczości zorganizowanej oprócz omówienia problemu dotyczącego tradycyjnego zhierarchizowanego związku porusza się także problem struktury sieciowej. We współczesnym świecie można wyróżnić powstałe niedawno struktury społeczne, głównie o charakterze sieciowym, które kreują określone zachowania. W tym zakresie wyróżnimy:

1) luźne układy sieciowe (wolne struktury sieciowe) – na przykład ruch ACTA – aktualnie określany jako najbardziej nieprzewidywalny, a więc i groźny (np. w związku z możliwością przeprowadzania nieskoordynowanych cyberataków sprowadzających się do wielości reakcji w stosunku do pojedynczych bodźców). Nie można go jednak określić jako układ samodzielny. Aktywizuje się on od czasu do czasu i nie ma skonkretyzowanej struktury; jego członkowie nie dążą do utrzymania się przez dłuższy czas (aktywizuje ich raczej luźno określony cel), a relacje pomiędzy nimi nie są na tyle trwałe, żeby tworzyć określoną strukturę. Układy te są budowane poprzez gromadzenie się wokół określonej idei, ale bez brania odpowiedzialności i uznawania potrzeby formalizowania struktury. Satysfakcję osiąga się tu raczej poprzez wykreowanie organizacyjnej zgodności myśli niż zgodności potrzeby budowania organizacji.
2) organizacyjne układy sieciowe, charakterystyczne najczęściej dla organizacji terrorystycznych (również wtedy, gdy organizacje terrorystyczne odstępują od celu politycznego, przekształcając go w cel typowo kryminalny dla osiągnięcia zysku z działalności przestępczej, czy też dla stworzenia mechanizmów globalizacyjnych (w ekonomii czy działaniach społecznych) oraz funkcjonowania urządzeń (np. w teleinformatyce).

Ponadto należy zwrócić uwagę na możliwość wykorzystania sieci do popełniania przestępstw (np. cyberprzestępstw, w tym oszustw finansowych) przez podmiot indywidualny. Wydaje się, że główną rolę odgrywa organizator, który powinien przesądzić, czy działanie w celu pozyskiwania środków w wyniku popełniania przestępstw ma być realizowane w ramach systemu, czy nie. W przypadku założenia, że cel będzie realizowany w ramach systemu, organizator buduje go zgodnie z regułą (założeniem) charakterystyczną dla budowy systemu (tj. zgodnie z prezentowaną metodą systemową). Dodatkowo należy wskazać na to, że pojęcie systemu może odnosić się do skonkretyzowanej grupy czy związku, czyli bytu funkcjonującego, ale system taki może być pojmowany także znacznie szerzej i bardziej abstrakcyjnie jako sposób na realizację celu niekoniecznie lub nie tylko opartego na konstytutywnych regułach założeń odnośnie do budowy organizacji przestępczej.

W takim przypadku możliwe są dwa rozwiązania:

1) układ jest układem samodzielnym, tj. dąży do samosterowności poprzez przeorganizowanie struktury (np. z hierarchicznej w sieciową), zdecydowanie ograniczając relacje pomiędzy wewnętrznym organizatorem a poszczególnymi podukładami (elementami). Jako wewnętrzny organizator pozostawia sobie jednak wpływ na poszczególne podukłady (minimalizując relacje bezpośrednie), które uzyskują

[35] S. Mynarski, *Elementy teorii systemów...*, s. 16–17

zwiększoną samodzielność do samosterowania się i przeciwdziałania bodźcom mogącym ograniczać ich samosterowność[36] (struktura sieciowa układu);

2) w drugim przypadku wydaje się, że ma się do czynienia z jakimś układem i obok niego z równolegle działającymi innymi układami (nie podukładami), które w zgodności realizują określony (nadrzędny) cel działania. Jego realizacja odbywa się poprzez silne więzi (relacje) międzyukładowe (np. ideologiczne, religijne), a nie wewnątrzukładowe (hierarchiczne, wynikające z podporządkowania sobie poszczególnych elementów). Mamy wtedy do czynienia z siecią układów, czyli wielością układów organizującą się w celu zwielokrotniania zamierzonego celu działania. W takim przypadku poszczególne układy wchodzą w skład nadukładu umożliwiającego podniesienie możliwości optymalizacyjnych funkcjonowania. Innym rozwiązaniem jest oddziaływanie układów silniejszych (faza wzrostowa) wobec innych, słabszych i będących w fazie schyłkowej swojego istnienia (osłabienie relacji, nieskuteczność homeostatu, brak zdolności do samosterowności itp.). Relacje są na tyle luźne (ale nie dowolne), że pozwalają na realizację funkcjonalną ustalonego celu. Uznają hierarchiczność (nadrzędność) celu, a nie przywództwa organizacyjnego.

Jedną z istotnych prac dotyczących cybernetyki, jaką przedstawił M. Mazur, jest cybernetyczna teoria układów samodzielnych[37] (autonomów). Autonom to w cybernetyce system mający zdolność sterowania się i zdolność przeciwdziałania utracie zdolności sterowania się. Aby spełnić te dwa warunki istotne z punktu widzenia funkcjonowania autonomu, musi on zawierać (jako podsystemy) odpowiednio powiązane następujące organy: receptory, efektory, korelator, alimentator, akumulator i homeostat. Ograniczenie w takim stanie działania jednego z elementów ma wpływ na pozostałe, z czym mogą się wiązać pewne zakłócenia w układzie (które mogą doprowadzić do stanu odchylenia niezgodnego z przyjętą normą). Rozpatrując działanie poszczególnych wymienionych elementów i spełniane przez nie funkcje w układzie przestępczym, należy mieć na uwadze to, że niejednokrotnie poszczególni członkowie tych grup traktowani jako elementy układu mogą zachowywać postawę bierną, mając jednocześnie świadomość przynależności do układu. Przypisując przynależność elementu do grupy, wystarczające jest stwierdzenie, że sprawca przystąpił do grupy ze świadomością jej celu i form działania, gotowy poddać się panującej w grupie dyscyplinie i wziąć udział w jej działalności. Do wypełnienia znamion przynależności wystarczające jest samo stwierdzenie (świadomość) tej przynależności, nawet bez konieczności wykazania popełnienia w ramach tej grupy jakichkolwiek czynów zabronionych. Dla odpowiedzialności karnej nie robi różnicy, czy udział w grupie jest czynny, czy bierny[38]. Wydaje się jednak, że wskazane przez M. Mazura elementy wymagają postawy czynnej dla zachowania stałości układu. Stąd też układ przestępczy z pewnością będzie bardziej skomplikowanym tworem, który może pozwolić sobie na postawę bierną w układzie.

[36] Wydaje się, że w takim przypadku muszą powstawać inne mechanizmy obronne niż w układach zhierachizowanych. Na pewnym etapie główny homeostat musi posiadać wiedzę (informację) co do zakłóceń, oceniając, czy w sposób niebezpieczny nie została naruszona równowaga funkcjonalna. W innym przypadku układ traktowany jako całość, przynajmniej przez homeostat, może się rozpaść. Na przykład poprzez utratę zdolności do samosterowności większej liczby podukładów czy też poprzez wykorzystanie zbyt luźnych relacji poszczególne podukłady zaczynają żyć własnym życiem i stają się samodzielnymi układami odpowiedzialnymi, już niezależnie od głównego układu, za swoją samosterowność.

[37] M. Mazur, *Cybernetyczna teoria układów...*

[38] Wyrok z dnia 26 listopada 2008 r., wydany przez Sąd Apelacyjny w Krakowie, sygn. akt II AKa 168/08.

Postawa ta może dotyczyć innych form postępowania niż czynne, np. doradztwa, akceptacji decyzji itp. Bierne funkcjonowanie elementu nie oznacza, że jest zbędny, ale że jest on elementem niewykorzystywanym na każdym etapie aktywności układu. Na pasywność w układzie nie pozwala konieczność reagowania na bodźce z otoczenia oraz potrzeba oddziaływania wyjściowego wobec elementów otoczenia. Przy biernej postawie układ wykorzystuje potencjał, który dotychczas zgromadził bez zapewnienia sobie uzupełnienia energetycznego i informacyjnego, a tym samym swoim działaniem dąży do ustania układu.

Szczegółowa struktura organizacyjna związku przestępczego jako układu samodzielnego (autonomicznego)

Określając strukturę organizacyjną systemu uwzględnia się następujące jego elementy: receptory, korelator, akumulator, efektor i organizatora.

1. Receptor

Zarówno receptor, jak i efektor są elementami sterowniczymi w ramach układu. Receptor jest odpowiedzialny za wykrywanie bodźców, efektor zaś jest wykorzystywany przez układ do wytwarzania reakcji. Układ może posiadać zarówno wiele receptorów, jak i efektorów. Do wykrycia określonego oddziaływania jest potrzebny receptor wrażliwy na takie właśnie oddziaływanie. Im więcej jest receptorów wrażliwych na określone bodźce, tym więcej informacji dopływa do systemu autonomicznego[39]. Wydaje się, że „wrażliwość" jest związana z wyróżnianiem zachowań elementów otoczenia sprzyjających popełnianiu przestępstw (np. obnoszenie się z bogactwem, otwarcie nowej restauracji, poruszanie się samochodem, na który jest tzw. zamówienie itp.). W rozpoznawanym układzie związek przestępczy ma u podstaw największą liczbę takich elementów. Sama więc struktura i jej skuteczność wyzwalają potrzebę posiadania proporcjonalnie większej liczby receptorów i efektorów w odniesieniu do liczby elementów zarządczych i organizatora. W zakresie działania receptora jest pozyskiwanie z otoczenia (eksteroceptory) bodźców, na które układ będzie musiał w określony sposób zareagować. Dla bezpieczeństwa samego układu i stosowanych reakcji poszczególne bodźce możemy podzielić na:

a) inicjatywne – są to bodźce nowe, wyzwalające w układzie potrzebę przestępczego zareagowania. Przykładem takiego bodźca będzie powstanie nowej dyskoteki, z której może być pobierany haracz za tzw. ochronę,
b) stabilizacyjne – to bodźce znane, które w wyniku zaistnienia pozwalają na automatyczne wykonywanie czynności przez efektory układu. Można do nich zaliczyć systematyczne dystrybuowanie narkotyków i pobieranie w zamian pieniędzy,
c) zagrożeniowe – związane z planowanymi i realizowanymi działaniami ze strony organów ścigania. Przykładem może być tu uprzedzenie grupy przez funkcjonariusza współdziałającego z nią o planowanych zatrzymaniach,
d) obojętne – które nie wymagają reakcji ze strony układu. Są one obojętne z punktu widzenia realizowania celu układu i samemu układowi nie zagrażają (np. aresztowanie we Włoszech bossa mafii, z którą układ nie realizował wspólnych interesów przestępczych ani nie planuje przejęcia interesów aresztowanego).

[39] M Mazur, *Cybernetyka i charakter...*, s. 164.

Mimo, że receptorów można się doszukiwać przede wszystkim na poziomie wykonawczym, to z zachowaniem przynależnym receptorom można mieć do czynienia w przypadku każdego członka związku przestępczego. Wynika to przede wszystkim z relacji z otoczeniem, w tym z podobnymi układami. Przykładem jest np. sytuacja, gdy przywódcy dwóch związków chcą się ze sobą porozumieć co do zorganizowania przemytu znacznej ilości narkotyków. Rozmowy i ustalenia na ten temat nie będą prowadzone na poziomie wykonawczym, tylko na poziomie organizatora układu. Bodźcem będzie chęć podjęcia współpracy, zasygnalizowana w określony sposób. Jest oczywiste, że przeprowadzanie dalszych czynności w tym zakresie, dotyczących przygotowania takiego zorganizowanego przestępstwa, będzie należało do niższego szczebla członków związku. Organizator jednak może zastrzec sobie otrzymywanie przez korelator określonych informacji (bodźców) i dalsze współdziałanie na przyjętym poziomie zarządzania. Inaczej będzie z efektorem, co oznacza, że ze względu na różne czynniki, w tym bezpieczeństwo osobiste (niewiązanie organizatora z przestępstwem), jak również prestiż w samym układzie, efektorem będą elementy najniższego szczebla hierarchii przestępczej.

Ponadto w niektórych przypadkach receptor może być tożsamy z efektorem. Może to mieć miejsce wtedy, gdy receptor w wyniku przejęcia informacji od bodźca będzie jednocześnie wykonawcą reakcji na ten bodziec. Przykładem może być tu uzyskanie przez konkretnego członka organizacji wiadomości o uruchomieniu lokalu z dyskoteką, w którym nie ma „ochrony", a jednocześnie fizyczne przybycie przez tego członka na polecenie zwierzchnika związku do tego lokalu i wyegzekwowanie od właściciela środków finansowych za wymuszoną „ochronę".

Należy zauważyć, że M. Mazur wyróżnił także receptory wykrywające bodźce wewnętrzne, tj. pochodzące z różnych miejsc samego układu samodzielnego[40] (interoceptory). To dość ważne receptory; należy domniemywać, że takimi receptorami będą członkowie grupy przestępczej, którzy będą odpowiedzialni za pozyskiwanie bodźców powodujących nierównowagę funkcjonalną układu. Dotyczy to tych członków grupy, którzy mogą podjąć lub też podjęli współpracę z organami ścigania, a także wprowadzonych do grupy przestępczej funkcjonariuszy policji działających pod przykryciem, członków okradających z zysków organizację przestępczą (zatrzymujących większą część zysku niż należną w wyniku podziału), współpracujących z innymi grupami przestępczymi lub dokonujących przestępstw na własną rękę. Występowanie tego rodzaju receptorów będzie związane z zapewnieniem wewnętrznej dyscypliny i regulacji zachowań zmierzających do naruszenia równowagi układu.

2. Korelator

Korelator to organ układu, który ma za zadanie zapewnić przetwarzanie i przechowywanie informacji. W rzeczywistości funkcję korelatora będą pełniły osoby, które jako członkowie związku przestępczego będą uczestniczyć na określonych etapach w procesie decyzyjnym. Nie można także wykluczyć, że grupa w celu gromadzenia wiedzy czy planowania przestępczych aktów może posługiwać się urządzeniami technicznymi. Takie postępowanie jednak może być dla niej niebezpieczne i związane z tym, że wiedza ta może być pozyskana przez przedstawicieli organów ścigania chociażby w wyniku przeszukania. Znane są jednak przypadki prowadzenia rozliczeń na podstawie zapisków w notesach prowadzonych przez poszczególnych członków grupy

[40] M. Mazur, *Cybernetyczna teoria układów...*, s. 71.

przestępczej. Dane takie dotyczyły osób, od których egzekwowano haracz, czy którym wręczano korzyści majątkowe[41]. Przy aktualnym stanie techniki prawdopodobnym środkiem technicznym służącym do kumulowania informacji będzie komputer stacjonarny lub laptop (notebook) albo inne urządzenie techniczne (np. telefon komórkowy). Z pewnością skumulowane tu informacje będą w jakiś sposób zabezpieczone przez zagrożeniem (chociażby przed nagłym nieprzewidzianym przeszukaniem) różnego rodzaju kodami dostępu czy przez automatyczne zniszczenie danych. Ponadto sam zapis będzie mógł być kodowany. Największym atutem pozostanie jednak wiedza uzyskana przez poszczególnych członków związku przestępczego. Wiedza kumulowana w korelatorze będzie odnosiła się do dwóch kwestii. Pierwsza z nich będzie dotyczyć tych informacji, które będą potrzebne w związku z organizowaniem działalności przestępczej oraz przygotowywaniem i dokonywaniem konkretnych przestępstw (pozyskiwania informacji)[42]. Będzie ona związana z wykonywaniem funkcji układu i samosterowania się. Druga będzie się odnosiła do eliminacji czynników przeciwdziałających samosterowaniu się oraz pozyskiwaniu i gromadzeniu informacji świadczących o bodźcach mogących zagrozić równowadze funkcjonalnej układu. Ta wiedza będzie potrzebna do zorganizowania przeciwdziałania (wyeliminowanie członka grupy, zastosowanie kontrobserwacji, zniszczenie fantów, przygotowanie miejsc ukrywania się przed organami ścigania itp.), czyli przygotowania określonej reakcji. Rola korelatora będzie również istotna z punktu widzenia uzyskania optymalnej decyzji w celu wytworzenia (ustalenia) właściwego bodźca oddziałującego na elementy otoczenia. Wiedza (informacja) zsynchronizowana z kanałem energetycznym będzie wyzwalać decyzje organizatora co do zapewniania funkcjonalności układu i realizacji ustalonego celu (np. zgromadzenia odpowiednich narzędzi do popełnienia przestępstwa, ustalenia taktyki działania, wyznaczania stanu początkowego do realizowania przestępstwa).

3. Alimentator

Alimentator jest odpowiedzialny za pobieranie energii z otoczenia. Wraz z receptorami i efektorami zapewnia styczność systemu autonomicznego z otoczeniem. W strukturze systemu jest on uplasowany jako wejście systemu[43]. Alimentator uczestniczy w przebiegach energetycznych w układzie samodzielnym. Można go przyrównać do członka zorganizowanej grupy przestępczej odpowiedzialnego za pobieranie haraczu od opłacających się grupie elementów otoczenia (np. restauratorów, za możliwość prowadzenia działalności gospodarczej czy za tzw. ochronę miejsca wykonywania tej działalności). To także podmiot, który w imieniu układu zapewnia dopływ środków finansowych, np. z dystrybucji narkotyków rozprowadzanych przez dealerów, i stwarza mechanizmy pobierania energii z otoczenia (zakłada konta, skrytki bankowe, kontroluje wpływy z ustalonych źródeł finansowania grupy, odpowiada za odbiór gotówki z rynku dealerów narkotykowych). Alimentator nie jest w stanie pobierać energii z otoczenia, kiedy nie ma jej w pobliżu czy zasięgu układu. Dlatego też w samym układzie jako element wewnętrzny wprowadzono akumulator pozwalający na gromadzenie energii. Stąd też od sprawności alimentatora i jego skuteczności zależy, czy grupa będzie

[41] Przykładem może być notes Wiesława N., ps. „Wariat", jednego z przywódców gangu wołomińskiego, zabezpieczony przez organy ścigania w jego samochodzie.

[42] Zgromadzenie informacji o przeciwniku, ocena skali zagrożenia, przyjęcie rozwiązań alternatywnych itp.

[43] M. Mazur, *Cybernetyka i charakter...*, s. 163–164.

„konsumowała" poprzednio zgromadzone środki, czy też zdobywała je na bieżąco. Dodatkowo, gdy sam alimentator jest przeszkodą w zapewnieniu stałego dopływu środków dla organizatora, zauważa sie spadek zasilenia i potrzebę uruchomienia środków już skumulowanych. Do takiej sytuacji może dojść wtedy, gdy alimentator jest elementem o niewielkiej sprawności lub też oszukuje grupę, jeśli chodzi o dostarczane zasilenie energetyczne, tj. energia nie jest kumulowana w akumulatorze, tylko wyprowadzana na zewnątrz, a tym samym następuje zakłócenie w torze energetycznym. Ten rodzaj zakłócenia może doprowadzić do ograniczenia samosterowalności systemu, a w konsekwencji do osłabienia mocy decyzyjnej. Rola alimentatora jest szczególnie ważna, ponieważ jego działanie jest niejako emanacją decyzyjności organizatora i działań efektorów układu. Brak sprawdzalności tych decyzji przekłada się na niewystarczające zasilanie energetyczne układu przestępczego. Wiedząc, że układ ten opiera się przede wszystkim na pomnażaniu zysków przestępczych, poprzez nieefektywność alimentatora zostaje zakłócony cel funkcjonalny całości układu.

4. Akumulator

Akumulator to organ zapewniający przetwarzanie i przechowywanie energii w celu jej wykorzystania, w odpowiednim czasie i w zależności od potrzeb[44]. Akumulator z punktu widzenia funkcjonowania związku przestępczego jako układu autonomicznego, stanowi jeden z istotniejszych organów wewnętrznych. Związane jest to przede wszystkim z celem, w jakim powołano taki układ. Kumulacja energii może odbywać się poprzez gromadzenie środków w gotówce, przy wykorzystaniu instytucji finansowych podmiotów finansowo-gospodarczych, zainwestowaniu z zyskiem w udziały przedsiębiorstw, giełdę itp. (energia związana ze środkami finansowymi). Ponadto w ramach zasilenia energetycznego możliwe jest kumulowanie środków rzeczowych (oraz nieruchomości). Przykładem zasilenia będzie uzyskanie środków ze sprzedaży skradzionego samochodu. Energia z akumulatora będzie uwolniona w zależności od ustalonej sytuacji: przekazanie środków na ochronę prawną zatrzymanych członków związku przestępczego, przekupienie urzędnika, funkcjonariusza (korupcja), wykorzystanie samochodu do przyjazdu na miejsce dokonania napadu i ucieczki z niego, zainstalowanie na terenie nieruchomości urządzeń technologicznych służących do produkcji amfetaminy itp. Przyjmując, że działania zorganizowanych grup przestępczych są realizowane w formie świadczenia nielegalnych usług, możliwa jest również sytuacja, w której środki na zrealizowanie działalności przestępczej będą pochodziły spoza grupy lub związku. W takim przypadku układ otrzyma zasilenie zewnętrzne, w które sam nie będzie musiał się zaangażować. Rolą układu będzie jedynie zrealizowanie zadania na rzecz podmiotu zewnętrznego, przy określonym zysku własnym. *Akumulator powinien mieć pojemność energetyczną dostosowaną do długości przerw w pobieraniu energii z otoczenia*[45]. W odniesieniu do funkcjonowania organizacji przestępczych można wskazać na to, że aby dana organizacja była zdolna do utrzymania się w czasie, niezbędne jest, aby posiadała określone zasoby potrzebne do funkcjonowania (środki finansowe na prowadzenie nielegalnych interesów, wsparcie prawne dla aresztowanych członków organizacji oraz członków ich rodzin itp.). Nie chodzi tu o „pojemność" w sensie dosłownym, ale o potrzebę ustalenia takiej wysokości środków finansowych, która zabezpieczy organizację na wypadek odchyleń od wzorców

[44] J. Kossecki, *Cybernetyka kultury*, Warszawa 1974, PIW, s. 66.

[45] M. Mazur, *Wytyczne budowy autonomu* [online], M.A. Jędrecki (oprac.), www.autonom.pl.

funkcjonowania. Zapewnienie akumulacji energii autonomu może być zróżnicowane. Niekoniecznie będzie to związane np. z ukryciem środków pochodzących z przestępstwa jako tzw. żywej gotówki do dyspozycji homeostatu.

Innym rodzajem postępowania (może nawet bardziej niezawodnym) będzie zapewnienie sobie pomnażania tych środków na przyszłość (stąd potrzeba „wyprania" takich środków) czy zapewnienie sobie gwarancji stałego źródła ich dostarczania (np. regularne pobieranie haraczu od restauratorów). Z pewnością organizator, budując układ przestępczy (przy założeniu jego trwania w czasie), będzie musiał zapewnić także energię zagregowaną w akumulatorze również w przypadku czasowej utraty zasilenia układu (np. w przypadku zidentyfikowania i konfiskaty narkotyków przez organy ścigania, co ograniczy zyski planowane z ich sprzedaży).

5. Efektor

Efektor to organ układu zapewniający oddziaływanie na otoczenie. Za efektora uznaje się przede wszystkim tzw. „żołnierzy", czyli bezpośrednich wykonawców – sprawców przestępstw. Efektorem może być także element wskazany nie tylko ze względu na przynależność do związku, ale także ten, który otrzyma indywidualne polecenie dokonania określonego przestępstwa (wpływanie na otoczenie, zgodnie z rolą układu), czyli działający na polecenie kierownictwa, z pominięciem pozycji w hierarchii czyli np. z pominięciem bezpośrednich zwierzchników. Nie będzie nim natomiast osoba, która poprzez dokonanie przestępstwa według przyjętych przez związek norm nie spełniła dodatkowych warunków mogących potwierdzić jej przynależność do związku (element otoczenia współpracujący z układem). W takim przypadku nadal będzie ona traktowana jako element otoczenia. Wydaje się, że efektor w takim układzie ma zapewnić jedynie skuteczne wykonanie polecenia, tj. wyegzekwowanie haraczu, fizyczne odebranie środków finansowych w wyniku napadu, przekazanie środków zebranych w wyniku sprzedaży narkotyków, spowodowanie przelania środków finansowych przez instytucję finansową, przywłaszczenie rzeczy pochodzących z kradzieży, odebranie okupu, posłużenie się fałszywą (lub zeskanowaną) kartą płatniczą, zastraszenie osoby, dokonanie napadu, kradzieży itd.

Efektor odpowiada za przynależność do związku przestępczego, ale także za konkretne, dokonane przestępstwo (rozbój, kradzież, napad, handel ludźmi, oszustwo bankowe itp.). Jeżeli uczestnicy związku przestępnego lub zorganizowanej grupy przestępczej naruszają wszystkie elementy składowe czynu zabronionego określonego w części szczególnej *Kodeksu karnego*, czyli dokonują przestępstwa, odpowiedzialność za to pochłania odpowiedzialność za udział w związku lub grupie jako współukarany czyn poprzedni. Gdy następuje jedynie częściowa realizacja celów związku czy grupy, czyli zły zamiar jego uczestników nie zostaje osiągnięty, to sprawcy będą odpowiadali za udział w związku przestępczym lub w grupie zorganizowanej (art. 258 kk) oraz za popełnienie w jego (jej) ramach przestępstwa (przestępstw)[46].

[46] M. Bryła, *Porozumienie, zorganizowana grupa, związek przestępczy jako formy organizacyjne przestępczości zorganizowanej*, „Prokuratura i Prawo" 2000, nr 3, s. 24. Teza nr 4 25453/4.

6. Organizator oraz homeostat związku przestępczego jako układu autonomicznego[47]

Jeszcze przed podjęciem rozważań, jak należy traktować organizatora związku przestępczego jako układu cybernetycznego, należałoby odnieść się do poglądów przedstawionych przez J. Skałę[48]. Ich reprezentantami są też A. Wąsek i W. Cieślak. Według pierwszego z autorów możemy mówić o kierowaniu dokonaniem czynu zabronionego zarówno w znaczeniu szerokim, obejmującym organizowanie jego popełnienia (stadium przygotowania), jak i w znaczeniu wąskim, gdy mamy do czynienia z kierowaniem dokonaniem czynu zabronionego przez inną osobę (stadium usiłowania i dokonania)[49]. Zdaniem W. Cieślaka pod pojęciem „kierowania wykonaniem czynu zabronionego" należy rozumieć nie tylko kierowanie sensu stricto, lecz także organizowanie działalności przestępczej. Autor ten uważa, że organizatora należy traktować jako sprawcę kierowniczego, gdyż jego rezygnacja z kierowania akcją przestępczą i jej nadzorowania jest najczęściej wynikiem jego wolnej decyzji podyktowanej często obawą o własne bezpieczeństwo i chęcią uniknięcia zdemaskowania. Takie rozszerzające ujęcie sprawstwa kierowniczego umożliwi odzwierciedlenie właściwej roli organizatora, który stanowi zarzewie czynu zabronionego, swego rodzaju iskrę rozniecającą ogień[50]. Wydaje się, że powyższe poglądy odzwierciedlają to, czym jest działanie organizatora w związku przestępczym jako układzie cybernetycznym. W prezentowanym opisie układu przede wszystkim wyróżnimy organizatora wewnętrznego układu, który dodatkowo jest jego homeostatem. Taka sytuacja ma miejsce wtedy, gdy osoba zakładająca związek przestępczy pozostaje w nim na stanowisku kierowniczym i odgrywa rolę homeostatu, czyli osoby wpływającej na równoważenie funkcjonalne układu (tj. zabezpiecza jego byt w czasie).

Rolę organizatora będzie mogła odgrywać osoba, która od początku (pierwotnie) zakłada związek przestępczy (podejmuje decyzję co do jego ram organizacyjnych, doboru personalnego i zbudowania relacji pomiędzy nimi), ale także taka, która zdobyła pozycję kierowniczą w hierarchii przestępczej układu. Rolę tę może odegrać także podmiot zewnętrzny, np. kierujący innym związkiem przestępczym, który przejmuje sterowanie układem i zaczyna nim kierować (sterować) we własnym interesie. Ponadto organizatorem mogą być również inne podmioty. W odniesieniu do związków przestępczych o charakterze terrorystycznym organizatorami mogą być podmioty polityczne innego państwa (agenci służb specjalnych, służby bezpieczeństwa państwa). W ten sposób mogą one pośrednio realizować działania polegające na przeciwdziałaniu równowadze funkcjonalnej układu społecznego, wobec którego pozostają w sprzeczności. Taki układ staje się narzędziem walki z układem społecznym, do którego zmiany będzie dążył organizator.

---

[47] Dość często zdarza się, że osoby, które zakładają zorganizowaną grupę przestępczą później pełnią w niej funkcje kierownicze. Nie jest to jednak reguła. Jak wynika z badań przeprowadzonych przez O. Krajniak, wszystkie osoby znajdujące się na najwyższym szczeblu w grupie odgrywały rolę kierującego zorganizowaną grupą przestępczą. Nie wszystkie osoby kierujące grupami były jednak również ich założycielami. Zob. O. Krajniak, *Zorganizowane grupy przestępcze. Studium kryminalistyczne,* Warszawa 2011, Wolters Kluwer, s. 163–164.

[48] Zob. J. Skała, *Normatywne mechanizmy zwalczania przestępczości zorganizowanej w świetle przepisów kodeksu karnego* (cz. 2), „Prokuratura i Prawo" 2004, nr 4, s. 40.

[49] A. Wąsek, *Współsprawstwo w polskim prawie karnym*, Warszawa 1977, Wydawnictwo Prawnicze, s. 97

[50] W. Cieślak, *Kierowanie wykonaniem czynu zabronionego jako istota sprawstwa kierowniczego,* „Państwo i Prawo" 1992, nr 7, s. 73–74.

Rolę homeostatu odgrywa ścisłe kierownictwo układu, które nim zawiaduje, w tym wydaje polecenia, rozlicza wykonawstwo i na bieżąco organizuje działalność przestępczą (inicjuje i pobudza do działania w celu zasilania energią i informacją). Tym samym dba o stabilność funkcjonalną układu i niwelowanie odchyleń od ustalonej normy postępowania (np. jeżeli organizator ukierunkowuje działania na kradzieże samochodów, to niedopuszczalne jest organizowanie przez średni szczebel przy tej okazji, bez wiedzy organizatora, handlu narkotykami[51]). Należy zauważyć, że otoczenie działa na system zakłócająco, stara się ten system zniszczyć. Jest to zrozumiałe z punktu widzenia występowania związku przestępczego, który w ocenie organizatora układu społecznego generuje odchylenia ustalonego ładu funkcjonalnego[52]. Tym samym organizator układu społecznego stara się tak oddziaływać na układ przestępczy, aby doprowadzić do jego nierównowagi i ustania. System otwarty uruchamia mechanizmy obronne przed niszczącym działaniem otoczenia. System, który zdoła obronić się przed niszczącym działaniem otoczenia, jest systemem będącym w stanie dynamicznej równowagi[53]. Stąd też istotna pozostaje rola organizatora przy wyborze struktury organizacyjnej układu i sposobu bieżącego kierowania nim (przygotowywania reakcji na bodźce z otoczenia).

Choć pozostałe elementy struktury wewnętrznej związku przestępczego będą miały cechy organizatorskie, to nie będą jednak organizatorem układu, ale wykonawcami woli organizatora. Ich rola będzie się sprowadzała do zapewnienia równowagi funkcjonalnej dla układu jako całości na niższych szczeblach zarządzania (na poszczególnych szczeblach pośrednich). Wyznacznikiem bycia organizatorem układu może stać się także sposób określenia sprawstwa czynu zabronionego, jaki występuje w *Kodeksie karnym* (art. 18 § 1). Związane jest to z tym, że organizator jest postrzegany zarówno jako organizator czynów karalnych, realizujący tym samym funkcję systemu (wykonawstwo), jak i organizator układu – nieformalnego wzorca zapewniającego osiągnięcie optymalnego rezultatu dla działania układu (organizator struktury układu). Zgodnie z aktualnymi przepisami za sprawstwo odpowiada nie tylko ten, kto wykonuje czyn zabroniony sam albo wspólnie i w porozumieniu z inną osobą, ale także ten, kto kieruje wykonaniem czynu zabronionego przez inną osobę lub, wykorzystując uzależnienie innej osoby od siebie, poleca jej wykonanie takiego czynu. To określenie sprawstwa mieści w sobie nie tylko pojęcie sprawstwa kierowniczego, ale również sprawstwa polecającego. W tym drugim przypadku konstrukcja ta, która występowała dotąd jedynie przy określaniu odpowiedzialności rozkazodawcy (zob. art. 290 § 2 kk z 1969 r.), została rozszerzona na wszystkie wypadki uzależnienia i podporządkowania prowadzącego do wydawania poleceń. Pozwoli ona uznać za sprawcę takiego szefa organizacji lub grupy przestępczej, który wydaje jedynie wiążące polecenia, a nie zajmuje się kierowaniem ich wykonania. Należy dodać, że uzależnienie innej osoby od sprawcy polecającego nie musi mieć charakteru formalnego. Ważne jest to, żeby istniało faktycznie i oznaczało realną władzę nad inną osobą[54]. Tym samym rola organizatora zostaje wyznaczona także na podstawie przyjętych wewnątrzorganizacyjnych relacji pomiędzy poszczególnymi elementami przestępczego układu.

---

[51] Taki stan rzeczy może być związany z tym, że kradzieże samochodów są pod kontrolą organizatora, handel narkotykami natomiast nie został uzgodniony przy podziale wpływów i zysków z innym układem, co przy samowolnym jego realizowaniu może powodować zarzewie przyszłego konfliktu.

[52] Zob. Z. Biniek, *Elementy teorii systemów...*, s. 8.

[53] Tamże.

[54] Komentarz do art. 18 kk (Dz.U. z 1997 r. Nr 88, poz. 553), w: A. Marek, *Kodeks karny. Komentarz*, LEX, 2007, wyd. IV, stan prawny na 15.03.2007 r.

Homeostat koordynuje przepływy, w których uczestniczy korelator (przepływy informacyjne) i akumulator (przepływy energetyczne). Homeostatem będzie organ układu zapewniający przeciwdziałanie przepływom informacji i energii, zmniejszającym możliwość oddziaływania systemu na otoczenie. Tym samym dla zapewnienia funkcjonowania związku przestępczego niezbędne jest kojarzenie tych dwóch kanałów, które w rzeczywistości pozwalają na formułowanie odpowiednich związków zarządczych, a w konsekwencji – decyzji związanych z kierowaniem układem. Szczególną rolę pełni tu informacja (negentropia).

Jak wspomniano powyżej, organizatora można kojarzyć zarówno na poziomie fazy wstępnej, tj. zakładania związku przestępczego[55] – powstawania układu, jak i (jeżeli utrzyma tę rolę) na poziomie kierowania związkiem, czyli sterowania poziomem jego funkcjonowania[56]. Według orzeczenia Sądu Apelacyjnego w Lublinie pojęcie „kierowania" nie oznacza tylko sytuacji o charakterze statycznym, sprowadzającej się do sprawowania władztwa nad istniejącą strukturą. Pojęcie to należy rozumieć jako określające pewną dynamikę sytuacji. „Kierowanie" oznacza nie tylko stanie na czele zorganizowanej grupy przestępczej, ale też kierowanie konkretnymi działaniami tej grupy[57].

Zarówno jedno, jak i drugie zachowanie organizatora sprawdza się tak w jakości, jak i w praktyce działania. Oznacza to, że dopiero jakość „twórcza" i „zarządcza" organizatora jest widoczna w konfrontacji z otoczeniem i ze specyficznymi układami w jego otoczeniu, jakimi są układy odpowiedzialne za ściganie przestępstw. Dlatego też organizator musi zdawać sobie sprawę z tego, jaki potencjał mają organy ścigania, jakimi atrybutami dysponują wobec związku przestępczego oraz jak elementy otoczenia będą reagowały na działania związku, które staną się jego ofiarami. Słabość organizatora takiego związku będzie się przejawiała bądź w całkowitej likwidacji układu – zatrzymanie członków związku przestępczego i ich wyizolowanie społeczne, co spowoduje ustanie relacji między poszczególnymi elementami takiego układ czy też częściowe osłabienie, ale na tyle skuteczne, że organizator będzie się starał uzupełnić układ o kolejne elementy, aby znowu mógł on być funkcjonalnie stabilny. Wydaje się, że w luźniejszym systemie przestępczym, jakim są sieci, zarządzanie będzie polegało także na skorzystaniu z potencjału określonego układu, a przy niezrealizowaniu celu funkcjonalnego, na skorzystaniu z innego podobnego układu aktywnego w ramach sieci. Ponadto organizator homeostat musi mieć realny wpływ na działania korelatora i akumulatora. Tym samym musi stworzyć wewnętrzne mechanizmy analizy informacji i energii tak, aby w ramach wyznaczonego celu decyzyjnego (zgodnego z celem funkcjonalnym) zapewnić określoną proporcję sił i środków doprowadzających do dokonania przestępstwa. W związku z tym, że przestępstwo staje się źródłem zasilenia układu, to w konsekwencji musi zapewnić także taką kumulację środków w akumulatorze, aby skonkretyzowana energia pozwoliła na bieżące funkcjonowanie tego układu, utrzyma-

[55] Użyte w przepisie art. 258 § 3 kk pojęcie „zakłada" może polegać na podejmowaniu czynności nie mających nic wspólnego z podżeganiem. Czynności te mogą polegać np. na nawiązywaniu kontaktów, sporządzaniu planów przestępczej działalności i gromadzeniu środków niezbędnych do popełnienia przestępstwa. Należy zwrócić uwagę, że czasownik „zakłada" jest użyty w art. 258 § 3 kk w formie niedokonanej. Karalne jest więc już samo „zakładanie", a nie dopiero „założenie" zorganizowanej grupy albo związku przestępczego. Zob. M. Bryła, *Porozumienie, zorganizowana grupa*..., s. 24. Teza nr 1 25453/1.

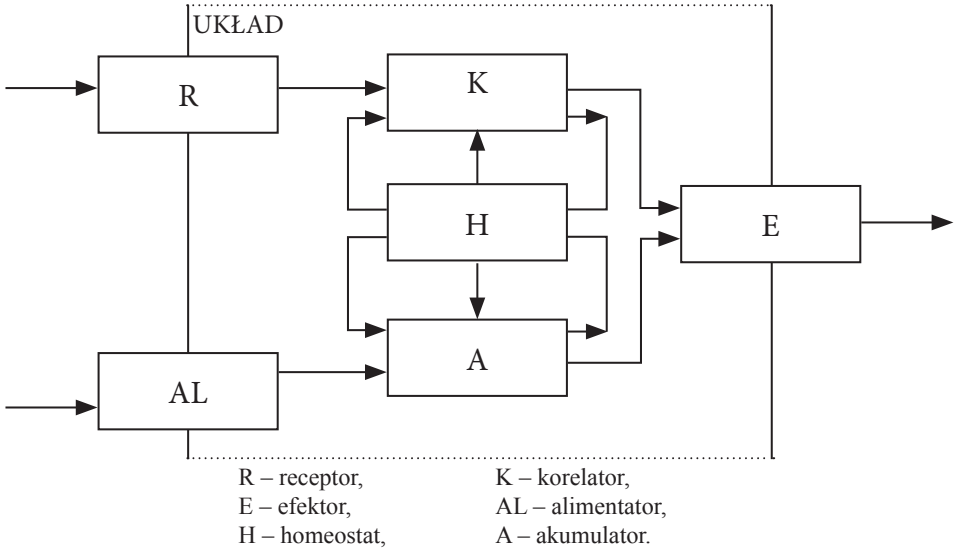
[56] Art. 258 § 3.: *Kto grupę albo związek określone w § 1, w tym mające charakter zbrojny zakłada lub taką grupą albo związkiem kieruje (…)*.

[57] Postanowienie Sądu Apelacyjnego w Lublinie z dnia 27 stycznia 998 r., A.OSA Lublin 1998, nr 1, k. 9.

nie bytu w ramach ograniczenia dostarczania energii oraz zaangażowanie energii w jej pomnażanie. Realny wpływ będzie związany z tym, że organizator będzie ośrodkiem decydującym o tym, gdzie, komu i w jakiej proporcji zapewni udział w przestępczym zysku, ale także gdzie, kiedy i z kim dokona się przestępstwa (czyli dokona się relacja przysporzeniowa między elementami systemu a elementami otoczenia). W takim przypadku organizator, wyznaczając zadania, będzie kierował się określoną wcześniej sterowalnością układu. Będzie się to wiązało z zarządzaniem informacją w ramach układu, a szczególnie tą informacją, która będzie dotyczyła bodźców zagrażających równowadze funkcjonalnej układu. Organizator będzie poszukiwał odpowiednich reakcji wobec tych bodźców, tak aby zapewnić realne bezpieczeństwo układu.

Pojęcie „organizatora układu" w odniesieniu do związku przestępczego należałoby rozumieć znacznie szerzej niż wyłącznie w rozumieniu przepisów prawa karnego. Wydaje się, że powinien on być postrzegany bardziej z punktu widzenia działań pozaprocesowych o charakterze operacyjno-rozpoznawczym. Organizator w układzie (związku) jest odpowiedzialny nie tylko za organizację i zlecanie przestępstw. Aktywność układu (związku) nie zawiera się wyłącznie w dokonywaniu przestępstw. Dlatego też rola organizatora (homeostatu) będzie dostrzegana także w: kierowaniu dystrybucją osiągniętych zysków przestępczych, doskonaleniu i wprowadzaniu nowych metod taktycznych w zakresie organizowania przestępstw, zlecaniu stosowania czynników bezpieczeństwa i wewnętrznej oceny efektów działania, kontrolowaniu i budowaniu relacji pomiędzy członkami grupy (związku) oraz innymi podobnymi układami, zasilaniu układu w atrybuty niezbędne do działania, tj. w broń, materiały wybuchowe, organizowanie działań kontrwykrywczych[58] itp.

Dla zobrazowania, jak wygląda struktura układu samodzielnego, można posłużyć się rysunkiem prezentowanym przez M. Mazura[59].



Rys. 1. Schemat układu samodzielnego.
Źródło: M. Mazur, *Cybernetyka i charakter*, Warszawa 1976, PWN, s. 164.

[58] To ogół przedsięwzięć podejmowanych przez zorganizowane grupy przestępcze, które zmierzają do stworzenia warunków niezbędnych do popełniania przestępstw, zwiększania hermetyczności grup oraz ich możliwości operacyjnych. Są to np.: infiltracja bezpośrednia, infiltracja pośrednia, działania wywiadowcze, dezintegrujące i dezinformacyjne. Zob. P. Michna, T. Safjański, J. Żelazek, *Działania kontrwykrywcze zorganizowanych grup przestępczych*, „Przegląd Policyjny" 2006, nr 4, s. 99–100.

[59] M. Mazur, *Cybernetyka i charakter…*, s. 164.

Analiza zachowań systemu

Pomiędzy związkami przestępczymi mogą zachodzić wzajemne relacje. Niekoniecznie i nie zawsze będą one oparte na synergii. Synergia działania oparta jest głównie na relacjach pojedynczego lub stałego współdziałania w czasie generowania zysków. Przykładem synergii mogą być powiązania przestępcze pomiędzy polskimi grupami zorganizowanymi (lata 90. XX wieku) a kartelami narkotykowymi działającymi na terenie Ameryki Południowej. Współpraca odbywała się na zasadzie wymiany – środki finansowe za towar (kokaina), który następnie był dystrybuowany na terenie Polski i Europy. Należy zauważyć, że niektóre rodzaje przestępstw wręcz wymuszają współdziałanie ustalonych partnerów przestępczych, gdzie synergia jest oparta na organizowaniu przestępstwa, a następnie na uczestniczeniu w podziale zysków. Występuje ona niezależnie od samodzielności poszczególnych grup (związków) działających na danym terenie. Przykładem jest handel żywym towarem, w którego przypadku w przestępczym przedsięwzięciu realizują się organizacje przestępcze z kraju inicjatywnego poprzez grupy działające w poszczególnych krajach przerzutowych, po kraj docelowy wykorzystujący przemycany „żywy towar" do działań przestępczych czy czerpania dochodów (np. prostytucja, zmuszanie do pracy w gospodarstwach itp.).

Układ samodzielny jest zarazem układem sterującym (wobec innego układu), jak i samosterownym (wobec samego siebie). Gdyby brakowało w układzie zdolności do samosterowania się, straciłby on status układu samodzielnego. Stąd też związki przestępcze muszą mieć wykreowane mechanizmy samosterowania. Dotyczyć one będą umiejętności zarządzania energią i informacją. Wiązać się to będzie z takimi działaniami, jak: podział zysków, decydowanie o przydziale efektorów i ich rozliczanie z wykonania zadań z elementami otoczenia, eliminowanie zagrożeń, tj. elementów współdziałających z organami ścigania oraz innymi konkurencyjnymi układami, nieuprawnionym pobieraniem energii z otoczenia bez wiedzy organizatora, reagowaniem na działania organów ścigania – zatrzymania, obserwację itp. oraz skompresowanie powiązania energii i wiedzy (informacji) do podjęcia dalszych planowanych zyskownych reakcji w otoczeniu.

Homeostat jako organizator pozostaje sprzężony w torze energetycznym z akumulatorem. Tym samym może wpływać na ilość energii w akumulatorze. Z pewnością ta możliwość z punktu widzenia fizyki może być realizowalna jako zachowania możliwe w środowisku przestępczości zorganizowanej. Zwiększenie mocy jałowej ogranicza nadmiar energii skumulowanej w akumulatorze. Wydaje się, że podobnym rozwiązaniem jest podjęcie przez kierownictwo związku przestępczego decyzji o udziale w większym przedsięwzięciu (nawet pozakryminalnym) mającym przynieść zyski w dalszej perspektywie. Zgromadzony (w akumulatorze) w ramach grupy zysk przestępczy nie będzie do końca satysfakcjonujący dla związku, ponieważ nie będzie ona pracowała na jego pomnażanie. Dlatego też w celu wyeksponowania nadmiaru energii (zysku) będzie możliwe zainwestowanie tych środków w zakup akcji przedsiębiorstw, udział w budowie biurowca w intratnym miejscu miasta, wykup nieruchomości pod budowę autostrad itp. Wydaje się, że nietrudno odnieść się do stwierdzenia, iż poprzez takie działanie związek stabilizuje się (utrzymuje równowagę funkcjonalną). Takie posunięcia związane z kontrolowanym wypływem energii do otoczenia pozwalają w dalszej perspektywie liczyć na kolejne zyski, tym razem niewygenerowane bezpośrednio, ale pośrednio z popełnianych przestępstw. Ta stabilizacja uwidocznia się w tym, że związek, mimo że nie będzie popełniał przestępstw, to będzie posiadał trwałe, stabilne podstawy funkcjonowania finansowego. Zarządzania energią można upatry-

wać także w optymalnym określaniu decyzji dotyczącej rodzaju źródeł pozyskiwania środków, a szczególnie typowania do dokonywania tych rodzajów przestępstw, które przy mniejszym nakładzie energetycznym powodują pozyskanie znacznych, nowych środków do akumulatora (przysporzenie energii).

Kolejnym istotnym zadaniem homeostatu jest sprzężenie go z torem informacyjnym, co również powinno zapobiegać deregulacji funkcjonalnej. Gromadzenie w korelatorze informacji (dzięki wykrywaniu bodźców przez receptory) o zmianach wywoływanych w otoczeniu (wskutek reakcji spowodowanych przez efektory) pozwala wpływać na otoczenie przez dobór reakcji usuwających z otoczenia czynniki mogące naruszyć równowagę funkcjonalną układu samodzielnego[60]. Przykładem takiego postępowania jest uzyskanie od funkcjonariusza współpracującego ze związkiem przestępczym informacji dotyczącej zbliżającej się realizacji ze strony organów ścigania czy korumpowanie pracowników wymiaru sprawiedliwości (zamiana środka karnego, zniszczenie lub ukrycie dowodów, sporządzenie niejednoznacznej ekspertyzy). W ostateczności homeostat podejmuje decyzje odnośnie do np. zmiany lub nieprzebywania w dotychczasowym miejscu zamieszkania, przeniesienia skradzionego samochodu z jednej „dziupli" do innej, spalenia środka transportu uczestniczącego w działaniach przestępczych w celu zniszczenia śladów itp.

Innym przykładem jest zapewnienie równowagi funkcjonalnej układu bez udziału czynników pochodzących z otoczenia. W takim przypadku oddziaływanie na otoczenie odbywa się bez aktywności homeostatu. Szczególną rolę odgrywają tu relacje zachodzące pomiędzy korelatorem a akumulatorem. Sytuacja taka może mieć miejsce wtedy, gdy średni szczebel zarządzania układem, w wyniku prowadzonych działań przestępczych, nie zapewnił ustalonych zysków dla kierownictwa związku. W konsekwencji intensyfikuje inne działania przestępcze w celu zebrania całości kwoty (np. nie tylko z handlu ulicznego narkotykami, lecz także z wymuszenia haraczu na kolejnych właścicielach sklepów czy restauracji). Podobnie rzecz się ma w przypadku niezrealizowania przestępstwa poprzez odstąpienie od niego ze względu na zwiększenie się zagrożenia dla sprawców (poszukiwanie źródeł popełnionego błędu – niewłaściwe rozpoznanie, współpraca członka grupy z organami ścigania, wprowadzenie funkcjonariusza w środowisko związku przestępczego).

Należałoby się zastanowić nad sprawdzalnością tego rodzaju struktury organizacyjnej w odniesieniu do tego typu związku. Czy jest ona optymalna, czy też jej wartość jest niska i przyjęcie jej dla tego typu związku uniemożliwiłoby osiągnięcie założonego celu (łącząc cel działania związku jako układu w zjawisku przestępczości zorganizowanej z celem istnienia czasowego układu samego w sobie)? Z pewnością do tego wzorca nie można podchodzić statycznie, gdyż jest on jedynie odniesieniem do procesów, jakie mogą zachodzić w układzie, szczególnie do możliwości śledzenia przepływów energetycznych (wygenerowanie środków – ich podział – zaangażowanie w pomnażanie zysków) i przepływu informacji (wartości informacji, jej źródła, sposobu przekazywania komunikatów, sposobu udzielania odpowiedzi na bodźce, utrzymywanie kontaktów z elementami otoczenia itp.)[61]. Wykonywanie określonego zadania

[60] M. Mazur, *Cybernetyczna teoria układów...,* s. 58.

[61] Na potrzeby walki z układem przestępczym będzie możliwe wykorzystanie teorii informacji, a zwłaszcza ograniczanie możliwości sterowniczych układu poprzez zakłócanie przekazywania informacji pomiędzy organami od nadawcy do odbiorcy, przy założeniu, że zniekształcenie informacji powoduje głównie zakłócenie wewnętrzne i zewnętrzne w kanale komunikacyjnym. Zob. A. Berg, *Informacja i cybernetyka*, Warszawa 1970, Wydawnictwo Naukowo-Techniczne, s. 102.

układu przestępczego (popełnienie przestępstwa) pozwala na jego zidentyfikowanie (pozyskanie informacji na temat charakterystycznych, przynależnych wyłącznie temu układowi cech aktywności). W rzeczywistości będziemy mieli do czynienia z wielokrotnością aktywnych receptorów, alimentatorów i efektorów[62], a także z łączeniem tych funkcji w danym elemencie.

W zależności od ukształtowania kierownictwa związku (organizatora) homeostat będzie ograniczony do jednej lub kilku osób z kierownictwa i homeostatycznych zachowań kierownictwa średniego szczebla w ograniczonym zakresie (o ile w danym związku organizator będzie przewidywał wystąpienie szczebla pośredniego). Dobór korelatora i akumulatora powinien być przede wszystkim zależny od homeostatu, ponieważ to on będzie współdziałał z tymi dwoma organami przy sterowaniu układem i odpieraniu zachowań mogących zagrozić równowadze funkcjonalnej układu jako całości. Wydaje się także, że występowanie w związku przestępczym korelatora i akumulatora wyzwala potrzebę budowania struktury (ogniw) pośredniej organów kumulujących informację i energię. Inaczej tę rolę musiałby przejąć sam organizator układu. Jednakże takie rozwiązanie byłoby na tyle niekorzystne, że w przypadku zatrzymania szczebla kierowniczego układ zaprzestawałby praktycznie swojej aktywności (ustanie układu).

Na potrzeby utrzymania równowagi funkcjonalnej układu homeostat może reagować w różny sposób. Taką reakcją będzie wzmocnienie kontroli hierarchiczności struktury i podjęcie decyzji o jej podziale. W tym drugim przypadku działanie może być powodowane ograniczonymi możliwościami sterowania związanymi np. z utworzeniem kilku szczebli pośrednich. Stąd możliwe jest spłaszczenie struktury i zwiększenie usamodzielnienia się poszczególnych członów wzajemnie ze sobą współdziałających. Należy jednak zauważyć, że dokonując podziału dużej struktury nie zawsze można utworzyć strukturę (wyodrębnioną) podobną. Wynika to z tego, że nie będzie ona zawierała wszystkich elementów struktury głównej. Odpowiedzią na takie postępowanie będzie powołanie podobnych struktur z zapewnieniem ich samosterowania, ale nie samodzielności. Tego typu działanie może doprowadzić do przekształcenia dotychczasowej struktury hierarchicznej w strukturę sieciową[63]. Konsekwentnie, na potrzeby utrzymania organizacji, układ samosterowny może po podjęciu takiej decyzji przez homeostat przejść w układ samodzielny. Układ zależny (czy współdziałający) nie może stanowić przeszkody w rozwoju i realizacji celu funkcjonalnego układu jako całości. Jego poszczególne elementy (organy), takie jak efektory i receptory, nadal muszą mieć zarówno zdolność do działania zgodnego z celem (reguła zgodności), jak i zdolność do spełniania się (reguła efektywności).

[62] Zgodnie z badaniami O. Krajniak na poziomie podstawowym następowała znaczna rotacja personalna, a ponadto był to poziom najliczniejszy. Jak stwierdza autorka, przyczyna tego stanu rzeczy mogła tkwić w naturze szczebla podstawowego, na którym działały osoby bezpośrednio uczestniczące w dokonywaniu przestępstw. Dlatego były one bardziej narażone na ryzyko wykrycia ich przez organy ścigania. Innym powodem było to, że ciągła rotacja powodowana była względami bezpieczeństwa grupy i potrzebą zwiększenia jej zysków. Zob. O. Krajniak, *Zorganizowane grupy przestępcze*… s, 129.

[63] Zmianę jednego stanu układu na drugi ze wskazaniem kierunku zmiany nazywa się także przejściem. Zbiór przejść dokonanych w pewnym zbiorze obiektów natomiast to transformacja. Zob. W. Szostak, *Cybernetyka społeczna*, Kraków 1978, Uniwersytet Jagielloński, s. 11.

Podsumowanie

Uwzględniając przedstawione uwagi można uznać, że wskazana wzorcowa struktura autonomu może posłużyć do przyjmowania różnych strukturalnych kształtów przez organizacje przestępcze. Podstawową rolą organizatora układu autonomicznego (organizacji przestępczej) jest takie jego zorganizowanie, aby pełnił swoją funkcję w realizacji ustalonego celu działania. Dlatego też organizator powinien zapewnić:
- odpowiednią liczbę efektorów i receptorów układu,
- właściwe relacje pomiędzy elementami korelator–homeostat–akumulator (refleksje homeostatu) dla zagwarantowania sprawnego kierowania (sterowania) organizacją,
- źródła zasilania energetycznego (rodzaj popełnianych przestępstw),
- stosowanie właściwych środków kontroli procesów decyzyjnych i zasileniowych dla układu[64].

Stąd też w przyszłości można zaproponować prowadzenie badań nad strukturami związków przestępczych charakteryzujących się popełnianiem przestępstw kierunkowych. Uzyskanie odpowiedzi pozwoli na ocenę, czy występują podobieństwa między poszczególnymi układami przestępczymi w zakresie doboru ich elementów wewnętrznych, sposobu zarządzania nimi i stosowania reakcji na bodźce zewnętrzne. Wydaje się, że tego rodzaju przedsięwzięcia powinny być częścią badań kryminalistycznych, także z wykorzystaniem dotychczasowych osiągnięć, jakie daje cybernetyka, a zwłaszcza teoria układów samodzielnych. Pozwala ona bowiem na typowanie rodzajów układu oraz jego elementów i przypisywanie im roli, jaką odgrywają w układzie, oraz na skupienie się na relacjach zachodzących pomiędzy elementami wewnętrznymi oraz elementami wewnętrznymi a otoczeniem. W konsekwencji będzie możliwe uzyskiwanie przez organy ścigania takiego poziomu wiedzy, który pozwoli na typowanie taktyki postępowania (przeciwdziałania) adekwatnej do zagrożenia.

Należy wspomnieć także o budowaniu charakterystyk i możliwych scenariuszy zachowań w układach przestępczych z wykorzystaniem psychocybernetyki[65]. Przede wszystkim ważna jest ocena układów przestępczych (w tym układów działających wyłącznie w strukturze sieciowej) w dobie ich przekształceń głównie w sieci przestępcze. W tym zakresie pewną odpowiedzią może być podejmowanie działań sieciocentrycznych[66]. Ponadto teorię układów samodzielnych będzie można wykorzystać do opracowywania optymalnych metod sterowania układami przestępczymi, gdzie założonym celem będzie doprowadzenie ich do deregulacji równowagi funkcjonalnej, a w konsekwencji do ustania układu.

---

[64] *Należy opracowywać konstrukcje autonomów z punktu widzenia ich własnej celowości, a nie celowości spotykanej w naturze*, w: M. Mazur: *Wytyczne budowy autonomu*...

[65] Zob. J. Kossecki, *Cybernetyka społeczna*, Warszawa 1981, PWN.

[66] Przyjęcie koncepcji działań sieciocentrycznych sprawi, że będą się one w coraz większym stopniu charakteryzować małymi, rozproszonymi, ale wysoce dynamicznymi elementami, sprzężonymi sieciami łączności i sieciami informatycznymi. Chociaż oddalone od siebie, uzyskają zdolność jednoczesnego zaatakowania wybranych, kluczowych, elementów (segmentów) przeciwnika, aby natychmiast po dokonaniu uderzenia rozproszyć się, tak aby nie stać się obiektem ataku. Zob. T. Szubrycht, *Sieciocentryczność – mity i rzeczywistość*, Zeszyty Naukowe Akademii Marynarki Wojennej, 2004, nr 4.

Abstrakt

Cybernetyka jako nauka uniwersalna i porządkująca jest obecnie wykorzystywana wszechstronnie. Znajduje ona swoje zastosowanie m.in. w naukach humanistycznych, w tym w naukach prawnych. W związku z powyższym na przykład dotychczasowe analizy kryminalistyczne dotyczące przestępczości zorganizowanej mogą zostać wsparte także analizą cybernetyczną tego zjawiska. W zakresie badań nad strukturami organizacyjnymi grup przestępczych (traktowanych jako układy cybernetyczne) – pojawiła się propozycja wykorzystania teorii układów samodzielnych. Autorem przedmiotowej teorii, zbudowanej na podstawie doświadczeń z obszaru nauk ścisłych i humanistycznych, jest Marian Mazur. Teoria układów samodzielnych pozwala na zuniwersalizowanie struktury organizacji przestępczej poprzez wyróżnienie poszczególnych elementów układu, istotnych dla jego samosterowania się. Usystematyzowanie takiej struktury pozwala następnie na badanie przebiegów informacyjnych i energetycznych. Ponadto teoria ta pozwala ocenić relacje zachodzące zarówno wewnątrz układu, jak i pomiędzy jego elementami oraz elementami znajdującymi się w jego otoczeniu. Wiedząc, jak działa taki układ, uzyskujemy informację, na której podstawie uprawnione organy ścigania będą mogły opracować taktykę działań ukierunkowanych na zwalczanie zorganizowanych grup przestępczych. Idąc dalej, opierając się na uzyskanych analizach zachowań układów przestępczych i reakcji na nie, możliwe będzie poszukiwanie bardziej optymalnych wzorców przeciwdziałania przestępczości zorganizowanej.

Abstract

Cybernetics is a universal and systematic branch of science. It is currently commonly applied, e.g. in the humanities, including legal studies. Therefore, forensic analyses that were carried out so far in the area of organized crime may also be supported with a cyber analysis of the issue. There has been a suggestion to use the theory of independent systems in the research of the structures of organized crime groups (treated as cyber systems). The author of this theory based on experiences from the areas of exact sciences and humanities is Marian Mazur. By applying the theory of independent systems, we are able to take a look at a universal nature of the structure of an organized crime group through a selection of elements that are essential to independent operation of the system. Once we determine the patterns of such a structure it is possible to examine its informational and energetic processes. Moreover, this theory helps to evaluate relations both inside the system, as well as between its particular elements and elements surrounding it. Such knowledge about how the system works, makes it possible for the law enforcement bodies to develop tactics of operations targeted at organized crime groups. Moreover, based on the results of the analysis of the behaviour of system crime groups and reactions to it, it will be possible to search for more optimal methods of counteracting organized crime.

Tomasz Safjański

Efektywność działań operacyjnych Europolu w zwalczaniu terroryzmu międzynarodowego – próba oceny

Państwa członkowskie od dawna deklarują zwalczanie terroryzmu międzynarodowego jako priorytet w polityce bezpieczeństwa. Poszukiwanie skutecznych rozwiązań w tym zakresie zainicjowano już w latach 70. XX wieku jako odpowiedź na spektakularne ataki terrorystyczne (m.in. na zamach na sportowców podczas Igrzysk Olimpijskich w Monachium w 1972 r.). Z tych samych powodów poszukiwania te nabrały rozmachu w pierwszej dekadzie XXI wieku, po zamachach w Nowym Jorku, Madrycie i Londynie. Jednym z narzędzi przeciwdziałania zagrożeniom terrorystycznym stała się Europejska Agencja Egzekwowania Prawa (*European Law Enforcement Agency*), zwana potocznie Europolem[1].

Europol jest platformą wielostronnej współpracy służb policyjnych, ochrony granic, celnych, finansowych, imigracyjnych, żandarmerii, a niekiedy nawet służb specjalnych państw członkowskich UE[2]. Zapotrzebowanie na tego typu formę współdziałania ujawniło się w Europie w następstwie unijnych procesów integracyjnych, które wraz ze zniesieniem ograniczeń w swobodnym przepływie osób, towarów, usług i kapitału, stworzyły nowe perspektywy dla powstawania zagrożeń transgranicznych.

Pierwotnie przestępstwa terrorystyczne nie należały do zakresu przedmiotowego działania Europolu. Zostały one włączone do mandatu organizacji na mocy *Decyzji Rady z 3 grudnia 1998 r. polecającej Europolowi objęcie działalnością przestępstw przeciwko życiu, zdrowiu, wolności osobistej lub mieniu, popełnionych lub takich, których popełnienie jest prawdopodobne podczas działań terrorystycznych (1999/C 26/06)*[3].

Działania Europolu są oparte przede wszystkim na prowadzeniu wywiadu kryminalnego. W praktyce obejmują gromadzenie, przetwarzanie (analizę, ocenę, interpretację) oraz wymianę informacji. Upoważnienie Europolu do realizowania tego rodzaju czynności ukierunkowanych na zwalczanie terroryzmu – z zachowaniem określonych ograniczeń – jest zawarte w art. 88 *Traktatu o funkcjonowaniu Unii Europejskiej*[4]. Z ust. 2 tego artykułu wynika też uprawnienie tej struktury do koordynowania, organizowania i prowadzenia dochodzeń i działań realizowanych wspólnie z właściwymi organami państw członkowskich lub w ramach wspólnych zespołów dochodzeniowych, w stosownych przypadkach, w powiązaniu z Eurojustem. Oprócz zwalczania terroryzmu Europol prowadzi działania ukierunkowane na przeciwdziałanie przestępczości zorganizowanej i innym formom poważnej przestępczości oraz

[1] Do końca 2009 r. obowiązywała nazwa Europejskie Biuro Policji (European Police Office). W literaturze i dokumentach stosowano również nazwy: Europejski Urząd Policji lub Biuro Policji Europejskiej.

[2] Europol, mimo multiagencyjnego wymiaru, jest głównie platformą współpracy policyjnej. Wynika to z faktu, że służby specjalne nie są w Europolu reprezentowane wystarczająco.

[3] Dz.Urz. UE C 26 z 30 stycznia 1999 r., s. 22 (zakończenie ważności aktu: 31 grudnia 2009 r. – przyp. red.).

[4] Dz.Urz. UE C 326 z 26 października 2012 r.

przestępstwom z nimi powiązanym, które dotyczą co najmniej dwóch państw członkowskich (zagrożenia transgraniczne)[5].

W odniesieniu do wspomagania dochodzeń zadaniem Europolu jest przekazywanie krajowym służbom państw członkowskich wszelkich istotnych informacji potrzebnych do skutecznego prowadzenia działań operacyjnych. Wykorzystanie informacji i danych wywiadowczych przekazywanych przy udziale Europolu – w ramach prowadzonych dochodzeń i działań wspólnych zespołów śledczych – podlega krajowym przepisom o ochronie danych obowiązujących w państwie członkowskim otrzymującym informacje. Uzyskane informacje i dane wywiadowcze podlegają takim samym przepisom o ochronie danych, jak gdyby zostały zgromadzone w otrzymującym je państwie członkowskim[6].

Zakładając, że jednym z elementów decydujących o skuteczności walki z terroryzmem jest uzyskanie informacji o planowanym lub dokonanym akcie terrorystycznym, należy się zastanowić, jaka jest efektywność działań Europolu w tym zakresie. Hipotetycznie działania tej struktury powinny pozwalać na realizację chociażby jej funkcji rozpoznawczej i zapobiegawczej, gdyż podstawową rolą tej agencji jest pośredniczenie i inspirowanie państw członkowskich do wymiany informacji kryminalnych oraz danych wywiadowczych o wspólnych zagrożeniach. Teoretycznie w rezultacie działań związanych z prowadzeniem wywiadu kryminalnego w ramach Europolu powinny istnieć większe możliwości współpracy transgranicznej państw członkowskich w zakresie wspólnych przedsięwzięć antyterrorystycznych.

A jak jest w praktyce? Z całą pewnością członkostwo Polski w Europolu pozwala polskim służbom ochrony porządku prawnego na korzystanie ze wsparcia tej instytucji oraz na prowadzenie współpracy w tym zakresie ze wszystkimi państwami z nim współpracującymi. Polska jest państwem granicznym UE, dlatego też polskie służby odgrywają szczególną rolę w zwalczaniu zagrożeń terrorystycznych. Obecnie we współpracę w ramach Europolu jest zaangażowanych w naszym kraju sześć służb: Policja, Straż Graniczna, Centralne Biuro Antykorupcyjne, Agencja Bezpieczeństwa Wewnętrznego, Generalny Inspektor Informacji Finansowej oraz Służba Celna. W teorii Polska podczas tej współpracy wykorzystuje wszystkie metody i formy działań operacyjnych Europolu, obejmując swoim działaniem wszystkie rodzaje przestępstw wymienione w załączniku do decyzji o Europolu. Mimo kilkunastoletniej praktyki współdziałania Polski w ramach Europolu, jego wsparcie jest wykorzystywane przez właściwe służby krajowe w sposób incydentalny, a niektóre spośród metod i form działań w ogóle nie są stosowane. Czy w obecnym kształcie organizacyjnym i prawnym Europol może skutecznie prowadzić działania związane z przeciwdziałaniem terroryzmowi? Innymi słowy, czy ma odpowiedni potencjał do podejmowania tego rodzaju działań, a zatem czy istnieje uzasadnienie dla dalszego funkcjonowania tej agencji w obecnym kształcie prawno-organizacyjnym?

Analiza działań operacyjnych Europolu w odniesieniu do takich samych działań służb krajowych wykazała, że agencja nie dysponuje nawet formalnymi uprawnieniami do egzekwowania obowiązków w stosunku do państw członkowskich. Zgodnie z art. 88

---

[5] Art. 3 i 4 ust. 1 *Decyzji Rady z dnia 6 kwietnia 2009 r. ustanawiającej Europejski Urząd Policji (Europol) (2009/371/WSiSW)* (Dz.Urz. UE L 121 z 15 maja 2009, s. 37).

[6] Art. 8 pkt. 2 *Decyzji Ramowej Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej* (Dz.Urz. UE L 386 z 29 grudnia 2006, s. 89).

ust. 3 traktatu: *wszelkie działania operacyjne Europolu są prowadzone w powiązaniu i w porozumieniu z organami Państwa Członkowskiego lub Państw Członkowskich, których terytorium dotyczą. Stosowanie środków przymusu należy do wyłącznej kompetencji właściwych organów krajowych*[7]. Europol nie ma zatem autonomicznych środków działania o charakterze kontrterrorystycznym. W tym kontekście nie ma żadnych uprawnień, jakie zazwyczaj są przypisane krajowym służbom, jak prawo do zatrzymania, przeszukiwania mieszkań lub stosowania kontroli operacyjnej.

W odniesieniu do Europolu można wyszczególnić kilka metod działań operacyjnych, które w większości są zbliżone do siebie rodzajowo. Wspólnym mianownikiem znacznej części tych metod jest posługiwanie się informacjami lub zarządzanie danymi wywiadowczymi. Wydają się one tworzyć, z punktu widzenia Europolu, spójny system działań z elementami synergii między poszczególnymi metodami i formami. Przykładem czynności, których państwa członkowskie nie są w stanie skutecznie realizować bez wsparcia Europolu, są analizy strategiczne na potrzeby predykcji zagrożenia przestępczością zorganizowaną oraz terroryzmem. Z punktu widzenia działań kontrterrorystycznych szczególnie interesująca jest rola rozpracowań analitycznych dokonywanych przez Europol, w których ramach są gromadzone i przetwarzane szczegółowe dane (w tym osobowe) o zagrożeniach transgranicznych.

Dla skuteczności omawianych działań istotne znaczenie ma przede wszystkim liczba i jakość (aktualność oraz ważność) informacji przekazywanych do Europolu. Spójność systemu zarządzania informacjami ma znaczenie wtórne. Głównymi dostarczycielami informacji kryminalnych, a także odbiorcami danych wywiadowczych uzyskanych w wyniku analiz prowadzonych przez Europol, są państwa członkowskie. W gruncie rzeczy uzależnienie informacyjne Europolu od państw członkowskich należy uznać za całkowite. Dlatego rezultaty działań operacyjnych agencji są zależne od pełnej współpracy z państwami członkowskimi, która ma kluczowe znaczenie dla całokształtu działalności wywiadowczej Europolu. Bez wkładu informacyjnego państw członkowskich agencja ta nie jest w stanie spełnić oczekiwań pokładanych w niej przez Radę UE, Komisję Europejską czy państwa członkowskie.

W celu skutecznego wykonywania zadań Europol ma specjalną strukturę organizacyjną, własne kadry i finanse. Na tę strukturę składają się: kwatera główna w Hadze (centrala organizacji i krajowe biura łącznikowe) oraz krajowe jednostki Europolu państw członkowskich. W państwach trzecich znajdują się krajowe punkty kontaktowe do współpracy z Europolem.

Zadania Europolu są zbyt złożone i niespójne. Zasadnicze obowiązki wykonują oficerowie łącznikowi będący pracownikami instytucji krajowych. Powoduje to, że nie są oni ściśle powiązani z Europolem. Kierownictwo agencji nie posiada uprawnień do kontrolowania działalności oficerów łącznikowych państw członkowskich oraz ich nadzorowania. Podlegają oni wyłącznie odpowiednim przepisom wewnętrznym państwa delegującego, co, jak się wydaje, jest pewnego rodzaju słabością organizacyjną.

Personel Europolu ma charakter międzynarodowy i wywodzi się ze służb i instytucji krajowych odpowiedzialnych za zwalczanie przestępczości we wszystkich państwach członkowskich UE. Dzięki kierunkowej selekcji kandydatów Europol ma szanse zatrudniania ekspertów o wysokich kwalifikacjach zawodowych i językowych. Personel Europolu posługuje się wieloma językami, reprezentuje różne kultury i narodowości, co stanowi o jego wysokich walorach. Obecna struktura zatrudnienia

[7] Strona 84 *Traktatu o funkcjonowaniu Unii Europejskiej.*

w agencji ogranicza jednak jej skuteczność w zakresie działań operacyjnych, gdyż jedynie jedna trzecia jej kadr realizuje działania o charakterze operacyjnym. Pozostałe osoby wykonują zadania pomocnicze i administracyjne. Według oficjalnych danych tylko co siódmy pracownik jest analitykiem.

Z analizy obowiązujących przepisów wynika, że działania Europolu podlegają licznym rygorom prawnym (m.in. dotyczącym ochrony danych osobowych i informacji niejawnych). Odnosi się do nich także wiele gwarancji związanych z nadzorem i kontrolą. Działalność agencji jest poddana kontroli m.in.: Rady UE, Parlamentu Europejskiego, Komisji Europejskiej, kontroli sądowniczej Trybunału Sprawiedliwości UE, zarządu Europolu, parlamentów krajowych, ombudsmana[8] oraz Wspólnego Organu Nadzorczego. Wielość ośrodków nadzorujących działalność Europolu jest jego zasadniczą słabością. Wydaje się, że system politycznego nadzoru nad Europolem jest zanadto rozbudowany i mało elastyczny. Jest to spowodowane stałym wzmacnianiem kontroli nad tą instytucją, która w istocie skupia znacznie większe siły i środki, niż te kierowane do samych działań operacyjnych.

Przy ocenie skuteczności działań Europolu natrafia się na podstawową trudność dotyczącą niemożności określenia konkretnych skutków, jakie podjęte już działania wywarły na rzeczywisty stan zagrożenia terroryzmem. W wielu państwach członkowskich wciąż trudno dokonać wyraźnego rozróżnienia, czy wyniki działań zostały osiągnięte dzięki współpracy z Europolem, czy też są skutkiem bezpośredniej współpracy pomiędzy właściwymi służbami.

Omawiając źródła efektywności Europolu, należy wskazać na występującą od początku istnienia tej instytucji przewagę czynników politycznych nad czynnikami merytorycznymi w kształtowaniu jej zadań. Potencjał Europolu do zwalczania zagrożeń terrorystycznych jest pochodną woli politycznej państw członkowskich oraz Rady UE. Obecnie Europol działający jako agenda UE podlega większym wpływom Komisji Europejskiej. Z perspektywy unijnej polityki bezpieczeństwa agencja jest postrzegana jako uniwersalny instrument o charakterze zaradczym, który powinien być wykorzystywany – niekoniecznie w sposób skuteczny – do zwalczania wszelkich zagrożeń, zwłaszcza o istotnym znaczeniu dla opinii publicznej. Mówiąc inaczej, Europol jest wrażliwy na to, czego chcą politycy w UE. Państwom członkowskim i UE brakuje wspólnej wizji oraz konsekwencji odnośnie do rozwoju potencjału Europolu. W rezultacie nie ma on możliwości pełnego integrowania organizacyjnego tego rodzaju zadań oraz zdefiniowania wyraźnych zakresów współpracy z innymi agendami i organami UE. Wyraźnie widać, że agencja ta jest politycznie sterowana zarówno przez polityków unijnych, jak i polityków państw członkowskich, czego rezultatem jest jej pewna dysfunkcja. Z jednej strony są widoczne działania zmierzające do zwiększenia możliwości Europolu w zakresie zwalczania zagrożeń występujacych na terenie Europy, czego potwierdzeniem jest znaczna liczba aktów dotyczących Europolu przyjętych przez Radę UE od momentu jego utworzenia. Dzięki tym aktom następujące po sobie prezydencje w Radzie UE rozszerzały kompetencje Europolu o kolejne uprawnienia i obowiązki z zakresu zwalczania zagrożeń transgranicznych. Z drugiej zaś strony wprowadzano inicjatywy promujące zasady dostępności i bezpośredniego współdziałania, które w sposób naturalny marginalizują znaczenie Europolu jako platformy wielostronnej i multiagencyjnej współpracy. Przykładem tego typu inicjatyw są: *Decyzja Rady 2008/615/WSiSW z dnia 23 czerwca 2008 r. w sprawie intensyfikacji współpracy*

[8] Europejski Rzecznik Praw Obywatelskich – przyp. red.

transgranicznej, szczególnie w zwalczaniu terroryzmu i przestępczości transgranicznej (tzw. decyzja Prüm)[9] oraz *Decyzja ramowa Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej* (tzw. inicjatywa szwedzka)[10]. Na skutek tych inicjatyw dostęp do informacji i danych wywiadowczych mają jedynie strony bezpośrednio wymieniające te dane. Powoduje to ograniczenie możliwości wykorzystania tego typu informacji przez Europol w procesach analitycznych.

Najważniejszą przeszkodą w skuteczności działania Europolu jest wciąż ograniczone zaufanie do tej agencji praktyków, którzy z niechęcią przekazują informacje. W rezultacie jakość, aktualność, a nawet format danych operacyjnych otrzymywanych od państw członkowskich nie są tak dobre, jak być powinny. Problemem jest również brak informacji zwrotnych od państw członkowskich. Sytuację można porównać z „błędnym kołem", gdyż Europol nie jest w stanie skutecznie wywiązywać się z nałożonych na niego zadań bez otrzymywania odpowiednich informacji od służb krajowych. Działanie agencji jest proporcjonalne do zaangażowania państw członkowskich.

Należy pamiętać, że nie jest możliwe sprowadzenie dyskusji o skuteczności Europolu tylko i wyłącznie do tej instytucji. Przeciwdziałanie przestępczości zorganizowanej i terroryzmowi wymaga aktywności w wielu różnorodnych obszarach, dlatego też liczba służb oraz organów, które biorą udział w zapobieganiu tym zagrożeniom, jest duża. Dla porównania – w państwach członkowskich UE na płaszczyźnie krajowej działa przeszło 300 służb i instytucji wykonujących zadania w zakresie zapewniania bezpieczeństwa, które współpracują i wymieniają między sobą informacje. Europol jest umiejscowiony w międzynarodowym systemie zwalczania przestępczości na styku poziomów narodowego, unijnego i globalnego. Przepływ informacji jest tu elementem łączącym te trzy poziomy. Słabością omawianej struktury bezpieczeństwa jest wielość instytucji i mechanizmów o kompetencjach, które często nakładają się na siebie.

Podsumowując, Europol nie dysponuje odpowiednim potencjałem do realizacji zadań związanych ze zwalczaniem terroryzmu. Ze względu na koszty uzyskania i wrażliwość danych współpraca w tym zakresie jest oparta na systemie bezpośrednich relacji między służbami antyterrorystycznymi zainteresowanych państw, co przeczy ogólnej idei współpracy wielostronnej w ramach Europolu. Z całą pewnością działania antyterrorystyczne nie mogą być skutecznie koordynowane przy wykorzystaniu sieci oficerów łącznikowych agencji.

Przedstawiona konstatacja jest prawdopodobnie jedną z przyczyn poszukiwania w UE nowych propozycji współpracy, w tym tak problematycznych, jak idea powołania Europejskiej Agencji Wywiadu (*European Intelligence Agency*)[11].

Abstrakt

Artykuł jest próbą usystematyzowania wiedzy na temat roli Europolu w zwalczaniu terroryzmu międzynarodowego. Przedstawiono tu uwarunkowania wewnętrzne i zewnętrzne działań agencji, która wspiera pracę służb państw członkowskich ukierunkowaną na przeciwdziałanie zagrożeniom terrorystycznym. Podjęto też próbę oceny

[9] Dz.Urz. UE L 210 z 6 sierpnia 2008 r., s. 1.

[10] Dz.Urz. L 386 z 29 grudnia 2006 r., s. 89.

[11] Zob. P. Bryksa, *Wybrane zagadnienia polityki bezpieczeństwa wewnętrznego Unii Europejskiej. Szanse i zagrożenia dla Polski*, Warszawa 2008, BBN, s. 73.

efektywności tych działań, co jest zadaniem nadzwyczaj skomplikowanym z powodu specyfiki działania Europolu, zakresu działań prowadzonych przez tę agencje oraz jej umiejscowienia w systemie instytucjonalnym UE.

Abstract

The aim of the article is an attempt at systematizing the knowledge about the role of Europol's covert activities in combating international terrorism. The article contains a few examples of the Agency's activities supporting the tasks of services of EU Member States aiming at preventing terrorist threats. Moreover, the author has made an attempt to evaluate those activities which is a rather complicated task, taking into consideration the special role of the Europol's covert activities and its placement in the institutional system of the EU.

Mariusz Cichomski
Mirosław Kumanek

Administracyjne metody przeciwdziałania przestępczości – Nieformalna Sieć ds. Administracyjnego Podejścia do Przeciwdziałania i Zwalczania Przestępczości Zorganizowanej

Administracyjne podejście do przeciwdziałania przestępczości

Administracyjne podejście do przestępczości zakłada wykorzystywanie prawnoadministracyjnych instrumentów w celu eliminowania lub ograniczania sfer aktywności przestępczej między innymi przez stosowanie mechanizmów kontrolnych, prowadzenie odpowiedniej polityki wydawania pozwoleń, koncesji czy innego rodzaju decyzji administracyjnych, a także tworzenie skutecznego ustawodawstwa.

W procesie prawotwórczym założeniem administracyjnego podejścia do przestępczości jest wyposażenie organów administracji (centralnej i samorządowej) w narzędzia pozwalające nie tylko na ograniczanie podatności tych podmiotów na zagrożenia ze strony środowisk przestępczych (aspekt prewencyjny), lecz także zapewniające organom administracji instrumenty prawne służące ograniczeniu różnego rodzaju sfer działalności przestępczej.

Administracyjne podejście może więc polegać zarówno na samodzielnych działaniach prowadzonych przez organy administracji, jak i na ich bezpośredniej współpracy z organami ścigania. Przepisy administracyjne mogą również obligować adresatów tych przepisów do działań umożliwiających tym organom realizację funkcji kontrolnych (np. poprzez przekazywanie określonego rodzaju dokumentacji w związku z prowadzonymi transakcjami). Ponadto same organy ścigania w swojej działalności korzystają z instrumentów administracyjnych. Jednym z nich jest umożliwianie tym organom dostępu do baz danych będących w posiadaniu różnych organów administracji publicznej, w których znajdują się zasoby użyteczne w ściganiu sprawców przestępstw.

Korzystanie z instrumentów administracyjnych w celu ograniczania działalności przestępczej, w tym o charakterze zorganizowanym, może mieć charakter bieżący, wynikający z realizacji rutynowych zadań, lub być elementem kompleksowych, ukierunkowanych działań (uregulowań) mających zminimalizować zagrożenie daną formą przestępczości.

W Polsce przykładem ukierunkowanych działań administracyjnych zmierzających do eliminacji określonej sfery aktywności przestępczej była walka ze sprzedażą tzw. nowych narkotyków (dopalaczy). W tym celu wprowadzono m.in. możliwość karania osób wytwarzających lub wprowadzających do obrotu na terenie RP środki zastępcze[1], na podstawie decyzji właściwego państwowego inspektora sanitarnego, wydawanej na podstawie znowelizowanej w tym celu tawy o przeciwdziałaniu

[1] Substancje pochodzenia naturalnego lub syntetycznego w każdym stanie fizycznym lub produkt, roślina, grzyb lub ich część, zawierające taką substancję, używane zamiast środka odurzającego lub substancji psychotropowej lub w takich samych celach jak środek odurzający lub substancja psychotropowa, których wytwarzanie i wprowadzanie do obrotu nie jest regulowane na podstawie przepisów odrębnych; do środków zastępczych nie stosuje się przepisów o ogólnym bezpieczeństwie produktów.

narkomanii[2]. Wynikiem tych działań było przede wszystkim wyeliminowanie stacjonarnych punktów dystrybucji dopalaczy, do czego przyczyniła się nie tyle działalność organów ścigania, ile przedstawicieli innych podmiotów publicznych, w tym wypadku inspekcji wchodzących w skład administracji zespolonej.

Innym przykładem działań administracyjnych, tym razem opartych na stricte prawnych rozwiązaniach służących eliminowaniu podstaw do prowadzenia działalności przestępczej, było wdrożenie przepisów zmieniających system naliczania i odliczania podatku od towarów i usług w obrocie złomem, między innymi poprzez przesunięcie obowiązku odprowadzania podatku VAT ze sprzedawcy złomu na jego ostatecznego nabywcę, ograniczając tym samym możliwość ubiegania się przez sprzedawcę o zwrot podatku z urzędu skarbowego[3]. Założeniem tych działań było doprowadzenie do zmian w mechaniźmie rozliczania VAT i eliminacji nadużywanego przez podatników prawa do odliczenia podatku naliczonego za pomocą tzw. słupów, a także wystawiania na nie pustych faktur.

Należy podkreślić, iż to właśnie w sferze przestępczości ekonomicznej, zwłaszcza związanej z wyłudzeniami akcyzy i VAT oraz zaniżaniem należności publicznoprawnych, przepisy administracyjne odgrywają kluczową rolę w przeciwdziałaniu przestępczości, a także są podstawą prowadzenia przez organy podatkowe (kontrolne) działań zmierzających do ustalenia faktu wystąpienia nieprawidłowości w określonych transakcjach.

Administracyjne metody wpisują się w ideę zintegrowanego podejścia[4] do przestępczości zorganizowanej, wskazywanego na forum Unii Europejskiej jako kluczowe dla wzmocnienia zdolności poszczególnych krajów do przeciwdziałania i zwalczania tej formy przestępczości. Zintegrowane podejście zakłada z jednej strony pogłębianie współpracy między organami ścigania, czego wynikiem ma być zwiększenie ich skuteczności w zwalczaniu przestępczości (określane na poziomie UE jako czynności operacyjne, które należy jednak rozumieć szerzej, uwzględniając przede wszystkim czynności operacyjno-rozpoznawcze i dochodzeniowo-śledcze). Z drugiej strony podkreśla ono subsydiarne znaczenie wykorzystania metod alternatywnych[5], polegających na bezpośredniej współpracy organów ścigania z podmiotami zewnętrznymi – sektorem prywatnym (przede wszystkim ze zrzeszeniami branżowymi czy koncernami), organizacjami pozarządowymi, środkami masowego przekazu czy jednostkami naukowymi, a także z innymi organami administracji publicznej.

---

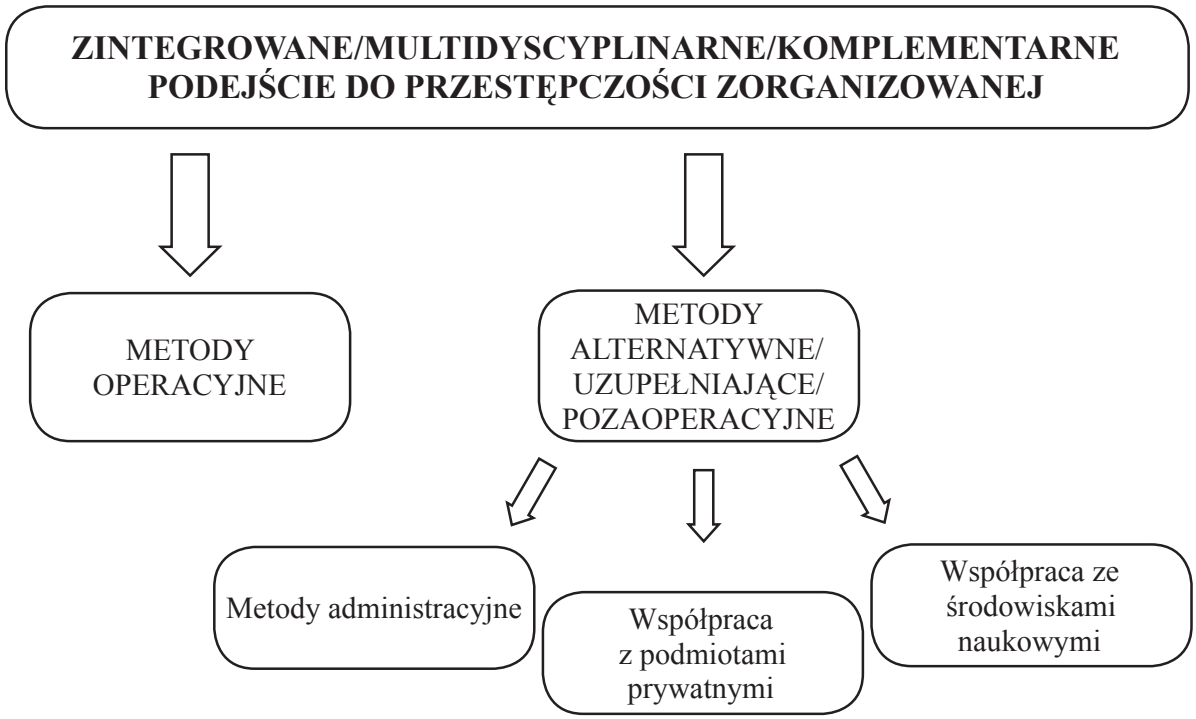
[2] *Ustawa z dnia 8 października 2010 r. o zmianie ustawy o przeciwdziałaniu narkomanii oraz ustawy o Państwowej Inspekcji Sanitarnej* (Dz.U. Nr 213, poz. 1396).

[3] *Ustawa z dnia 18 marca 2011 roku o zmianie ustawy o podatku od towarów i usług oraz ustawy – Prawo o miarach* (Dz.U. Nr 64, poz. 332).

[4] Wymiennie są też stosowane określenia: „podejście multidyscyplinarne" lub „podejście komplementarne".

[5] Analogicznie jak w przypadku zintegrowanego (multidyscyplinarnego, komplementarnego) podejścia, również w przypadku metod używa się zamiennych terminów: „uzupełniające" lub „pozaoperacyjne".

Podział zintegrowanego podejścia do przestępczości na elementy składowe, zgodnie z rozumieniem prezentowanym na forach UE, przedstawiono na poniższym rysunku.



Rysunek. Administracyjne podejście do przestępczości zorganizowanej w kontekście innych metod przeciwdziałania i zwalczania tej formy przestępczości.
Źródło: Opracowanie własne autorów.

Zasadność rozwijania administracyjnych metod przeciwdziałania przestępczości zorganizowanej została ujęta w Konwencji Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej[6] z 2000 r. Wskazano w niej między innymi na potrzebę wykorzystania środków o charakterze ustawodawczym i administracyjnym do zapobiegania przestępczości przez: tworzenie rejestrów osób prawnych, zakazy sprawowania kierowniczych stanowisk w podmiotach działalności gospodarczej przez osoby skazane za przestępstwa, tworzenie rejestrów osób objętych tymi zakazami, a także międzynarodową wymianę informacji zawartych we wspomnianych rejestrach[7].

Potrzeba wykorzystania administracyjnych środków w walce z przestępczością zorganizowaną została dostrzeżona również na forum Unii Europejskiej. Wprawdzie w decyzji w sprawie zwalczania przestępczości zorganizowanej z 2008 r.[8] nie wskazano wprost na konieczność rozwijania tego rodzaju metod, zobowiązano w niej jednak państwa członkowskie do działań wpisujących się w to podejście[9]. W przyjętym w 2009 r. przez Radę Europy Programie Sztokholmskim[10] natomiast wśród metod zapobiegania

[6] *Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r.* (Dz.U. z 2005 r. Nr 18, poz. 158, z późn. zm).

[7] Tamże, art. 31.

[8] *Decyzja Ramowa Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej* (Dz.Urz. UE L 300 z 11 listopada 2008 r.), s. 42.

[9] Na przykład w artykule 6.

[10] *Program Sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli* (*2010/C 115/01*) (Dz.Urz. UE C 115 z 4 maja 2010 r.), s. 1.

tej formie przestępczości wskazano na wykorzystanie środków administracyjnych i propagowanie współpracy między organami administracyjnymi, szczególnie w kontekście wymiany doświadczeń państw członkowskich w tym zakresie.

W 2009 r. na forum funkcjonującej wówczas grupy roboczej UE *Multidyscyplinary Group on Organized Crime* – MDG (obecnie GENVAL), przedstawiciele Holandii wystąpili z inicjatywą przeprowadzenia wśród państw członkowskich ankiety dotyczącej wykorzystywania instrumentów administracyjnych. Na podstawie uzyskanych wyników opracowano *Analizę administracyjnych i pozakarnych instrumentów w różnych państwach członkowskich oraz propozycje przyszłych działań*[11]. Także w tym dokumencie wskazano na potrzebę wymiany doświadczeń pomiędzy państwami.

O znaczeniu pozaoperacyjnych metod przeciwdziałania przestępczości zorganizowanej świadczy również ujęcie tego zagadnienia w *Strategii bezpieczeństwa wewnętrznego Unii Europejskiej*[12] z 2010 r.

Potrzeby rozwijania administracyjnych metod przeciwdziałania przestępczości zorganizowanej dostrzeżono również podczas przewodnictwa Węgier w Radzie Unii Europejskiej, przypadającego na pierwszą połowę 2011 r. Efektem działań było opublikowanie podręcznika pt. *Uzupełniające podejście i działania w zakresie przeciwdziałania i zwalczania przestępczości zorganizowanej. Zbiór przykładów dobrych praktyk Państw Członkowskich Unii Europejskiej*[13] stanowiącego zestaw innowacyjnych praktyk i instrumentów stosowanych w państwach członkowskich, które uzupełniają tradycyjne operacyjne metody działania wykorzystywane przez organy ścigania. Podręcznik jest wynikiem siedmiu miesięcy prac grupy ekspertów z Węgier, Polski[14], Belgii, Finlandii, Włoch, Holandii, Szwecji, Wielkiej Brytanii, a także Komisji Europejskiej, Europolu i Sekretariatu Rady, działających pod auspicjami Stałego Komitetu Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego – COSI.

Podczas przygotowań do objęcia przewodnictwa w Radzie UE w drugiej połowie 2011 r. Polska zadeklarowała chęć zaktualizowania wspomnianego podręcznika, a także wsparcie działań zmierzających do wzmocnienia wykorzystywania administracyjnych metod przeciwdziałania przestępczości zorganizowanej, czego przejawem było zaangażowanie w rozwój Nieformalnej Sieci ds. Administracyjnego Podejścia do Przeciwdziałania i Zwalczania Przestępczości Zorganizowanej.

Nieformalna Sieć ds. Administracyjnego Podejścia do Przeciwdziałania i Zwalczania Przestępczości Zorganizowanej

Podstawą do stworzenia Nieformalnej Sieci ds. Administracyjnego Podejścia do Przeciwdziałania i Zwalczania Przestępczości Zorganizowanej były konkluzje Rady UE ds. Sprawiedliwości i Spraw Wewnętrznych z 2010 r. w sprawie zwalczania

[11] *Analysis Administrative/Non-Penal Instruments in various Member States & Proposal Future Steps*, Brussels, 25 February 2010 (13460/2/09).

[12] *Strategia Bezpieczeństwa Wewnętrznego Unii Europejskiej – Dążąc do europejskiego modelu bezpieczeństwa,* Luksemburg 2010, Urząd Publikacji Unii Europejskiej.

[13] *Complementary approaches and actions to prevent and combat organized crime. A collection of good practice examples from EU Member States.*

[14] W pracach nad podręcznikiem Polskę reprezentował przedstawiciel Centralnego Biura Śledczego Komendy Głównej Policji.

przestępczości tzw. grup mobilnych[15]. Zawierały one m.in. wezwanie państw członkowskich i Komisji Europejskiej do uaktywnienia współpracy w ramach nieformalnej sieci punktów kontaktowych, właściwych w obszarze administracyjnych środków przeciwdziałania zjawisku mobilnych grup przestępczych, a także innych obszarów przestępczej działalności.

W konkluzjach określono główne zadania Sieci, do których zalicza się:

- promowanie administracyjnych metod zapobiegania przestępczości,
- zbadanie możliwości wzmocnienia wymiany informacji pomiędzy organami administracji i organami ścigania państw członkowskich UE, z wykorzystaniem istniejących instrumentów międzynarodowej wymiany informacji i uwzględnieniem ograniczeń w tym zakresie wynikających z ustawodawstwa obowiązującego w krajach członkowskich UE,
- szerzenie dobrych praktyk w stosowaniu administracyjnych metod zapobiegania przestępczości,
- proponowanie nowych inicjatyw w zakresie stosowania administracyjnego podejścia do przeciwdziałania i zwalczania przestępczości zorganizowanej,
- informowanie właściwych grup roboczych Rady UE ds. Sprawiedliwości i Spraw Wewnętrznych o wynikach swoich prac za pośrednictwem państw sprawujących przewodnictwo w Radzie UE,
- przeprowadzanie spotkań Sieci co najmniej raz na pół roku.

We wrześniu 2011 r., w trakcie polskiej prezydencji w Radzie UE, Stały Komitet Współpracy Operacyjnej w zakresie Bezpieczeństwa Wewnętrznego postanowił, że Nieformalna Sieć powinna uwzględniać administracyjne podejście nie tylko w celu zapobiegania działalności mobilnych grup przestępczych[16], lecz także pozostałych grup działających w innych obszarach przestępczości zorganizowanej, określonych przez Radę UE ds. Sprawiedliwości i Spraw Wewnętrznych jako priorytetowe, tj. narkotyków syntetycznych i nowych substancji psychoaktywnych, handlu ludźmi, cyberprzestępczości, nielegalnej migracji, nielegalnego przemytu narkotyków i towarów akcyzowych drogą morską z wykorzystaniem kontenerów, przestępczości zorganizowanej wywodzącej się z Bałkanów Zachodnich, a także z Afryki Zachodniej[17]. Podczas duńskiej prezydencji w Radzie UE, przypadającej na pierwszą połowę 2012 r., zakres ten został rozszerzony i odnosi się obecnie do przestępczości poważnej i zorganizowanej.

Posiedzeniom Nieformalnej Sieci przewodniczy kraj sprawujący w danym okresie prezydencję w Radzie UE wspólnie z Komisją Europejską. Nieformalna Sieć ustala plan swoich prac, uwzględniając ewentualne sugestie COSI oraz okresowo informuje COSI o realizowanych przedsięwzięciach.

Nieformalna Sieć koncentruje się na wymianie dobrych praktyk w zakresie szczególnie interesującym kraje członkowskie, a także na promowaniu wykorzystywania administracyjnych instrumentów zapobiegania przestępczości poważnej i zorganizowanej.

---

[15] *Council conclusions on the fight against crimes committed by mobile (itinerant) criminal groups*, 3051st Justice and Home Affairs Council meeting, Brussels, 2 and 3 December 2010.

[16] *Council conclusions on the fight against crimes...* definiują mobilne grupy przestępcze jako grupy przestępcze posiadajace szeroki obszar działania, również w wymiarze miedzynarodowym, systematycznie pozyskujące dobra poprzez kradzieże i oszustwa.

[17] *Council conclusions on setting EU's priorities for the fight against organised crime between 2011 and 2013*, 3096th Justice and Home Affairs Council meeting, Luxemburg, 9 and 10 June 2011.

Polska podczas swojej prezydencji wspólnie z Europolem zainicjowała pod koniec 2011 r. prace nad utworzeniem na potrzeby Nieformalnej Sieci, w ramach wirtualnej Platformy Ekspertów Europolu (*Europol Platform For Experts*), praktycznego narzędzia współpracy w postaci strony internetowej dedykowanej administracyjnemu podejściu do zapobiegania przestępczości zorganizowanej[18]. Prace nad stroną były prowadzone w 2012 r. przez przedstawicieli punktów kontaktowych Nieformalnej Sieci[19] tworzących tzw. wąską grupę ekspercką (*core group*), w której skład wchodzą przedstawiciele Polski[20], Belgii, Cypru, Holandii, Wielkiej Brytanii, Włoch oraz Komisji Europejskiej, Europolu i Eurojustu. Strona ta ma ułatwić członkom Nieformalnej Sieci bieżącą wymianę informacji (nie mogą one zawierać danych osobowych) oraz doświadczeń w stosowaniu administracyjnych metod przeciwdziałania przestępczości zorganizowanej. Współpraca ma być prowadzona zarówno poprzez bezpośrednie kontakty na forum Platformy, jak i umieszczanie na niej tematycznych materiałów.

W dłuższej perspektywie jest planowane umożliwienie dostępu do tej strony, poza przedstawicielami organów ścigania, również innym organom administracji czy reprezentantom środowisk naukowych prowadzącym badania nad przestępczością zorganizowaną. Platforma pozwala na wprowadzenie różnych poziomów uczestnictwa (zakresów dostępu), dlatego też możliwe jest częściowe włączanie do niej podmiotów zewnętrznych[21].

W listopadzie 2012 r., podczas cypryjskiej prezydencji Rady UE, strona dotycząca administracyjnego podejścia do zapobiegania i zwalczania przestępczości zorganizowanej na Platformie Ekspertów Europolu została oficjalnie udostępniona wszystkim członkom Nieformalnej Sieci.

Wyzwania

Rozwijanie administracyjnych metod przeciwdziałania przestępczości wiąże się z istotnymi wyzwaniami. Należy podkreślić zarówno różny poziom rozwoju tego rodzaju instrumentów w poszczególnych państwa członkowskich UE, jak i odmienny stosunek do korzystania z nich przedstawicieli organów ścigania.

Na gruncie krajowym szczególnie istotne pozostaje podjęcie działań służących zapoznaniu właściwych instytucji ochrony porządku prawnego z możliwościami rozwijania administracyjnych instrumentów zapobiegania przestępczości, a także z narzędziami wspierającymi międzynarodową wymianę doświadczeń w tym zakresie, jak strona dedykowana temu zagadnieniu na Platformie Ekspertów Europolu. Należy się jednak spodziewać, że w początkowej fazie funkcjonowania strony większość krajów UE, w tym Polska, będzie korzystać z doświadczeń krajów bardziej zaawansowanych we wprowadzaniu administracyjnego podejścia, tj. Belgii, Holandii i Wielkiej Brytanii.

---

[18] Jeszcze w czerwcu 2011 r. Konwencja Szefów Policji Europejskich przyjęła zalecenia odnoszące się między innymi do bardziej kreatywnego podejścia do zwalczania przestępczości zorganizowanej, wykraczającego poza tradycyjne metody dochodzeniowe organów ścigania i obejmującego środki administracyjne i zapobiegawcze.

[19] Polski punkt kontaktowy Nieformalnej Sieci został umiejscowiony w Wydziale Przeciwdziałania Zagrożeniom Terrorystycznym i Przestępczości Zorganizowanej Departamentu Nadzoru Ministerstwa Spraw Wewnętrznych.

[20] W pracach uczestniczy przedstawiciel Ministerstwa Spraw Wewnętrznych.

[21] Uzyskanie dostępu do uczestnictwa w wirtualnej platformie jest możliwe za pośrednictwem krajowego punktu kontaktowego, po weryfikacji dokonanej przez wąską grupę ekspercką i Europol.

Istotne pozostaje także dokonanie pogłębionej diagnozy zjawisk sprzyjających działalności zorganizowanych grup przestępczych (obszarów kryminogennych) w kontekście możliwości ich ograniczenia przy wykorzystaniu administracyjnych instrumentów, wraz ze wskazaniem ewentualnych środków rekomendowanych do przyjęcia lub zastosowania w tym zakresie.

W dłuższej perspektywie ważne jest również pozyskanie do prowadzenia współpracy w przedmiotowym zakresie partnerów spośród przedstawicieli administracji publicznej (spoza organów ścigania), a w dalszej kolejności również środowisk naukowych czy sektora prywatnego.

Z perspektywy rozwijania administracyjnych metod przeciwdziałania przestępczości zorganizowanej oraz wymiany międzynarodowych doświadczeń istotne znaczenie mają również przygotowywane obecnie założenia do holenderskiego projektu badawczego, którego celem jest analiza zakresu stosowania administracyjnych instrumentów zapobiegania przestępczości zorganizowanej, a także wymiana informacji między organami ścigania i strukturami administracyjnymi w wybranych państwach Unii Europejskiej, w tym w Polsce. Projekt ten ma być realizowany poprzez analizę istniejącego ustawodawstwa, a także nawiązanie kontaktów z przedstawicielami organów ścigania, administracji i środowisk naukowych.

Bibliografia

1. *Analysis Administrative/Non-Penal Instruments in various Member States & Proposal Future Steps, Brussels, 25 February 2010* (*13460/2/09*).
2. *Complementary approaches and actions to prevent and combat organized crime. A collection of good practice examples from EU Member States.*
3. *Council conclusions on the fight against crimes committed by mobile (itinerant) criminal groups, 3051st Justice and Home Affairs Council meeting,* Brussels, 2 and 3 December 2010.
4. *Council conclusions on setting EU's priorities for the fight against organised crime between 2011 and 2013, 3096th Justice and Home Affairs Council meeting,* Luxemburg, 9 and 10 June 2011.
5. *Decyzja Ramowa Rady 2008/841/WSiSW z dnia 24 października 2008 r. w sprawie zwalczania przestępczości zorganizowanej* (Dz.Urz. UE L 300 z 11 listopada 2008 r.).
6. *Konwencja Narodów Zjednoczonych przeciwko międzynarodowej przestępczości zorganizowanej przyjęta przez Zgromadzenie Ogólne Narodów Zjednoczonych dnia 15 listopada 2000 r.* (Dz.U. z 2005 r. Nr 18, poz. 158, z późn. zm).
7. *Ustawa z dnia 8 października 2010 r. o zmianie ustawy o przeciwdziałaniu narkomanii oraz ustawy o Państwowej Inspekcji Sanitarnej* (Dz.U. Nr 213, poz. 1396).
8. *Ustawa z dnia 18 marca 2011 roku o zmianie ustawy o podatku od towarów i usług oraz ustawy – Prawo o miarach* (Dz.U. Nr 64, poz. 332).
9. *Program Sztokholmski – Otwarta i bezpieczna Europa dla dobra i ochrony obywateli* (*2010/C 115/01*) (Dz.Urz. UE C 115 z 4 maja 2010 r.).
10. *Strategia Bezpieczeństwa Wewnętrznego Unii Europejskiej – Dążąc do europejskiego modelu bezpieczeństwa*, Luksemburg 2010, Urząd Publikacji Unii Europejskiej.

Abstrakt

Administracyjne podejście do przestępczości zorganizowanej polega na wykorzystywaniu prawnoadministracyjnych instrumentów w celu eliminowania lub ograniczania sfer aktywności przestępczej. Stanowi ono subsydiarne narzędzie względem innych metod walki z tego rodzaju przestępczością i wpisuje się w ideę zintegrowanego podejścia do przestępczości zorganizowanej, zakładającego z jednej strony pogłębianie wzajemnej współpracy między organami ścigania, z drugiej zaś uwzględniającego uzupełniające znaczenie metod alternatywnych, zakładających bezpośrednią współpracę organów ścigania z podmiotami zewnętrznymi.

Rozwijanie metod administracyjnych, wskazywanych na forum Unii Europejskiej jako kluczowe dla wzmocnienia zdolności poszczególnych krajów w zakresie przeciwdziałania i zwalczania przestępczości zorganizowanej, wiąże się z istotnymi wyzwaniami, w tym w kontekście zróżnicowanego poziomu rozwoju tego rodzaju instrumentów w poszczególnych państwach oraz rzeczywistego stosunku służb do korzystania z tego rodzaju instrumentów.

Mając powyższe na uwadze, w okresie polskiego przewodnictwa w Radzie UE Polska zaangażowała się w popularyzowanie administracyjnych metod przeciwdziałania przestępczości na forum unijnym. Przejawem tych działań był aktywny udział w Nieformalnej Sieci ds. Administracyjnego Podejścia do Przeciwdziałania i Zwalczania Przestępczości Zorganizowanej oraz w pracach nad utworzeniem, w ramach wirtualnej Platformy Ekspertów Europolu, praktycznego narzędzia współpracy w postaci strony dedykowanej temu zagadnieniu.

Abstract

The administrative approach in preventing and combating organized crime involves the use of administrative legal instruments to eliminate or reduce criminal activity. It is a tool subsidiary to other methods of combating crime. It also corresponds with the concept of an integrated approach to organized crime, which includes, on the one hand, tightening the cooperation between law enforcement and, on the other hand, the use of alternative methods, provided that law enforcement authorities and external entities cooperate directly.

The development of administrative methods of preventing and combating organized crime, has been considered by the EU as crucially important in strengthening the capacities of individual countries to prevent and combat organized crime. However, this also entails considerable challenges, especially when it comes to various levels of development of these methods across the EU as well as their actual use by law enforcement authorities in various EU countries.

Therefore, Poland, during its EU Presidency, was engaged in promoting the development of administrative methods aimed at preventing and combating organized crime by active participation in the Informal Network of Contact Points for Administrative Approach in Preventing and Combating Organized Crime as well as in the development of a practical tool of cooperation on the Europol Platform For Experts.

Dariusz Pożaroszczyk

Federalny Urząd Ochrony Konstytucji – zadania i charakterystyka zwalczanych zagrożeń[1]

Federalny Urząd Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV) jest największą służbą specjalną Republiki Federalnej Niemiec[2]. Służba ta ma swoją siedzibę w Kolonii oraz oddział w Berlinie. Oprócz BfV, który posiada kompetencje ogólnokrajowe, w Niemczech funkcjonują także Krajowe Urzędy Ochrony Konstytucji (Landesbehörden für Verfassungsschutz – LfV), działające na poziomie landów. W związku z federalnym ustrojem państwa niemieckiego[3], LfV nie są podporządkowane organizacyjnie ani kompetencyjnie BfV[4].

Federalny Urząd Ochrony Konstytucji został utworzony 7 listopada 1950 r.[5] na podstawie ustawy Bundesverfassungsschutzgesetz (BVerfSchG)[6]. Aż do początku lat 90. XX wieku, w związku z podziałem Niemiec, BfV działało legalnie jedynie na terenie Republiki Federalnej Niemiec – RFN (Bundesrepublik Deutschland – BRD)[7]. Odpowiednikiem BfV w dziedzinie kontrwywiadu i bezpieczeństwa wewnętrznego na obszarze Niemieckiej Republiki Demokratycznej – NRD (Deutsche Demokratische Republik – DDR) było utworzone w lutym 1950 r. Ministerstwo Bezpieczeństwa Państwowego Niemieckiej Republiki Demokratycznej (Ministerium für Staatssicherheit – MfS), znane jako Stasi[8]. Do 1955 r. BfV wykonywało powierzone mu zadania pod kontrolą Sił Sojuszniczych, a jego podstawowa działalność była wymierzona w wywiady państw komunistycznych. Upadek reżimu hitlerowskiego i istnienie do 1949 r.

---

[1] Opisane w artykule zadania i podstawowe zagrożenia zwalczane przez BfV zostały zaczerpnięte z oficjalnej strony Federalnego Urząd Ochrony Konstytucji, http://www. verfassungsschutz.de/de/arbeitsfelder [dostęp: 30 III 2013].

[2] Oprócz Federalnego Urzędu Ochrony Konstytucji niemieckimi służbami specjalnymi są Federalna Służba Wywiadowcza (Bundesnachrichtendienst – BND), wywiad cywilny i Służba Ochrony Sił Zbrojnych (Amt für den Militärischen Abschirmdienst – MAD), pełniąca funkcję kontrwywiadu wojskowego. Zob. J. Gawryszewski, *Służby specjalne w Republice Federalnej Niemiec,* „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 6, s. 11–22.

[3] Więcej o systemie federalnym panującym w Niemczech zob. w: A. Schneider*, Staatsbürger-, Gesetzes- und Berufskunde für Fachberufe im Gesundheitswesen*, Berlin 2003, Springer, s. 30–32; *Föderalismus in Deutschland*, K. Detterbeck, K. Renzsch, W. Schieren (red.), München 2010, Oldenbourg.

[4] Zob. § 5 *Bundesverfassungsschutzgesetz vom 20. Dezember 1990 (BGBl. I S. 2954, 2970), das zuletzt durch Artikel 2 des Gesetzes vom 20. August 2012 (BGBl. I S. 1798) geändert worden ist*, określony jako Abgrenzung der Zuständigkeiten der Verfassungsschutzbehörden, tj. paragraf formułujący rozdzielenie kompetencji między Federalny Urząd Ochrony Konstytucji a Krajowe Urzędy Ochrony Konstytucji.

[5] Dwie pozostałe niemieckie służby specjalne powstały w roku 1956.

[6] Ustawa została uchwalona 27 września 1950 r.

[7] W Polsce Republika Federalna Niemiec do układu PRL–RFN z 7 grudnia 1970 r. była określana jako Niemiecka Republika Federalna (NRF).

[8] W tym miejscu należy zauważyć, że Stasi będące w dużej mierze kalką KGB posiadało znacznie szerszy zakres działania niż BfV. W ramach Stasi funkcjonowały, nieobecne w strukturze BfV, Główny Zarząd Wywiadu (Hauptverwaltung Aufklärung) oraz IX Główny Wydział (Hauptabteilung IX – HA IX) mający uprawnienia dochodzeniowo-śledcze.

okupacyjnych stref alianckich na terenie zachodnich landów miało istotny wpływ na określenie kompetencji powstałej pięć lat po zakończeniu II wojny światowej BfV.

Po proklamowaniu w 1949 r. utworzenia dwóch państw niemieckich – RFN i NRD – przedstawiciele państw zachodnich zaczęli dostrzegać potrzebę odtworzenia niemieckich służb specjalnych na terytorium, które dotyczczas znajdowało się pod ich wpływami. Równocześnie jednak – mimo świadomości zagrożeń, jakie niosło za sobą sąsiedztwo NRD, sojusznika ZSRR – obawiali się utworzenia organu, którego szeroki zakres kompetencji mógłby stać się zagrożeniem dla nowych, demokratycznych i liberalnych wartości stanowiących podstawy RFN[9]. Wynikiem tych sprzecznych dążeń jest paragraf 2 ustawy BVerfSchG, w którym wyrażono zakaz, tzw. Trennungsgebot (w rozwiniętej postaci określany jako Trennungsgebot zwischen Nachrichtendiensten und Polizei)[10]. Jest on obecnie uznawany za podstawową zasadę niemieckiego systemu bezpieczeństwa i zakłada pozbawienie służb specjalnych uprawnień policyjnych, przy pozostawieniu im roli czysto informacyjnej[11]. Trennungsgebot jest traktowany jako reakcja na nadużycia i zbrodnie hitlerowskiej Geheime Staatspolizei[12]. Uczynienie z BfV służby specjalnej o charakterze czysto informacyjnym było także nawiązaniem do rozwiązań funkcjonujących w Republice Weimarskiej, w której ówczesny odpowiednik BfV, tj. działający w latach 1920–1929 Reichskommissar für Überwachung der öffentlichen Ordnung (Komisarz Rzeszy do spraw kontroli porządku publicznego), również nie miał uprawnień procesowych. Ponadto nieprzyznanie BfV uprawnień policyjnych wyraźnie odróżniało tę służbę od enerdowskiej Stasi[13].

Konsekwencją zakazu wynikającego z § 2 wyżej wymienionej ustawy jest redakcja § 3 ustawy, w którym wymieniono zadania BfV. Zgodnie z tym przepisem BfV jest organem właściwym w zakresie zbierania informacji, szczególnie wiadomości i przekazów o osobach, które podejmują działania skierowane przeciwko demokratycznemu porządkowi, bytowi i bezpieczeństwu zarówno całego kraju (przez który należy rozmieć państwo niemieckie jako całość), jak i poszczególnych landów. Służba zbiera także informacje o osobach zmierzających do bezprawnego utrudniania funkcjonowania konstytucyjnych organów Niemiec oraz osobach, których celem są członkowie tych organów. BfV zdobywa również dane na temat działalności obcych sił oraz o ruchach

---

[9] Wyrazem tych sprzecznych odczuć był tak zwany „Polizeibrief", pismo aliantów zachodnich do Parlamentarische Rat (zgromadzenia konstytucyjnego ówczesnych Niemiec Zachodnich) z 14 kwietnia 1948 r. Pismo to jest uważane za „miejsce" narodzin tzw. Trennungsgebot.

[10] J. Singer, *Das Trennungsgebot – Teil 1: Politisches Schlagwort oder verfassungsrechtliche Vorgabe?,* „Die Kriminalpolizei" 2006, nr 3, s. 85–86; D. Kugelmann, *Polizei und Ordnungsrecht,* Berlin 2011, Springer, s. 52.

[11] Zasada ta powoduje, że zakres uprawnień BfV jest wyraźnie węższy od kompetencji jego polskiego odpowiednika, Agencji Bezpieczeństwa Wewnętrznego, który oprócz realizacji zadań informacyjnych ma także uprawnienia dochodzeniowo-śledcze. Ostatnio z powodu wzrostu przestępczości, zwłaszcza przestępczości o charakterze terrorystycznym i zorganizowanym, dochodzi do intensywnego rozwoju prawa karnego. Ewolucja niemieckiego systemu ścigania karnego prowadzi do coraz wyraźniejszego zacierania się różnic między służbami policyjnymi a specjalnymi. Zob. H.H. Kühne, *Eine systematische Darstellung des deutschen und europäischen Strafverfahrensrecht,* Heidelberg 2011, s. 245; V. Krey, *Kriminalitätsbekämpfung um jeden Preis Innere Sicherheit durch kontinuierliche Ausweitung des Bereichs verdeckter Ermittlungen*, „Rechtspolitisches Forum" 2003, nr 9, s. 25–26.

[12] W 1946 r. Gestapo zostało uznane przez Międzynarodowy Trybunał Wojskowy w Norymberdze za organizację przestępczą, winną ludobójstwa i zbrodni wojennych. Zob. więcej J. Delarue, *The Gestapo: A History of Horror*, Mervyn Savill (tłum.), New York 2008.

[13] Wydziałem śledczym Stasi był Hauptabteilung IX (HA IX). Zob. K. Mackrakis, *East German Foreign Intelligence: Myth, Reality and Controversy*, New York 2009, s. 1–20.

i ugrupowaniach, które planują posłużyć się przemocą w celu zmiany konstytucyjnego porządku, a także zagrażają międzynarodowej pozycji Niemiec. W kręgu zainteresowania urzędu znajdują się również dążenia skierowane przeciwko ideom i postanowieniom traktatów międzynarodowych, dotyczących zwłaszcza pokojowego współistnienia narodów. Dodatkowym zadaniem BfV jest sprawdzanie osób, którym ze względu na interes publiczny zostaną powierzone obowiązki, z którymi jest związany dostęp do tajemnicy państwowej. Do kompetencji urzędu należy również ochrona bezpieczeństwa przemysłowego. Działania z tym związane są ukierunkowane na przeciwdziałanie sabotażowi gospodarczemu. Federalny Urząd Ochrony Konstytucji podejmuje ponadto działania mające na celu ograniczenie proliferacji broni masowego rażenia.

Kluczowym słowem użytym w § 3 ustawy jest termin „„Bestrebungen", który należy przetłumaczyć jako „dążenia". Używając tego określenia, ustawodawca niemiecki wskazuje, że BfV nie jest uprawniony do podejmowania działań przeciwko osobom wyrażającym własne, nawet niepopularne poglądy. Reakcji BfV nie może uruchomić niechęć danego obywatela do wartości wyrażonych w niemieckiej ustawie zasadniczej. Podstawą podjęcia określonych kroków przez BfV mogą być dopiero rzeczywiste i realne działania sprzeczne z porządkiem prawnym[14].

W ramach normatywnie wyznaczonych przez § 3 ustawy zadań i celów, praktyka największej niemieckiej służby specjalnej jest kształtowana przez obiektywne warunki społeczne, gospodarcze i historyczne[15]. Wymienione uwarunkowania powodują, że w obszarze prawnie określonych kierunków zainteresowania działania BfV są wymierzone w konkretne zjawiska, odznaczające się szczególnym niebezpieczeństwem dla państwa niemieckiego. Zagrożeniami tymi są ekstremizm lewicowy i prawicowy, ruchy narodowowyzwoleńcze skupiające środowiska imigrantów, ruch islamistyczny i towarzyszący mu terroryzm islamski, działalność obcnych wywiadów, szczególnie rosyjskiego i chińskiego, a także organizacja scjentologiczna[16].

Ukierunkowany na realizację utopijnych koncepcji marksistowskich, trockistowskich i maoistowskich oraz innych rozmaitych idei anarchistycznych ruch lewacki ma w Niemczech długą i krwawą tradycję[17], stanowiąc realne zagrożenie dla wartości demokratyczno-liberalnych. Z danych prezentowanych przez BfV wynika, że w 2010 r. na terenie państwa niemieckiego doszło do 944 aktów przemocy popełnionych przez członków różnych organizacji lewicowych (w 2009 r. takich przypadków zanotowano

---

[14] *Islamismus aus der Perspektive des Verfassungsschutzes,* Köln 2008, Bundesamt für Verfassungsschutz, s. 5.

[15] W literaturze politologicznej poświęconej zagadnieniom bezpieczeństwa pisze się o otoczeniu służb, przez które rozumie się wszystkie czynniki wpływające na działania służby. Zob. J. Gryz, *Teoretyczne aspekty funkcjonowania służb specjalnych RP*, „Studia i Materiały" 2012, nr 1, s. 90. Autor wyróżnia otoczenie: prawne, programowania strategicznego, ekonomiczne, technologiczne, kulturowe, polityczne. Wydaje się, że do powyższego katalogu można dodać także otoczenie społeczne.

[16] Zob. strona internetowa Bundesamt für Verfassungsschutz, http://www.verfassungsschutz.de. [dostęp 10 X 2012].

[17] Najbardziej znaną terrorystyczną organizacją lewicową w Niemczech była tak zwana Frakcja Czerwonej Armii (Rote Armee Fraktion – RAF) działająca z różnym nasileniem od lat 60. XX wieku aż do początku lat 90. XX wieku. Członkowie tej przestępczej organizacji byli odpowiedzialni za co najmniej 34 zabójstwa, głównie policjantów i amerykańskich żołnierzy. Od lat 70. grupa ta współpracowała także z palestyńskimi terrorystami z ugrupowania Fatah. Zob. więcej S. Schweizer, *Rote Armee Fraktion-Ideologie und Strategie im Wandel*, Bremen 2009, Bremen Europ. Hochsch; S. Colvin, *Ulrike Meinhof and West German Terrorism: Language, Violence, and Identity*, New York 2009, Rochester. O porwaniach dokonywanych przez członków RAF piszą również J. Kaczmarek i M. Kierszka w: J. Kaczmarek, M. Kierszka, *Porwania dla okupu,* Warszawa 2008, ABC, s. 22–23.

1115). Dla wielu przedstawicieli ruchów lewackich stosowanie agresji fizycznej to jedyny środek umożliwiający przekształcenie społeczeństwa oraz przerwanie rzekomej opresji i wyzysku właściwych dla systemu kapitalistycznego[18]. Do najniebezpieczniejszych niemieckich organizacji lewackich, zalicza się obecnie: Deutsche Kommunistische Partei (DKP); Kommunistische Partei Deutschlands (KPD), Marxistisch-Leninistische Partei Deutschlands (MLPD), Rote Hilfe e.V. (RH), Antifaschistischen Aktion (AA), organizację pod nazwą Die Linke oraz ruch trockistowski, którego głównym przedstawicielem jest ugrupowanie o nazwie marx21[19]. Łączna liczba osób zrzeszonych w około 115 niemieckich, skrajnie lewicowych, organizacjach przekracza 32 tys., z czego ponad jedna piąta należy do organizacji, które stosują i propagują przemoc[20]. Przytoczone liczby, obrazujące skalę lewackiego ekstremizmu, wyjaśniają fakt, dlaczego motywowane ideologią komunistyczną i anarchistyczną czyny przestępne są od wielu lat fenomenem kryminologicznym w Niemczech. Okoliczność ta wymusza na BfV poddanie ruchów lewackich stałej obserwacji i infiltracji.

W kontekście zagrożeń politycznemu pluralizmowi, demokracji i rządom prawa charakter zbliżony do organizacji lewicowych ma, znajdujący się na ideologicznie przeciwległym biegunie, ekstremizm prawicowy. Pojęcie „skrajna (radykalna) prawica" jest przykładem terminu zbiorczego, obejmującego wiele zróżnicowanych ruchów i prądów, takich jak: ugrupowania faszystowskie, nazistowskie i antysemickie[21]. Prawicowy ekstremizm zabarwiony ideologią o wyższości rasy aryjskiej jest ruchem immanentnie sprzecznym z wyrażoną w artykule 3 niemieckiej Ustawy Zasadniczej ideą równości wszystkich obywateli[22]. Środowisko prawicowych ekstremistów w Niemczech nie tworzy skonsolidowanego ruchu skupionego wokół jednej organizacji. Federalny Urząd Ochrony Konstytucji szacuje, że na terenie państwa działa około 200 organizacji neofaszystowskich[23] grupujących blisko 26 tys. członków. Liczba aktów przemocy popełnionych z motywów neofaszystowskich w ostatnich latach wynosi blisko 800[24]. Oprócz niewiel-

---

[18] R. Karapin, *Protest Politics in Germany: Movements on the Left and Right Since The 1960s*, London 2007, The Pennsylvanian State University, s. 23–24.

[19] *Faltblatt „Feinde der Demokratie – Linksextremisten",* Potsdam 2010, Ministerium des Innern des Landes Brandenburg Stand, s. 21; U. Backes, P. Moreau, *Communist and Post-Communist Parties in Europe*, Göttingen 2008, Vanderhoeck & Ruprecht, s. 74–82.

[20] Strona internetowa BfV, zakładka Linksextremismus, http://www. verfassungsschutz.de/de/arbeitsfelder/af_linksextremismus [dostęp 10 X 2012].

[21] O różnicach i podobieństwach między poszczególnymi odłamami ekstremizmu prawicowego zob. U. Backes, *„Rechtsextremismus" Konzeptionen und Kontroversen,* w: *Rechtsextreme Ideologien in Geschichte und Gegenwart*, U. Backes (red.), Köln, Weimar 2003, s. 16–52.

[22] C. Dressler, *Die Wehrhafte Demokratie und der Rechtsextremismus: Wie sich der Staat gegen seine Verfassungsfeinde wehrt*, Hamburg 2012, s. 4.

[23] W 2010 r. było ich 219, w 2009 r. natomiast 195, zob. http://www.verfassungsschutz.de [dostęp: 10 X 2012].

[24] W 2009 r. odnotowano 891 takich czynów, w 2010 r. natomiast 762. Zob. http://www. verfassungsschutz.de [dostęp 10 X 2012]. Na przełomie 2011 i 2012 r. opinią publiczną w Niemczech wstrząsnęła sprawa skrajnie prawicowej organizacji o nazwie Narodowosocjalistyczne Podziemie (Nationalsozialistischer Untergrund – NSU). Organizacja działała w Niemczech w latach 1998–2011. W tym okresie jej członkowie popełnili prawdopodobnie co najmniej dziesięć morderstw, a także dopuścili się wielu innych aktów terroru i przemocy. Ich ofiarami byli głównie imigranci z Turcji. Członkowie grupy są odpowiedzialni także za zabójstwo w 2007 r. policjantki Michèle Kiesewetter. Fakt, iż BfV od wielu lat posiadał informatorów w otoczeniu NSU, a mimo to nie potrafił przerwać działania tej organizacji, doprowadził w lipcu 2012 r. do odejścia ze stanowiska Dyrektora BfV Heinza Fromma, zob. *Nach Pannen bei NSU-Ermittlungen Verfassungsschutzpräsident Fromm tritt zurück* [online], Süeddeutsche.de z 2 lipca 2012,

kich ugrupowań działających na pograniczu systemu społecznego, a często poza nim, do 2011 r. ze skrajną prawicą związane były dwie ogólnoniemieckie partie polityczne: założona 28 listopada 1964 r. w Hanowerze Nationaldemokratische Partei Deutschlands (NPD) i, nieco mniejsza, utworzona w 1971 r. jako związek, a w 1987 r. przekształcona w partię, Deutsche Volksunion (DVU). Od 1 stycznia 2011 r. wymienione partie połączyły się, tworząc Nationaldemokratische Partei Deutschlands – Die Volksunion.

Kolejnym zagrożeniem, z jakim muszą się zmagać niemieckie służby specjalne, są różnego rodzaju zagraniczne organizacje ekstremistyczne. Sytuacja gospodarcza państwa niemieckiego jest powodem napływu co roku ogromnej liczby obcokrajowców[25]. Obecnie w Niemczech żyje około 7,5 mln imigrantów, co stanowi 8,8 proc. całej populacji[26]. Większość cudzoziemców osiedlających się w Niemczech poszukuje miejsca dającego szansę na dostatnie i spokojne życie. Istnieje jednak liczna grupa przybyszów, która nie zrywa kontaktów z różnymi organizacjami czynnie działającymi w państwach ich pochodzenia. Ludzie ci wykorzystują Niemcy jako bazę służącą do zaopatrzenia i przygotowania akcji przeprowadzanych przez ugrupowania, z którymi są związani. Według szacunków BfV około 26,5 tys. imigrantów jest powiązanych z zagranicznymi organizacjami ekstremistycznymi i terrorystycznymi. Jedną z groźniejszych organizacji terrorystycznych posiadających silne wsparcie wśród napływowej ludności niemieckiej jest założona 27 listopada 1978 r. Partia Pracujących Kurdystanu (PPK), znana także jako KADEK lub Kongra-Gel. Celem tego lewicowego ugrupowania jest utworzenie niepodległego państwa kurdyjskiego. Od wielu lat prowadzi ono regularną wojnę o charakterze partyzanckim z państwem tureckim. Organizacja ta jest również zamieszana w handel narkotykami i przemyt broni. Stosowane przez PPK metody spowodowały, iż jest ona uznawana przez wiele krajów oraz Unię Europejską za ugrupowanie terrorystyczne[27]. W Niemczech od 26 listopada 1993 r. działalność PPK jest zabroniona[28].

Na terenie Niemiec działają także ekstremistyczne organizacje tureckie, w tym także wyrażające ideologię lewicową. Aktywność tych grup jest wymierzona przeciwko legalnym władzom państwa tureckiego, a także Unii Europejskiej oraz polityce imigracyjnej Niemiec. Największymi nielegalnymi organizacjami tureckimi są, uznawane przez UE i rząd turecki za organizacje terrorystyczne, Revolutionären Volksbefreiungspartei-Front (DHKP-C) oraz powiązana z nim Anatolische Föderation. Federalny Urząd Ochrony Konstytucji zwraca także uwagę, że wśród mniejszości tureckiej silne wpływy mają ugrupowania nacjonalistyczne.

---

http://www.sueddeutsche.de/politik/nach-pannen-bei-nsu-ermittlungen verfassungsschutzpraesident-fromm-tritt- zurueck-1.1399028 [dostęp: 10 X 2012].

[25] Zob. przykładowe dane umieszczone na stronie internetowej http://www.tatsachen-ueber-deutschland.de. [dostęp: 10 X 2012].

[26] http://www.verfassungsschutz.de/. [dostęp: 10 X 2012]. Z kolei R. Geißler podaje, że w Niemczech na początku 2005 r. żyło 6,7 mln cudzoziemców, co stanowiło 8,1 proc. całej populacji. Zob. R. Geißler, *Die Sozialstruktur Deutschlands: Zur gesellschaftlichen Entwicklung mit einer Bilanz zur Vereinigung. Mit einem Beitrag von Thomas Meyer,* Wiesbaden 2010, VS Verlag für Sozialwissenschaften, s. 231.

[27] Na marginesie warto dodać, że najbardziej znany lider PPK Abdullah Öcalan został pojmany w 1999 r. w Kenii w wyniku wspólnej akcji CIA, Milli İstihbarat Teşkilatı (Narodowej Służby Wywiadowczej – wywiadu tutreckiego) i Mossadu.

[28] Powodem zakazania PPK działalności były akty przemocy wymierzone w mieszkającą w Niemczech mniejszość turecką, których dopuszczali się jej członkowie. Były to groźby, pobicia, podpalenia, a nawet zabójstwa. Więcej o działalności PPK w Niemczech zob. T. Schwarz, *Bedrohung, Gastrecht, Integrationspflicht: Differenzkonstruktionen im deutschen Ausweisungsdiskurs*, Bielefeld 2010, s. 131–135.

Mniejszościami etnicznymi, które również poddane są zwiększonej czujności niemieckich służb, są diaspora irańska oraz mniejszości azjatyckie powiązane z działającymi w Azji licznymi ruchami separatystycznymi. Jako organizację szczególnie niebezpieczną BfV wymienia powstałe w 1976 r. ugrupowanie Tygrysów Wyzwolenia Tamilskiego Ilamu (LTTE). Jest to organizacja wojskowa o charakterze partyzanckim, żądającą utworzenia w północnej części Sri Lanki niepodległego tamilskiego państwa Ilamu. W maju 2009 r. organizacja poniosła ogromną klęskę i teoretycznie 17 maja ogłosiła zawieszenie broni. Biorąc jednak pod uwagę, iż podłoże konfliktu tamilsko – syngaleskiego nie wygasło, a wręcz przeciwnie[29] – nasila się, BfV uznaje, że LTTE przechodzi obecnie fazę głębokiej reorganizacji i prawdopodobnie szykuje się do podjęcia nowych działań. W Niemczech osoby powiązane z LTTE dążą do zdobycia środków finansowych, przy czym często wykorzystują nielegalne metody, m.in. handel narkotykami.

Nie lekceważąc zagrożeń wiążących się opisanymi ruchami wywrotowymi, należy uznać, że obecnie w Niemczech oraz w całym zachodnim świecie, największe zagrożenie dla wolności, demokracji i humanizmu stanowi islamizm[30] oraz towarzyszący mu, naznaczony ideologią dżihadu, terroryzm. Dane podawane przez BfV wskazują, iż w Niemczech przebywa od 3,8 do 4,3 mln muzułmanów. Z tej grupy, według wskazań z 2010 r., 37 470 było członkami 29 organizacji islamistycznych działających wówczas w Niemczech. Należy podkreślić, że zdecydowana większość niemieckiej społeczności muzułmańskiej nie jest zaangażowana w działalność, która zagraża bezpieczeństwu wewnętrznemu. Równocześnie jednak liczebność diaspory muzułmańskiej powoduje, że jest ona mocno zróżnicowana. Fakt ten wpływa z kolei na niejednorodność organizacji islamskich działajacych w Niemczech. Na jednym krańcu znajdują się ugrupowania promujące religię islamską przez prowadzenie działalności kulturalnej i edukacyjnej[31], na drugim zaś sytuują się ruchy otwarcie wzywające do przemocy i gloryfikujące akty terroru. Również i to ostatnie środowisko nie jest jednorodne i obejmuje zarówno większe organizacje utrzymujące kontakty z ugrupowaniami terrorystycznymi z zagranicy oraz małe wyizolowane grupy fanatyków, jak i osoby działające pojedynczo[32]. Do organizacji terrorystycznych działających na terenie Niemiec niemieckie służby specjalne zaliczają przede wszystkim Al-Kaidę

[29] Zob. informacje dotyczące zbrodni wojennych popełnionych w czasie wojny domowej na Sri Lance dostępne na stronie http://en.wikipedia.org/wiki/Alleged_war_crimes_during_the_Sri_Lankan_Civil_War [dostęp: 10 X 2012].

[30] Islamizm jest odłamem (odmianą) fundamentalizmu islamskiego. W perspektywie islamizmu islam jest nie tylko religią, ale i doktryną polityczna. Zob. J. Esposito, *Political Islam: Beyond the Green Menace*[onlone], http://islam.uga.edu/espo.html. [dostęp: 10 X 2012]. W nauce podkreśla się, że termin „islamizm" jest pojęciem kontrowersyjnym i niejednorodnym.

[31] Największym ugrupowaniem o tym charakterze jest Islamische Gemeinschaft Millî Görüs e.V. (IGMG). Zob. W. Schiffauer: *Die Islamische Gemeinschaft Millî Görüş.* Centrum voor Islam in Europa (Universiteit Gent), Gent ohne Datum, http://www.flw.ugent.be/cie/CIE2/schiffauer1.htm [dostęp: 10 X 2012]. Mimo pokojowego nastawienia, ideologia Millî Görüs powoduje, że BfV uznaje tę organizację za antydemokratyczną i odrzucającą wartości kultury zachodniej. Zob. *Verfassungsschutzbericht 2009*, Berlin 2009, Bundesamt für Verfassungsschutz, s. 265. Inne organizacje promujące islam, i islamizm na terenie Niemiec, to Islamische Gemeinschaft in Deutschland e.V., która jest związana z Bractwem Muzułmańskim, a także umiejscowione w wielu niemieckich miastach ośrodki funkcjonujące pod nazwą Islamischen Zentren.

[32] http://www.verfassungsschutz.de/de/arbeitsfelder/af_islamismus/zahlen_und_fakten_islamismus/ [dostęp: 10 X 2012].

(Die Basis)[33] oraz powiązane z nią, mające charakter jej terytorialnych odłamów, ruchy takie, jak Al-Qaida im Irak, Islamischer Staat Irak[34], Al-Qaida im islamischen Maghreb (AQM)[35] oraz Al-Qaida auf der Arabischen Halbinsel (AQAH)[36]. Organizacje o charakterze terytorialnym nie podejmują bezpośrednich akcji na terenie Niemiec, kraj ten natomiast, podobnie jak wiele innych ugrupowań terrorystycznych i przestępczych, traktują jako swoistą bazę zapewniającą ekonomiczne wsparcie i personalne zaplecze. Oprócz organizacji skupionych wokół Al-Kaidy BfV wymienia jako związek terrorystyczny stanowiący zagrożenie dla Niemiec i niemieckich obywateli Islamski Ruch Uzbekistanu (Islamischen Bewegung Usbekistans – IBU). Ugrupowanie to nie tylko prowadzi agresywną kampanię internetową wzywającą do świętej wojny przeciwko państwu niemieckiemu, lecz także jest odpowiedzialne za co najmniej kilka ataków na niemieckich żołnierzy stacjonujących w Afganistanie[37]. Organizacjami terrorystycznymi wykazującymi aktywność na terenie Niemiec są także, zdaniem BfV, Ansar al-Islam (AAI)[38], Islamisch Jihad-Union (IJU)[39], mająca około dwustu członków na terenie Niemiec Hezb-e Islami-ye Afghanistan – HIA (Islamische Partei Afghanistans)[40], organizacja o nazwie Al-Shabab[41], libańska Partei Gottes (Hizb Allah)[42] oraz palestyński Islamische Widerstandsbewegung (HAMAS)[43]. Jako niebezpieczne dla demokratycznych wartości wyrażonych w niemieckiej konstytucji wymienione są także ugrupowania powiązane z ideologią salaficką[44], z którą na terenie państwa niemieckiego silnie utożsamia się co najmniej 3,5 tys. osób[45].

Kolejnym poważnym zagrożeniem, z którym walczy BfV, jest szpiegostwo. Przywoływana już w tekście sytuacja gospodarcza, a także znaczenie i pozycja polityczna Niemiec powodują, iż państwo to jest celem obcych wywiadów całego świata[46]. W zakresie nielegalnego pozyskiwania informacji oraz kradzieży technologii najbardziej aktywnymi są służby chińskie i rosyjskie[47]. Nielegalnie pozyskiwane informacje dotyczą sytuacji politycznej, w tym militarnej, oraz kwestii technologicznych i gospodarczych. Istotne znaczenie w obliczu wzrastającej konkurencji na rynku światowym mają również dane powiązane z biznesem, dotyczące konkretnych strategii marketingowych oraz

---

[33] *Verfassungsschutzberich 2011*, Berlin 2011, Bundesamt für Verfassungsschutz, s. 199.

[34] Tamże, s. 204.

[35] Tamże, s. 205.

[36] Tamże, s. 206.

[37] *Verfassungsschutzbericht 2011*, Hamburg 2011, Landesamt für Verfassungsschutz, s. 35–36.

[38] *Verfassungsschutzbericht 2011*…, s. 208.

[39] Tamże, s. 212.

[40] Tamże, s. 213.

[41] Tamże, s. 215.

[42] W Polsce znana pod nazwą Hezbollach.

[43] Islamski Ruch Oporu został założony w 1987 r. przez szejka Ahmeda Ismaila Jassina. Zob. A. Tai, *Widerstand im Namen Allahs – Hamas als politischer Faktor im Friedensprozess,* w: *Der Friedensprozess Im Nahen Osten: Eine Revision, Band 1: Konfrontation Und Kooperation Im Vorderen Orient,* Hrsg. F. Ibrahim, A. Ashkenasi, Münster 1998, s. 143–162.

[44] J. Danecki, *Podstawowe wiadomości o islamie,* tom 1, Warszawa 1997, Dialog, s. 211.

[45] *Verfassungsschutzbericht 2011*…, s. 216.

[46] *Spionage gegen Deutschland – Aktuelle Entwicklungen*, Köln 2008, Bundesamt für Verfassungsschutz, s. 4.

[47] Tamże, s. 5–8.

planów inwestycyjnych[48]. Część wiadomości znajdujących się w sferze zainteresowań obcych służb jest zdobywana dzięki stosowaniu nowoczesnych technologii. Fakt, że cenne informacje są przechowywane w systemach informatycznych powoduje ciągły wzrost ataków w cyberprzestrzeni ze strony zagranicznych wywiadów.

Służby niemieckie obserwują także nasilenie działalności wywiadowczej inspirowanej przez Koreę Północną oraz Iran. Przyczyną aktywności szpiegowskiej prowadzonej przez te kraje są dążenia do uzyskania broni masowego rażenia oraz technologii koniecznych do jej przenoszenia. Z realizacją tych celów wiążą się próby sprzecznego z prawem nabywania produktów podwójnego zastosowania[49].

Innym zagrożeniem, z którym walczy BfV, jest organizacja scjentologiczna[50]. Ruch scjentologiczny w Niemczech rozwija się dzięki luźno powiązanym z sobą organizacjom od początku lat 70. XX wieku[51]. Ideologia scjentologiczna w wielu krajach (np. we Francji, w Wielkiej Brytanii czy w Kanadzie) jest uważana za wysoce kontrowersyjną. Podstawowe zarzuty dotyczą manipulacji emocjonalnej, która jest oparta na głębokiej i intensywnej kontroli psychicznej[52]. Intensywne oddziaływanie scjentologii na sferę mentalną członków tego ruchu w pełni uzasadnia uznanie go za sektę destruktywną. Oprócz tego Kościół scjentologiczny jest także podejrzewany o prowadzenie przestępczości gospodarczej, a także pospolitej, objawiającej się głównie atakami i groźbami na byłych członków. Przywołane zastrzeżenia i równoczesne finansowe oraz społeczne zaplecze ruchu scjentologicznego powodują, iż stanowi on realne zagrożenia dla idei wolności i godności, będących fundamentalnymi wartościami wyrażonymi w niemieckiej konstytucji[53]. Fakt ten uzasadnia objęcie organizacji scjentologicznej wzmożoną czujnością przez Federalny Urząd Ochrony Konstytucji.

Spostrzeżenia na temat funkcji Federalnego Urząd Ochrony Konstytucji pozwalają wysnuć wniosek, że podstawowe kierunki działania tej instytucji wynikające z charakteru powierzonych jej zadań (przede wszystkim zapewnienia wewnętrznego bezpieczeństwa) są tożsame z funkcjami analogicznych instytucji innych państw demokratycznych, w tym z kierunkami zaangażowania jej polskiego odpowiednika, jakim jest ABW. Konkretne zagrożenia natomiast, którymi w ramach realizacji swoich ustawowych funkcji zajmuje się BfV, są odmienne. Różnice w katalogu szczegółowych działań wynikają zarówno z doświadczeń historycznych, jak i obecnej sytuacji społecznej i ekonomicznej Republiki Federalnej Niemiec.

---

[48] Tamże, s. 9.

[49] Tamże, s. 4.

[50] Więcej informacji na temat ruchu scjentologicznego można znaleźć na stronie internetowej http://www.psychomanipulacja.pl/art/scjentologia-podstawowe-informacje.htm. [dostęp: 11 X 2012].

[51] M.S. Fifka, N. Sykora, *Scientology in Deutschland und den USA*, Münster 2009, s. 89.

[52] Charakterystyczną praktyką Kościoła scjentologicznego jest tak zwany *auditing*, będący formą psychoanalitycznego przesłuchania, które prowadzi do ujawnienia przez osobę audytowaną wielu szczegółów dotyczących życia osobistego, w tym tych najbardziej intymnych. Zob. M.J. Gordon, *The Church of Scientology*, Salt Lake City 2000, Signature Press, s. 28.

[53] Zob. art. 1. Grundgesetz für die Bundesrepublik Deutschland: *Die Würde des Menschen ist unantastbar. Sie zu achten und zu schützen ist Verpflichtung aller staatlichen Gewalt* (Godność człowieka jest nienaruszalna. Jej poszanowanie i ochrona jest obowiązkiem wszystkich władz państwowych – tłum. aut.).

Abstrakt

Prezentowany artykuł omawia podstawowe kompetencje Federalnego Urzędu Ochrony Konstytucji (Bundesamt für Verfassungsschutz – BfV), będącego największą służbą specjalną Republiki Federalnej Niemiec. Autor przedstawia tu kluczowe zadania BfV oraz ich genezę wiążącą się z powstaniem Urzędu kilka lat po zakończeniu II wojny światowej. W artykule podkreślono, że konkretne działania BfV, będące realizacją normatywnie zakreślonych zadań, wynikają nie tylko z przepisów prawa, ale w praktyce są kształtowane również przez obiektywne czynniki zewnętrzne.

W artykule zostały omówione główne zagrożenia zwalczane przez BfV, do których należą ekstremizm lewicowy, prawicowy, narodowościowy i religijny. Szczególnie groźną postacią tego ostatniego jest islamizm i towarzyszący mu terroryzm. Kilka słów poświecono również działalności na terenie RFN obcych wywiadów, przede wszystkim rosyjskego i chińskiego. Charakterystycznym, krótko omówionym w artykule zagrożeniem zwalczanym przez BfV, jest także organizacja scjentologiczna.

Abstract

The article presents the Federal Office for the Protection of the Constitution (*Bundesamt für Verfassungsschutz* – BfV) which is the biggest special service in the Federal Republic of Germany. The author has depicted the major tasks of the BfV and their origin, referring to the establishment of the Bundesamt für Verfassungsschutz a few years after the Second World War. The author points out that the specific BfV activities, such as execution of the normatively outlined tasks, result not only from the regulations, but they are in practice also shaped by objective external factors.

The article also shows the fundamental threats that BfV counteracts, i.e. the left, right, ethnic and religious extremism. A particularly dangerous form of the latter is Islamism and terrorism related to it. The author also describes briefly the activities of foreign intelligence in the Federal Republic of Germany, especially the Russian and Chinese ones. A characteristic threat that is shortly presented in the article, which BfV fights, is the scientology organization.

Krzysztof Danielewicz

Komórka sztabowa 2X w operacji typu COIN – wybrane zagadnienia

Wstęp

Konflikty zbrojne w Iraku i Afganistanie znacząco zmieniły podejście do kwestii prowadzenia rozpoznania operacyjnego. Jest to wynik konieczności prowadzenia konfliktu według zasad COIN[1], w których najważniejszym elementem rozpoznania są człowiek i jego środowisko. Głównym celem COIN jest bowiem neutralizacja warunków mogących powodować rozwój ruchów powstańczych lub im sprzyjającym[2].

W przypadku operacji typu COIN znacznej modyfikacji uległo wykorzystanie systemów rozpoznania. Zaczęło przeważać stosowanie tych, które wykorzystują informacje pochodzące od ludzi – czy to zdobyte w sposób jawny, czy poprzez stosowanie specjalnych technik i procedur.

Celem artykułu jest przedstawienie wybranych aspektów rozpoznania osobowego (HUMINT) i kontrwywiadu (KW) na podstawie doświadczeń amerykańskich wyniesionych z Iraku i Afganistanu. Zaprezentowano w nim niektóre zagadnienia, szczególnie dotyczące komórki sztabowej G2X/S2X[3] centralizującej i koordynującej działania HUMINT i KW na danym terytorium działań oraz podległych jej elementów wykonawczych. Krótko omówiono także system szkolenia dla specjalistów HUMINT i KW opierając się na nowych doświadczeniach zdobytych w trakcie ostatnich konfliktów.

Charakterystyka rozpoznania w operacji typu COIN[4]

W przeciwieństwie do typowego konfliktu zbrojnego, w którym najważniejsze jest zlikwidowanie jak największej części sił zbrojnych i infrastruktury nieprzyjaciela, z reguły znanego i łatwego do zidentyfikowania, w operacji typu COIN podstawowym kryterium efektywności jest zniszczenie lub znaczne ograniczenie skuteczności przeciwnika i jego możliwości wykorzystania lokalnej ludności do własnych celów[5].

---

[1] COIN (ang. *counterinsurgency* – działania przeciw partyzanckie) można także zdefiniować jako operację wojskową, psychologiczną, ekonomiczną oraz cywilną podjętą przez rząd lub władze tymczasowe w celu zwalczenia ruchu powstańczego. Zob. *Counterinsurgency*, Field Manual (dalej: FM) 3–24, 15 December 2006, s. 1.

[2] *Counterguerilla Operations*, FM 90–8/MCRP 3–33A, U.S. Marine Corps, 29 August 1986, s. 1–5.

[3] W zależności od szczebla czy konfiguracji sił na danym teatrze możemy spotykać różne oznaczenia, np. S2X (do szczebla brygady), G2X (powyżej szczebla brygady), J2X (w przypadku operacji połączonych) czy CJ2X (w przypadku operacji połączonych i wielonarodowych), zawsze jednak pozostanie oznaczenie 2X, które wskazuje na element sztabowy, centralizujący działania HUMINT i KW.

[4] Więcej na temat rozpoznania w operacji typu COIN w: K. Danielewicz, *Charakterystyka rozpoznania w operacji typu COIN*, „Bezpieczeństwo Teoria i Praktyka" 2012, nr 1, s. 45–63.

[5] L.S. Turner, D. Corbould, J.T. Adair, L. Hamel, *Optimizing Deadly Persistence in Kandahar: Armed UAV Integration in the Joint Tactical Fight* [online], „The Canadian Army Journal Volume", s. 124, www.armyforces.go.ca/caj [dostęp: 14 II 2010].

Zrozumienie zasad panujących w otoczeniu COIN pozwala na odpowiednią alokację posiadanych środków rozpoznawczych.

Aby lepiej pojąć znaczenie rozpoznania w tak skomplikowanych warunkach, niezbędne jest przedstawienie sześciu cech odróżniających operację COIN od innych operacji zbrojnych. Cechy te zostały wypracowane na podstawie doświadczeń zdobytych podczas ostatnich konfliktów[6].

1. **Najważniejszą rzeczą w COIN jest rozpoznanie dotyczące ludzi**. Dowódca podczas działań musi rozumieć lokalną ludność, zależności występujące w strukturach państwa gospodarza, ludzi przystępujących do zbrojnej opozycji, ich motywację oraz czynniki, które sprzyjają siłom rebelianckim i powodują ich rozwój. Na tym etapie istotna jest również znajomość systemu wierzeń i rozumienie zależności występujących w społeczeństwie oraz sposób podejmowania decyzji.
2. **COIN jest wojną informacyjną oraz wojną systemów rozpoznawczych**. Zarówno rebelianci (*insurgents*), jak i siły COIN (*counterinsurgents*) potrzebują efektywnego rozpoznania. Kluczem do sukcesu jest w tym przypadku zorganizowanie sprawnego systemu pozyskiwania i opracowywania informacji oraz neutralizacja zdolności rozpoznawczych strony przeciwnej.
3. **Istnieje ścisły związek pomiędzy operacjami prowadzonymi na teatrze działań wojennych a pozyskanymi informacjami o przeciwniku.** Wiarygodne dane pozwalają prowadzić skuteczne działania, które w konsekwencji przyczyniają się do uzyskiwania kolejnych istotnych informacji rozpoznawczych.
4. **Wszystkie operacje zawierają elementy rozpoznawcze.** Każdy uczestnik operacji bierze udział w aktywnym zbieraniu informacji – poprzez swoje kontakty z lokalną ludnością, siłami bezpieczeństwa czy też przedstawicielami lokalnych władz.
5. **Informacje w COIN,** na które należy zwrócić szczególną uwagę, **są przesyłane od elementów najniższego szczebla do wyższych struktur dowódczo-sztabowych**.
6. **Jednostki wszystkich szczebli prowadzą swoje działania w złożonym systemie, w którego skład wchodzą elementy wojskowe i cywilne sił koalicyjnych oraz państwa gospodarza, a także elementy zewnętrzne.** W związku z powyższym wszystkie szczeble są zmuszone koordynować swoje działania rozpoznawcze z wymienionymi komórkami[7].

Na podstawie wyżej wymienionych cech widać, że w konflikcie niekonwencjonalnym w centrum uwagi pozostaje człowiek, jego potrzeby, powiązania i motywacje, a także krąg kulturowy, religia i tradycje panujące w danym regionie. W związku z tym w takich warunkach najlepiej sprawdzają się te rodzaje rozpoznania, które pozwalają na bezpośredni kontakt z człowiekiem skutkujący otrzymaniem informacji. Należą do nich HUMINT oraz KW, w których przypadku źródłem informacji pozostaje głównie człowiek. Inne rodzaje rozpoznania, takie jak: OSINT, MASINT, TECHINT, SIGINT, GEOINT, IMINT czy RADINT[8], korzystają z technicznych źródeł informacji będących

[6] K. Teamey, J. Sweet, *Organizing Intelligence for Counterinsurgency,* „Military Review" 2006, s. 24–25.

[7] *Counterinsurgency*…, s. 3–25.

[8] Ogólnie źródła informacji możemy podzielić na techniczne i osobowe. Do najistotniejszych technicznych źródeł informacji możemy zaliczyć: TECHINT **(***Technical Intelligence*) – rozpoznanie techniczne, polegające na uzyskiwaniu informacji rozpoznawczych poprzez analizę sprzętu, wyposażenia oraz środków bojowych przeciwnika, MASINT (*Measurement and Signatures Intelligence*) – rozpoznanie polegające na eksploatacji oraz analizie śladów pozostawianych przez przeciwnika, GEOINT (*Geospatial Intelligence*) – rozpoznanie wykorzystujące dane obrazowe, przestrzenne oraz geograficzne w celu sporządzenia opisu oraz

w takim przypadku uzupełnieniem dla HUMINT-u czy kontrwywiadu. W zależności od sytuacji najbardziej efektywna metoda rozpoznania jest wspierana przez pozostałe, mniej skuteczne, ale ważne dla poszerzenia i potwierdzenia informacji.

Doświadczenia amerykańskie nabyte podczas konfliktów w Iraku czy Afganistanie pokazały także, że w wielu przypadkach liczne i mobilne kompanie musiały polegać na rozpoznaniu przygotowanym przez kilku lub kilkunastu żołnierzy, w dużej mierze młodych i niedoświadczonych, którzy właśnie ukończyli kursy czy szkolenia rozpoznawcze. Ich zadaniem było nie tylko dostarczyć dowódcom informacje na temat aktualnej sytuacji i przygotować pakiety targetingowe[9], lecz także przewidzieć możliwy rozwój wypadków, co na tak niskim szczeblu było trudne, a często wręcz nierealne – również z powodu niepełnego obrazu wydarzeń.

Niewystarczające wsparcie rozpoznawcze powodowało, że wysyłanie dodatkowych sił bojowych nie polepszało sytuacji. Wywoływało to frustracje wśród wyższych przełożonych, którzy pomimo dobrze rozwiniętego aparatu rozpoznawczego na wyższym szczeblu nie mieli informacji na temat tego, co dzieje się w terenie. Dowódcy niższego szczebla z kolei zgłaszali uwagi, że w związku z niedostatecznym rozpoznaniem nie są w stanie odpowiednio chronić własnych żołnierzy[10].

Geneza powstania i zakres odpowiedzialności komórki 2X

Ogromne znaczenie HUMINT i KW zostało zauważone już w latach 90. XX wieku po działaniach wojennych w Bośni. Jednak struktury organizacyjne i doktryny rozpoznawcze w dalszym ciągu były przygotowywane na warunki typowego konfliktu pełnowymiarowego.

W listopadzie 2001 r. dowódca Amerykańskiego Centrum Rozpoznawczego i Fortu Huachuca (United States Army Intelligence Centre and Fort Huachuca – USAIC&FH)[11] powołał specjalną komórkę – Zintegrowany Zespół Koncepcyjny (Integrated Concept Team), której celem była transformacja HUMINT i KW, co w konsekwencji miało się przyczynić do sprostania wymaganiom dotyczącym sytuacji międzynarodowej. Problem polegał na tym, że armia amerykańska zawsze była organizacyjnie „skrojona" według aktualnych zagrożeń dla USA. W okresie zimnej wojny KW miał rozpoznawać i neutralizować wysiłek rozpoznawczy Armii Radzieckiej, HUMINT natomiast – jej możliwości bojowe i plany, co z kolei wspierało działania komórek planistycznych

analizy geograficznej terenu, OSINT (*Open Source Intelligence*) – rozpoznanie oparte na ogólnodostępnych, jawnych źródłach informacji, SIGINT (*Signal Intelligence*) – rozpoznanie sygnałowe oraz IMINT (*Imagery Intelligence*) – rozpoznanie obrazowe, wykorzystujące dane uzyskane z analizy zdjęć fotograficznych, promieniowania elektromagnetycznego, promieniowania cieplnego czy danych pochodzących z radarów. HUMINT oraz kontrwywiad to rodzaje rozpoznania, podczas których wykorzystuje się informacje przekazywane przez ludzi. Zob. *Counterinsurgency*…, s. 26–28.

[9] Targeting to proces polegający na typowaniu obiektów infrastruktury lub ludzi, którzy powinni być rażeni przez siły własne. W przypadku ludzi nie zawsze oznacza to likwidację fizyczną; w warunkach COIN w niektórych przypadkach stosuje się inne środki, takie jak usunięcie ze stanowiska czy marginalizację. W targetingu znaczenie informacji zdobywanych przez HUMINT czy KW jest ogromne. Pakiet targetingowy do zbiór informacji niezbędny do realizacji całej operacji.

[10] G. Moore, *Ten Principles of Intelligence on the Battlefield*, „Military Intelligence Professional Bulletin" 2007, s. 22. Kpt. Gregory Moore odbył dwie tury w Iraku jako oficer rozpoznania batalionu, służąc w 10. Górskiej Dywizji i 5. Grupie Sił Specjalnych.

[11] Jest to najważniejsze centrum szkolenia specjalistów w zakresie rozpoznania. Szkoleni są głównie żołnierze amerykańscy, ale centrum jest otwarte takż na specjalistów z innych państw. W zależności od potrzeb prowadzi też szkolenia pozamiejscowe.

odpowiedzialnych za tworzenie koncepcji działań skierowanych przeciwko Rosjanom. Po zakończeniu zimnej wojny HUMINT i KW pozostawały w stanie zawieszenia, co było rezultatem braku jasno określonego wroga. Lata 90. to okres misji pokojowych i stabilizacyjnych, a HUMINT i KW były dobierane i konfigurowane w zależności od potrzeb danej misji i wizji dowódcy. Głównym zadaniem w tym okresie było pozyskiwanie informacji zgodnie z wymaganiami informacyjnymi dowódcy (PIR – *Priority Information Requirements*). Okres ten charakteryzował się brakiem sprecyzowanych wizji i doktryn określających działania HUMINT i KW, co w konsekwencji doprowadziło do znacznej redukcji znaczenia KW. Spowodowane to było także brakiem określonej wrogiej struktury rozpoznawczej, którą należało wyodrębnić i zneutralizować. Traktowanie KW jako kolejnego źródła informacji działającego w odpowiedzi na wymagania dowódców powodowało u niektórych z nich postrzeganie kontrwywiadu jako swoistego HUMINT-u. Niemniej jednak zarówno HUMINT, jak i KW przez cały ten czas były ważnymi narzędziami pozyskiwania informacji, które bez względu na warunki geograficzne czy pogodowe można było szybko przekazać w dowolne miejsce na ziemi, by zapewnić dowódcy wsparcie informacyjne[12].

Jedną ze zmian w amerykańskim systemie rozpoznania było zwiększenie możliwości rozpoznawczych w nowo utworzonej Brygadzie Rozpoznania Pola Walki (BfSB – Battlefield Surveillance Brigade), w której znacznie wzrosła liczba komórek HUMINT i KW. W strukturze batalionu rozpoznawczego brygady znalazło się osiem sekcji kontrwywiadu oraz 55 sekcji HUMINT. Najwyższym szczeblem koordynującym działania tych dwóch elementów była Taktyczna Sekcja Operacyjna HUMINT (THOPS – Tactical HUMINT Operations Section). Sekcja ta, składająca się z jednego lub dwóch specjalistów, zarządzała działaniami m.in. HUMINT-u i KW w trakcie operacji na Bałkanach w latach 90. XX wieku. Na podstawie doświadczeń zdobytych podczas tego konfliktu zdecydowano się stworzyć w ramach G2/S2[13] sekcję o oznaczeniu G2X lub S2X w zależności od szczebla, ale pierwsze kursy 2X zorganizowano dopiero w latach 2005 i 2006. Komórka 2X, będąca komórką sztabową, miała w zamyśle odpowiadać za koordynację całości zagadnień związanych z działalnością kontrwywiadu i rozpoznania osobowego HUMINT. Do sekcji 2X początkowo należały jedna lub dwie osoby; z czasem rozwinęła się ona do trzech komórek zarządzających całością operacji HUMINT i kontrwywiadu, tzn. do komórki zarządzania KW, komórki zarządzania HUMINT oraz komórki wsparcia. W konsekwencji komórki 2X powstały na wszystkich szczeblach dowodzenia od brygady wzwyż[14].

Na podstawie doświadczeń z Bośni, Kosowa czy Afganistanu można stwierdzić, że prawie 80 proc. wszystkich informacji pochodzi od kontrwywiadu i HUMINT. Koncepcja 2X jest bardzo dobrym kierunkiem, który poprawia efektywność wymienionych wcześniej metod rozpoznawczych. Struktura 2X przez ostatnie lata ulegała ciągłej modyfikacjom w związku z nowo zdobytymi doświadczeniami. W dużej mierze zależy ona także od wielkości danej misji, liczby elementów podległych HUMINT i KW, a także charakteru misji (narodowego lub międzynarodowego).

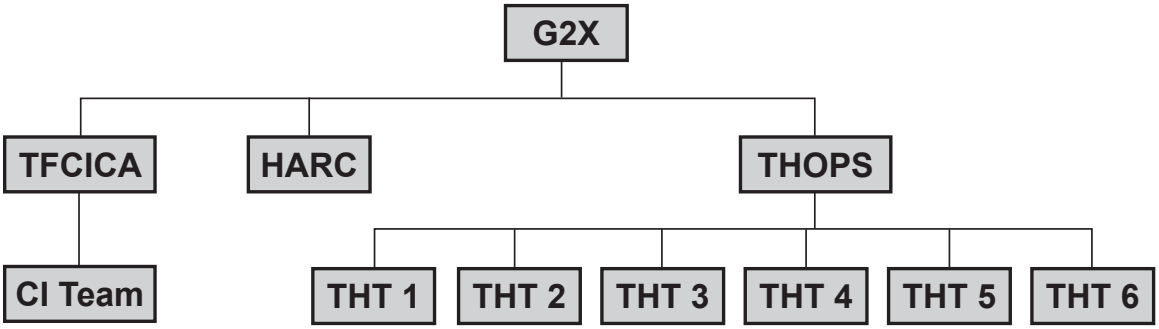
---

[12] L. Norris, *Transforming Counterintelligence and Human Intelligence* [online], „Military Intelligence Professional Bulletin" 2003, s. 47–48, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

[13] S2 i G2 są to komórki sztabowe zajmujące się rozpoznaniem. Oznaczenie S, G czy J zależy od szczebla dowodzenia i charakteru misji.

[14] R. Bukowski, *Bridging the Doctrine Gap: A CI and HUMINT Focused Look at the Transformation of MI Doctrine*, „Military Intelligence Professional Bulletin" 2008, wydanie specjalne, s. 5–14.

Jako przykład może tu posłużyć struktura G2X z misji SFOR 13 (The Stabilization Force) w Bośni i Hercegowinie. Szefowi G2X podlegały wówczas następujące komórki: sekcja kontrwywiadu – TFCICA (Task Force CI Coordinating Authority), sekcja HUMINT – THOPS (Tactical HUMINT Operations) oraz sekcja analityczna i zarządzania wymaganiami informacyjnymi – HARC (HUMINT Analysis Requirements Cell) odpowiedzialna za analizę i publikację raportów HUMINT zgodnie z wymaganiami informacyjnymi dowódcy (PIR). Sekcjom HUMINT i KW z kolei podlegały zespoły HUMINT (THT – Tactical HUMINT Team) i zespoły KW (CI Team), które w praktyce wykonywały zadania. Należy podkreślić, że w tamtym przypadku w zespołach HUMINT funkcjonowali specjaliści nie tylko od HUMINT, ale także od KW oraz tłumacze, zespoły KW natomiast realizowały zadania stricte kontrwywiadowcze[15].



Rys. 1. Struktura G2X SFOR 13.
Źródło: R. Bukowski, *Bridging the Doctrine Gap: A CI and HUMINT Focused Look at the Transformation of MI Doctrine*, „Military Intelligence Professional Bulletin" 2008, wydanie specjalne, s. 5–14.

Ciekawie prezentują się także doświadczenia zdobyte przez amerykański Połączony Zespół Sił (CJTF – 180, Combined Joint Task Force) w ramach operacji Enduring Freedom[16] w Afganistanie w 2002 r. Mimo tego, że utworzona komórka 2X miała braki kadrowe, to jednak doświadczenie pracujących tam osób pozwoliło pomyślnie zrealizować zadania postawione przed HUMINT i KW. Według uczestników kluczem do sukcesu była tutaj odpowiednia obsada stanowisk szefa 2X, szefa sekcji HUMINT (HOC Chief – HUMINT Operation Cell Chief) i szefa sekcji KW (CICA Chief – CI Coordinating Authority Chief). Wspólnie byli oni odpowiedzialni za sprawne zarządzanie takimi zadaniami, jak: prowadzenie dochodzeń kontrwywiadowczych, kontrwywiadowczą ochronę osobowych źródeł informacji, operacje w terenie, prowadzenie przesłuchań i spotkań z osobami posiadającymi istotne informacje (*debriefing* i *interrogation*), prowadzenie jawnych operacji HUMINT czy wspieranie wrażliwych i tajnych operacji HUMINT. Pomimo tego, że były to początki działalności komórki CJ2X w Afganistanie, to była ona w stanie z powodzeniem zrealizować szereg przedsięwzięć, takich jak:

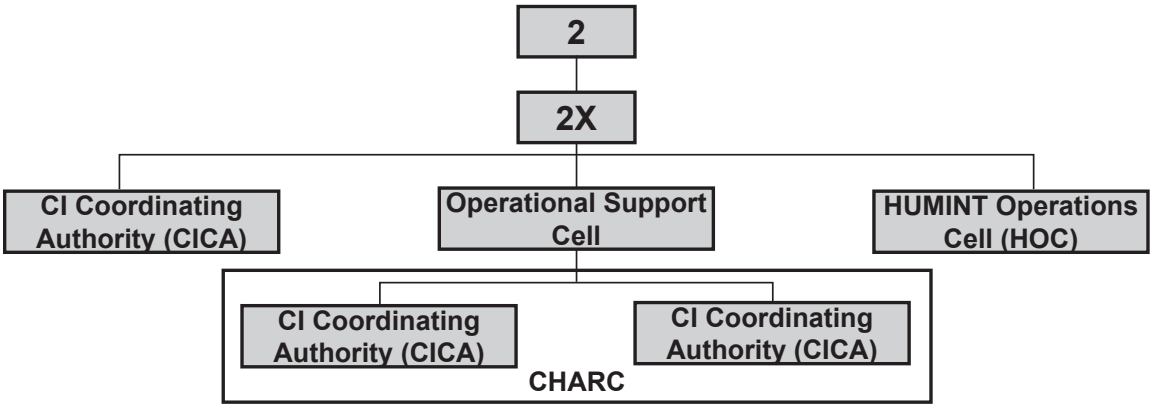
- poprawa struktury i podporządkowania posiadanych sił zgodnie z sytuacją operacyjną na teatrze,

[15] L. Lacy, *Lessons Learned: Army National Guard G2X in Bosnia* [online], „Military Intelligence Professional Bulletin" 2003, s. 38–39, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

[16] Operacja antyterrorystyczna realizowana w Afganistanie głównie przez siły amerykańskie.

- efektywna działalność związana z przesłuchaniami i uzyskiwaniem informacji przez podległe elementy, dzięki czemu w ciągu siedmiu miesięcy opublikowano 1500 raportów informacyjnych (IIR – Intelligence Information Report),
- poprawa systemu meldunkowego, skutkująca ograniczeniem czasu do 12 godzin od chwili uzyskania informacji do momentu jej przekazania właściwemu odbiorcy na teatrze. Po uzyskaniu przez CJ2X prawa do samodzielnego publikowania raportów[17] czas ten został skrócony do sześciu godzin,
- duży udział raportów HUMINT i KW w targetingu dzięki ich jakości i szybkiej dostępności,
- utworzenie i sprawne administrowanie bazą danych osobowych źródeł informacji (TSR – *Teather Source Register*), w której było około 300 aktywnych i nieaktywnych źródeł osobowych. Ustanowiono także odpowiedni proces ich rejestrowania i oceniania,
- przygotowanie odpowiednich stałych procedur operacyjnych (SOP – Standing Operating Procedures), w których opisano obowiązki, techniki i taktykę pracy na danych stanowiskach, co w rezultacie poprawiło skuteczność pracy,
- zwrócenie uwagi na to, by wysiłek informacyjny HUMINT i KW był zgodny z wymaganiami informacyjnymi dowódcy, jego priorytetami czy procesem targetingu,
- zwiększenie liczby zespołów KW z czterech (sześciu–dziewięciu żołnierzy) do dziewięciu (po czterech żołnierzy),
- zwiększenie liczby operatorów realizujących przesłuchania z siedmiu do piętnastu,
- ustanowienie systemu przesyłania uwag (feedback) dla operatorów HUMINT i KW, dzięki czemu mogli oni odpowiednio zadaniować swoje kontakty czy osobowe źródła informacji i kontrolować ich wiarygodność;
- próba połączenia pracy z osobowymi źródłami informacji z prowadzeniem przesłuchań[18].

Elementy podstawowej struktury komórki sztabowej 2X przedstawia poniższy rysunek:



Rys. 2. Podstawowa struktura amerykańskiej komórki 2X.
Źródło: L. Norris, *Transforming Counterintelligence and Human Intelligence* [online], „Military Intelligence Professional Bulletin" 2003, s. 47–48, http://www.fas.org/irp/agency/army/mipb/index.html.

[17] Wcześniej raporty były przesyłane do USA, a następnie po akceptacji i analizie wracały na teatr, co sztucznie i niepotrzebnie wydłużało czas ich dostępności dla wojsk na teatrze.

[18] R. Stallings, M. Foley, *CI and HUMINT Operations in Support of Operation Enduring Freedom* [online], „Military Intelligence Professional Bulletin" 2003, s. 43–46, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

Szef komórki 2X w takiej konfiguracji kieruje pracą sekcji: kierowania KW (CICA – CI Coordinating Authority)[19], kierowania HUMINT (HOC – HUMINT Operations Cell), wsparcia operacyjnego (OSC – Operational Support Cell), analitycznej KW (Counterintelligence Analysis Cell) oraz analitycznej HUMINT (Human Intelligence Analysis Cell)[20].

Do obowiązków komórki 2X i jej szefa należy:

- doradzanie szefowi rozpoznania na teatrze w zakresie funkcjonowania HUMINT i KW,
- sprawowanie kontroli nad podległymi elementami HUMINT i KW przy pomocy CICA, HOC, OSC, CIAC i HAC,
- koordynowanie i dekonfliktowanie działalności HUMINT i KW z innymi elementami funkcjonującymi w tym samym rejonie operacji,
- przegląd i zatwierdzanie wymagań informacyjnych dla HUMINT i KW,
- wsparcie informacyjne i logistyczne podległych komórek,
- utrzymywanie łączności z innymi, niepodlegającymi bezpośrednio, amerykańskimi i koalicyjnymi, elementami HUMINT i KW[21],
- koordynowanie wykorzystania HUMINT i KW w sposób gwarantujący uzyskanie odpowiedzi na wymagania informacyjne dowódcy,
- rejestrowanie i dekonfliktowanie wykorzystywanych osobowych źródeł informacji,
- zapewnianie wsparcia w zakresie komentarzy (*reach back*) do raportów informacyjnych dla OMT[22].

Sekcja analityczna KW i HUMINT (CHARC) odpowiada za:

- analizę informacji pochodzących od HUMINT i KW,
- analizę możliwości przeciwnika pod kątem atakowania sił własnych na podstawie otrzymywanych raportów,
- identyfikowanie obszarów niepodlegających rozpoznaniu oraz określanie możliwości ich pokrycia informacyjnego,
- przygotowanie i dystrybucję raportów informacyjnych (INTSUM i inne) sporządzonych na podstawie raportów HUMINT i KW,
- przygotowanie długoterminowego planu zbierania informacji oraz komentarzy dla operatorów HUMINT i KW do sporządzonych przez nich raportów,
- dbałość o wykorzystanie elementów operacyjnych zgodnie z wymaganiami informacyjnymi dowódcy[23].

Sekcja Wsparcia Operacyjnego jest odpowiedzialna w ramach 2X m.in. za:

- prowadzenie bazy danych wszystkich osobowych źródeł informacji wykorzystywanych w ramach 2X,
- zarządzanie całością wyposażenia technicznego wykorzystywanego przez 2X,
- zarządzanie funduszem operacyjnym,

---

[19] Autor posługuje się nazewnictwem amerykańskim, najczęściej spotykanym w dostępnej literaturze. Ma to na celu zapoznać osoby zainteresowane tematem ze znaczeniem najważniejszych terminów.

[20] Często obie wymienione sekcje analityczne można spotkać pod nazwą CHARC (*Counterintelligence and Human Analysis Requirements Cell*), oznaczającą sekcję analityczną obu dyscyplin.

[21] L. Norris, *Transforming Counterintelligence*…, s. 50.

[22] *Counterintelligence* [online], „FM 2.0 – Intelligence", http://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap11.htm [dostęp: 26 XII 2012].

[23] L. Norris, *Transforming Counterintelligence*…, s. 50.

- zarządzanie i koordynację wsparcia 2X przez cywilnych kontraktorów, HUMINT i KW, a także tłumaczy – zgodnie z wymaganiami i zawartymi kontraktami[24].

Funkcjonowanie jednostek rozpoznania osobowego HUMINT i zakres ich obowiązków

Sekcja Operacyjna HUMINT (HOC) jest jedną z dwóch, poza KW, najważniejszych sekcji operacyjnych w ramach 2X. Jest to jednak w dalszym ciągu struktura, która w praktyce nie realizuje czynności operacyjnych.

Sekcja Operacyjna HUMINT w ramach 2X odpowiada za:

- koordynację i synchronizację wszelkiej działalności HUMINT w danym rejonie odpowiedzialności (AOIR – *Area of Intelligence Responsibility*),
- sprawowanie technicznej i merytorycznej kontroli nad całością podległych elementów HUMINT w wyznaczonym AOIR oraz neutralizację skonfliktowania tej działalności z innymi elementami HUMINT, tj. wyższego i niższego szczebla,
- koordynację własnej działalności z działalnością Sekcji Kontrwywiadu i Sekcji Wsparcia Operacyjnego,
- prowadzenie bazy danych osobowych źródeł informacji pozostających na łączności operatorów HUMINT,
- kierowanie procesem zbierania informacji przez elementy HUMINT zgodnie z wymaganiami informacyjnymi określonymi przez komórki odpowiedzialne za ten proces,
- przygotowanie części planu synchronizacji działań rozpoznawczych dotyczących HUMINT,
- koordynację elementów HUMINT przydzielonych do komórek odpowiedzialnych za prowadzenie przesłuchań i rozmów (*debriefingu*),
- proces przygotowywania raportów informacyjnych i ich dystrybucję zgodnie z obowiązującymi procedurami oraz utrzymywanie kontaktów łącznikowych z elementami HUMINT państwa gospodarza i innymi elementami HUMINT USA[25].

Działania operacyjne HUMINT wspomaga Sekcja Analityczna HUMINT, która odpowiada za analizę informacji oraz raportów od operatorów HUMINT. Sekcja ta jest odpowiedzialna m.in. za:

- identyfikację obszarów bez pokrycia informacyjnego oraz koordynację działalności rozpoznawczej z innymi źródłami informacji,
- wykorzystanie odpowiednich narzędzi analitycznych w celu przygotowania długoterminowego planu zbierania informacji oraz komentarzy (feedback) do wszystkich raportów HUMINT,
- przygotowywanie i dystrybucję produktów HUMINT oraz zapewnianie odpowiednich wstawek informacyjnych do zbiorczych raportów rozpoznawczych (*intelligence summary*),
- używanie narzędzi analitycznych w celu przygotowania długoterminowych analiz,
- przygotowywanie analiz na temat danych obszarów na podstawie informacji zebranych przez HUMINT,

[24] *Human Intelligence* [online], „FM 2.0", http://www.globalsecurity.org/intell/library/policy/army/fm/2-0/chap6.htm [dostęp: 26 XII 2012].

[25] Tamże.

- wspomaganie pakietów targetingowych przygotowywanych przez 2X zgodnie z planem zbierania informacji,
- analizowanie oraz przesyłanie meldunków dotyczących trendów i wzorców postępowania przeciwnika zidentyfikowanych na podstawie raportów HUMINT,
- analizowanie wiarygodności (*reliability*) źródeł informacji oraz rzetelności (*credibility*) meldunków oraz przekazywanie wniosków operatorom,
- przygotowywanie wymagań informacyjnych dotyczących HUMINT dla HOC,
- przygotowanie potrzeb informacyjnych dla HUMINT jako kontrybucji do PIR oraz przygotowywanie odpowiedzi na RFI (*Request for Information*) dotyczące działalności HUMINT.

Istotne jest, aby raporty HUMINT, w różnorodnej formie, były zawsze przesyłane przy pomocy środków zapewniających odpowiedni poziom bezpieczeństwa[26].

Kolejne dwa elementy – Sekcja Zarządzania Działalnością HUMINT (OMT – Operational Management Team) i zespoły HUMINT (HUMINT Team) w praktyce realizują zadania w terenie.

W zależności od sytuacji i teatru działań zespoły HUMINT mogą wykonywać operacje samodzielnie, pozostając pod bezpośrednią kontrolą sekcji operacyjnej HUMINT lub w ramach sekcji zarządzania działalnością HUMINT – OMT. OMT to komórka trzy-, czteroosobowa, kierowana przez doświadczonego żołnierza. Dodatkowo, w zależności od potrzeb, może w niej pracować także personel cywilny. Struktura organizacyjna i liczebność komórki zależą w głównej mierze od realizowanych zadań, tempa działań, szczebla czy liczby operatorów HUMINT. Z reguły OMT jest tworzone w przypadku wysyłania dwóch lub więcej zespołów HUMINT i kieruje ich działalnością. W związku z gromadzeniem informacji stanowiących odpowiedź na Priorytetowe Wymagania Informacyjne Dowódcy – PIR (*Priority Intelligence Requirements*) czy Wymagania Informacyjne (IR – *Information Requirements*) OMT prowadzi swoje działania w ścisłej współpracy z S2 i 2X. OMT realizuje następujące działania:

- przygotowuje wytyczne i sprawuje techniczną kontrolę na działalnością operacyjną podległych operatorów HUMINT,
- nadzoruje jakość zbieranych informacji,
- sprawuje jakościową kontrolę nad operatorami HUMINT oraz zajmuje się dystrybucją ich raportów,
- prowadzi analizę informacji uzyskanych przez HUMINT pod kątem ich zgodności z wymaganiami informacyjnymi dowódcy,
- jest elementem koordynującym pomiędzy innymi operatorami HUMINT, HOC, elementami wsparcia czy dowództwami,
- zapewnia wsparcie administracyjne, analityczne i logistyczne dla zespołów HUMINT, a także edukuje dowódców w rejonie działalności w kwestii możliwości oraz specyfiki działania podległych zespołów HUMINT[27].

Zespół HUMINT (HUMINT Team) jest najmniejszym elementem operacyjnym rozpoznania osobowego, składającym się z czterech specjalistów HUMINT, dwóch podoficerów i dwóch młodszych specjalistów[28]. W niektórych przypadkach, jeżeli jest to konieczne, w skład zespołu mogą wchodzić także cywile. Podobnie jak w poprzednim przypadku, ich stopień wojskowy, doświadczenie czy przygotowanie zawodowe zależą

[26] Tamże.

[00] Tamże, zob. także: L. Norris, *Transforming Counterintelligence*…, s. 53,

[00] Taka struktura dotyczy armii amerykańskiej; w przypadku innych państw może ona być odmienna.

od samej misji czy możliwości kadrowych. Przygotowanie i odbyte szkolenia są ściśle powiązane z wymaganiami i zakresem obowiązków na danym stanowisku w ramach zespołu HUMINT[29].

Przy okazji wątku HUMINT należy wspomnieć o doświadczeniach Amerykanów dotyczących rozpoznania osobowego z ostatnich lat. Działalność HUMINT jest definiowana przez Amerykanów jako proces zbierania informacji przez odpowiednio wyszkolonych operatorów wykorzystujących osobowe źródła informacji. Celem tej działalności jest zidentyfikowanie przeciwnika, a także jego intencji, struktury organizacyjnej, sił, możliwości, stosowanej przez niego taktyki oraz wyposażenia[30]. HUMINT realizuje swoje obowiązki poprzez taktyczne rozpytywanie, przesłuchania zatrzymanych (*interrogation*), rozmowy z żołnierzami i cywilami po zakończonych misjach, kontakty łącznikowe, kontakty z osobowymi źródłami informacji, badanie zdobytych dokumentów (DOCEX – *document exploitation*[31]) oraz badanie zdobytego wyposażenia (CEE – *captured equipment operations*)[32].

Pomimo swoich doświadczeń bojowych amerykańscy dowódcy mieli duży problem ze zrozumieniem specyfiki działalności HUMINT. Po zakończeniu zimnej wojny, a w związku z konfliktami w Iraku i Afganistanie, główny wysiłek operatorów HUMINT musiał ulec zmianie z prowadzenia dużej ilości przesłuchań, typowych dla konfliktu pełnowymiarowego (FSO – Full Spectrum Operation), na rzecz operacji ze źródłami osobowymi, co wynikało z charakterystyki konfliktu typu COIN. W konflikcie typu COIN sytuacja kreuje tak dużą różnorodność problemów wynikających z techniki i taktyki działania przeciwnika, że żadna stała struktura nie jest w stanie ich przewidzieć i w pełni się przed nimi zabezpieczyć[33]. Problem polegał na tym, że żołnierze HUMINT przygotowani do prowadzenia przesłuchań nie mieli przygotowania i doświadczenia w pracy ze źródłami osobowymi. Ci, którzy znali zasady pracy ze źródłami, nie znali procedur związanych z prowadzeniem przesłuchań. Przykładowo na szczeblu amerykańskiej Brygadowej Grupy Bojowej – BCT (Brigade Combat Team) działa kompania rozpoznawcza (MICO – Military Intelligence Company), w której ramach funkcjonują trzy (czasami cztery) zespoły HUMINT, kierowane przez OMT oraz około cztero-,

---

[29] *Human Intelligence.*

[30] *Intelligence*, FM 2–0, 17 May 2004, s. 1–6.

[31] Obecnie w literaturze przedmiotu częściej używana jest nazwa DOMEX (Documents and Media Exploitation). DOMEX traktowany jest jako samodzielna dyscyplina rozpoznania – niezwykle istotna, jeżeli weźmiemy pod uwagę jakość i liczbę informacji, które można uzyskać na podstawie przejętych dokumentów i materiałów. Przykładem może być akcja zabicia Osamy bin Ladena, kiedy to w trakcie operacji przechwycono szereg istotnych informacji DOMEX. Podczas analizy twardych dysków odnaleziono m.in. dokumenty z 2002 r. dotyczące finansowania radykalnych ugrupowań islamskich przez islamskie organizacje charytatywne na Bałkanach na początku lat 90. oraz informacje ze spotkań w Pakistanie z 1988 r. dotyczących założenia Al-Kaidy. W trakcie przeszukania zabudowań znaleziono około 100 pamięci przenośnych z danymi dotyczącymi wymiany mailowej pomiędzy bin Ladenem a jego ludźmi na całym świecie. Na podstawie analizy materiałów ustalono, że Ayman al-Zawahiri także przebywa na terenie Pakistanu. Z dokumentów wynika m.in., że bin Laden planował zmienić nazwę swojej terrorystycznej organizacji z Al-Kaida na inną. K. Danielewicz, *Rola Centralnej Agencji Wywiadowczej w wykryciu i zabiciu Osamy bin Ladena, w: Służby specjalne w systemie bezpieczeństwa państwa, Przeszłość – teraźniejszość – przyszłość. Materiały i studia*, t. II, A. Krzak, D. Gibas-Krzak (red.), Szczecin–Warszawa 2012, Wojskowe Centrum Edukacji Obywatelskiej, s. 199–200.

[32] R. Stallings, M. Foley, *CI and HUMINT…*, s. 43–46,

[33] C. Payne, Ch. LeBoeuf, *HUMINT from COIN to FSO: A Way Ahead* [online], „Military Intelligence Professional Bulletin" 2011, s. 24, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

pięcioosobową S2X. Z założenia BCT powinna móc, w razie potrzeby, przydzielić po jednym zespole HUMINT do każdego batalionu manewrowego, w którym musiały one realizować całe spektrum zadań HUMINT[34].

Skupienie się tylko na operacji COIN powoduje, że po powrocie do typowej struktury w pełnowymiarowym konflikcie operatorzy HUMINT realizujący operacje ze źródłami osobowymi (MSO – Military Source Operation) nie będą w stanie prowadzić przesłuchań[35], które szczególnie w początkowej fazie konfliktu całkowicie pochłaniają HUMINT. Idealnym rozwiązaniem byłoby szkolenie operatorów rozpoznania osobowego zarówno w zakresie prowadzenia przesłuchań, jak i operacji z osobowymi źródłami informacji. Jest to o tyle istotne, że w trakcie przesłuchań często są uzyskiwane informacje o osobach posiadających dostęp do wartościowych danych, co powinno być rozwijane przez operatorów HUMINT w ramach operacji z osobowymi źródłami informacji. Podczas operacji w Afganistanie często rdzenne elementy HUMINT z BCT były w całości zaangażowane w operacje ze źródłami. W związku z tym, że w operacji typu COIN także istnieje potrzeba prowadzenia przesłuchań, obowiązki te były realizowane przez zespoły HUMINT z Brygady Rozpoznawczej (MI BDE) czy też innych elementów, jak np. Brygada Monitorowania Pola Walki (Battlefield Surveillance Brigades), skupionych typowo na prowadzeniu przesłuchań. Sytuacja ta wykreowała dwa rodzaje operatorów HUMINT: prowadzących operacje przesłuchań i prowadzenie osobowych źródeł informacji. W związku z tym w armii amerykańskiej pojawiły się różne pomysły na jego rozwiązanie, a mianowicie: częsta rotacja operatorów HUMINT w celu zdobywania różnego rodzaju doświadczeń – zarówno jeżeli chodzi o przesłuchania, jak i pracę ze źródłami osobowymi. Wszyscy operatorzy HUMINT powinni przechodzić szkolenie z zakresu przesłuchań jako element podstawowy i obowiązkowy. Trzecim rozwiązaniem jest formalne uznanie dwóch specjalności HUMINT, tj. przesłuchiwania i pracy z osobowymi źródłami informacji[36].

W trakcie operacji w Iraku i Afganistanie dało się zauważyć także kilka innych problemów dotyczących odpowiedzialności HUMINT i relacji z dowódcami, np.: traktowanie rozpoznania osobowego przez dowódców jako elementu pasywnego i przydzielanie po jednym operatorze HUMINT do każdej kompanii manewrowej; wyznaczanie HUMINT do realizacji zadań niezwiązanych z rozpoznaniem osobowym, takich jak: wypytanie taktyczne (TQ – *tactical questioning*), badanie dokumentów (DOCEX) czy wypytywanie uczestników patroli (*patrol debriefs*); angażowanie HUMINT w operacje typowego rozpoznania wojskowego (*reconnaisance*) bez możliwości wchodzenia w interakcje z ludnością lokalną, co uniemożliwiało tworzenie warunków do przyszłego werbowania osobowych źródeł informacji; brak zrozumienia dla działalności HUMINT ze strony dowódców, mylenie przesłuchania z taktycznym wypytywaniem, co skut-

[34] Tamże.

[35] Przesłuchanie (*interrogation*) jest bardzo ważnym źródłem informacji, o czym świadczy operacja zabicia Osamy bin Ladena. Jedna z wersji głosi, że pierwsze informacje, które naprowadziły agentów CIA na trop bin Ladena, pochodzą ze stycznia 2004 r., kiedy to siły kurdyjskie zatrzymały kuriera Al-Kaidy – Pakistańczyka o nazwisku Hassan Ghul. Wykonywał on wówczas zadanie polegajace na dostarczeniu listu od lidera terrorystów w Iraku Abu Musaba Zarqawiego do bin Ladena. Ghul został przetransportowany do jednego z tajnych więzień CIA. W trakcie przesłuchań początkowo wykazywał odporność na presję fizyczną, w związku z czym zastosowano bardziej wyrafinowane techniki mające na celu złamanie jego oporu. Po ich zastosowaniu Ghul przekazał m.in. pseudonim kuriera bin Ladena – Abu Ahmeda al-Kuwaiti, *Trial to Bin Laden began with CIA detainee, officials say* [online], „Los Angeles Times", http://www.latimes.com/news [dostęp: 05 V 2011].

[36] C. Payne, Ch. LeBoeuf, *HUMINT from COIN to FSO…*, s. 24–25.

kowało odwoływaniem spotkań ze źródłami osobowymi na rzecz prowadzenia TQ; ścisłe egzekwowanie przepisów ochrony wojsk (*Force Protection*) wobec wszystkich żołnierzy, co uniemożliwiało realizację zadań przez HUMINT w związku z brakiem swobody przemieszczania się; zmuszanie HUMINT do przemieszczania się w ramach dużych, dobrze chronionych patroli, co miało negatywny wpływ na pracę z osobowymi źródłami informacji[37].

Jednym z ważniejszych problemów w pracy HUMINT jest brak pełnego zrozumienia sytuacji na teatrze przez operatorów HUMINT. Skupieni i zajęci pracą ze źródłami nie rozumieją oni całego szeregu zależności. Powoduje to, że niezaznajomieni z pracą analityczną operatorzy wykorzystują te źródła informacji, które są najbardziej rozmowne, ale nie najlepsze i najcenniejsze. Bez znajomości całego systemu powiązań operatorzy HUMINT nie są w stanie w pełni odpowiadać na wymagania informacyjne dowódców. W takich przypadkach bezpośrednie wsparcie analityków powoduje, że działania HUMINT stają się precyzyjniejsze, efektywniejsze, a rezultat ich pracy nie jest marnotrawiony. Dzięki temu przy mniejszej liczbie zespołów HUMINT osiąga się takie same wyniki, jak przy ich większej liczbie[38].

Kontrwywiad – zakres odpowiedzialności oraz specyfika pracy

Drugą najważniejszą sekcją w ramach 2X jest Sekcja Operacyjna KW (CICA – Counterintelligence Coordinating Authority) koordynująca działalność wszystkich elementów KW działających na rzecz rozmieszczonych wojsk. W przypadku funkcjonowania na tym samym terenie różnych 2X, jej część kontrwywiadowcza jest odpowiedzialna m.in. za integrację, synchronizację i neutralizowanie konfliktów całości podległych elementów KW. Komórka jest także odpowiedzialna za analizę możliwości i struktury organizacyjnej systemu rozpoznawczego przeciwnika, w tym organizacji terrorystycznych czy rebeliantów, oraz planowanie przedsięwzięć neutralizujących jego działalność, osiągane m.in. poprzez rozpoznawanie jego możliwości i podejmowanie na tej podstawie czynności zaradczych[39].

Sekcja analityczna KW prowadzi m.in.:

- analizę możliwości rozpoznawczych zagranicznych organizacji i służb specjalnych zaangażowanych w działalność terrorystyczną i działania sabotażowe,
- planowanie działań związanych z ochroną wojsk (FP) z wykorzystaniem posiadanych możliwości technicznych,
- analizę możliwości technicznych przeciwnika w zakresie HUMINT, IMINT, SIGINT i MASINT w celu planowania środków umożliwiających ich neutralizację,
- działania podczas informacyjnego (rozpoznawczego) przygotowania rejonu działań bojowych (IPB – *Intelligence Preparation of Battlefield*)[40],

---

[37] Tamże.

[38] E. Epp, J. Thornton, *The Joint HUMINT Analysis and Targeting Course: Analytical Support to Military Source Operations as a Combat Multiplier* [online], „Military Intelligence Professional Bulletin" 2010, s. 29–30, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

[39] *Counterintelligence*.

[40] IPB składa się z czterech części: zdefiniowanie środowiska konfliktu (*definition of the battlefield environment*), opis wpływu środowiska konfliktu na operację (*description of the battlefield's effects*), ocena zagrożeń (*evaluation of the threats*) oraz określenie możliwych wariantów działania przeciwnika (COAs – *course of action*) oraz zagrożeń z tym związanych. *Intelligence Preparation of the Battlefield*, FM 34–130, Washington 1994, s. 1.

- przygotowanie i dystrybucję produktów kontrwywiadowczych,
- przygotowanie wymagań informacyjnych dla KW,
- analizę wiarygodności źródeł i rzetelności przekazywanych przez nich informacji jako wsparcia dla operatorów KW,
- identyfikację obszarów wymagających rozpoznania,
- wsparcie HAC w zakresie łączenia informacji KW z HUMINT oraz przygotowanie takich produktów analitycznych, jak: oceny kontrwywiadowcze, listy celów, produkty czy grafiki jako wsparcie dla dowódcy.

KW może funkcjonować podobnie jak HUMINT – samodzielnie lub w ramach OMT, a zespół KW posiada podobną do HUMINT strukturę[41].

W tym miejscu warto wspomnieć o zasadniczych różnicach w działalności HUMINT i KW. Dość często w środowisku wojskowym, szczególnie nierozpoznawczym, elementy te są mylone, co z kolei powoduje dodatkowe problemy dla KW i HUMINT. HUMINT w zdecydowanej większości przypadków zajmuje się zbieraniem informacji zgodnie z wymaganiami informacyjnymi dowódcy – PIR. Działalność HUMINT powinna wynikać z tych oczekiwań, a zebrane informacje – dawać możliwość przygotowania odpowiedzi na nie.

W dokumentach doktrynalnych USA kontrwywiad jest charakteryzowany jako dyscyplina rozpoznania odpowiedzialna za neutralizowanie działalności rozpoznawczej przeciwnika skierowanej przeciwko siłom własnym i sojuszników. Swoje działania realizuje poprzez uzyskiwanie informacji o charakterze kontrwywiadowczym, prowadzenie dochodzeń kontrwywiadowczych, realizację operacji, analizę i przygotowywanie produktów kontrwywiadowczych czy stosowanie urządzeń technicznych. KW obejmuje wszelkie działania mające na celu wykrywanie, identyfikację, badanie, analizę i neutralizowanie wszelkiej działalności rozpoznawczej sił sojuszniczych, konkurentów, przeciwników czy wrogów[42].

Głównym celem działalności kontrwywiadowczej jest przeciwdziałanie rozpoznaniu przeciwnika skoncentrowanemu na pozyskiwaniu informacji dotyczących personelu USA, aktywności tego kraju odnośnie do prowadzonych operacji, planowania, wyposażenia, obiektów, publikacji, technologii, dokumentów jawnych i niejawnych, mogącemu mieć negatywny wpływ na bezpieczeństwo i interesy USA. Zwalczanymi przeciwnikami są organizacje i struktury narodowe, międzynarodowe, sojusznicze, wrogie, rządowe i pozarządowe, firmy komercyjne, biznesowe, korporacyjne, agencje, ugrupowania terrorystyczne, kryminalne, partyzanckie i inne, demonstrujące postawy, poglądy czy opinie sprzeczne z interesami USA[43].

System szkolenia

Amerykanie przywiązują dużą wagę do szkolenia specjalistów z zakresu HUMINT i KW, o czym świadczy duża liczba przeprowadzanych kursów i szkoleń oraz profesjonalne podejście w trakcie ich realizacji. System ten znacznie się zmienił od czasu zimnej wojny i w chwili obecnej wykorzystuje wszystkie najnowsze doświadczenia.

Przed operacją w Iraku, a szczególnie w Afganistanie, operatorzy HUMINT byli przygotowywani do prowadzenia przesłuchań na poziomie podstawowym, prowadze-

[41] *Counterintelligence*.

[42] Tamże.

[43] Tamże.

nia strategicznych rozmów i wypytywań oraz działalności związanej ze zbieraniem informacji od osób. Dodatkowo byli odpowiedzialni za DOCEX. W trakcie operacji Enduring Freedom w Afganistanie okazało się, że ich trening był niewystarczający z uwagi na skomplikowane warunki misji afgańskiej. Poza brakami jakościowymi występowały też braki ilościowe, szczególnie jeśli chodzi o najbardziej doświadczonych specjalistów. Z uwagi na potrzebę zdobywania wiarygodnych informacji, zgłaszaną przez dowódców, HUMINT musiał szybko adaptować się do nowych warunków. Konieczne doświadczenia zdobywano w walce i nie znajdowało to odzwierciedlenia w odpowiednio sformalizowanym treningu. W związku z koniecznością uwzględniania nowych doświadczeń w formalnym szkoleniu specjalistów HUMINT powołano do życia Połączone Centrum Doskonalenia HUMINT HT-JCOE (HUMINT Training-Joint Center of Excellence). Szczególną uwagę skupiono na profesjonalnym przygotowaniu w zakresie pracy z osobowymi źródłami informacji (*military source operations*), a także na prowadzeniu przesłuchań i strategicznym debriefingu. Szkolenia są prowadzone przez najbardziej doświadczonych praktyków, którzy stacjonowali w Iraku i Afganistanie, i uwzględniają szczególnie najnowsze doświadczenia z tych krajów. Zapraszani są także najlepsi fachowcy z innych agencji i organizacji narodowych USA[44].

W HT-JCOE prowadzi się 11 typów kursów, z których do najważniejszych należą: Joint HUMINT Officer Course, Source Operations Course, Joint Interrogation Management Course, Advanced Source Operations Course oraz Joint Source Validation Course[45].

W ramach HT-JCOE funkcjonuje kilka wydziałów odpowiedzialnych za zakres szkolenia w ramach odpowiednich kursów. Trzy najważniejsze to:

I Wydział Prowadzenia Operacji związanych z Osobowymi Źródłami Informacji (MSOB – Military Source Operation Branch), który organizuje takie kursy, jak:
   - Source Operation Course (SOC) – Kurs prowadzenia osobowych źródeł informacji,
   - Advanced Source Operations Course (ASOC) – Zaawansowany kurs prowadzenia osobowych źródeł informacji,
   - Joint HUMINT Officer Course (JHOC) – Połączony oficerski kurs HUMINT,
   - Joint Source Validation Course (JSVC) – Połączony Kurs Oceny Źródeł,
   - Joint Foreign Materiel Acquisition Course – (JFMAC) – Połączony kurs pozyskiwania zagranicznych materiałów.

II Wydział Prowadzenia Rozmów (Uzyskiwania Informacji – The Debriefing Branch) organizuje kurs:
   - Defense Strategic Debriefing Course (DSDC) – Strategiczny obronny kurs prowadzenia rozmów.

III Wydział Przesłuchań (The Interrogation Branch) odpowiada za organizację następujących kursów:
   - Joint Senior Interrogator Course (JSIC) – Połączony kurs przesłuchań dla starszych specjalistów,

---

[44] J.R. Szypko, *Commander's Note, Defense Human Intelligence (HUMINT): Out of the Shadows, into the Limelight, and Under the Gun-Implications for Training and Educating Military HUMINT Professionals*, „Military Intelligence Professional Bulletin" 2010, s. 3–4, http://www.fas.org/irp/agency/army/mipb/index.html [dostep: 26 XII 2012].

[45] J. Turner, *Senior Enlisted Advisor's Note*, „Military Intelligence Professional Bulletin" 2010, s. 5, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

- Joint Interrogation Certificate Course (JICC) – Certyfikowany połączony kurs przesłuchań,
- Joint Interrogation Management Course (JIMC) – Połączony kurs zarządzania przesłuchaniami,
- Joint Analyst and Interrogator Collaboration Course (JAICC) – Połączony kurs analityczny i przesłuchań – integracja informacji.

W artykule zostaną omówione tylko trzy kursy, po jednym prowadzonym przez każdy wydział. Pozwoli to zrozumieć stopień skomplikowania takiego procesu nauczania oraz konieczność zaangażowania w niego wielu osób.

Zaawansowany kurs prowadzenia osobowych źródeł informacji – ma na celu przygotowanie specjalistów HUMINT do prowadzenia operacji z osobowymi źródłami informacji w środowisku zagrożenia niezależnie od położenia geograficznego. Głównym zadaniem operatorów HUMINT jest nauka zbierania informacji na temat struktur terrorystycznych, rebelianckich i grup kryminalnych oraz nauka zbierania informacji w środowisku wrogim. Kurs ten jest organizowany trzy razy w roku, grupa liczy 42 osoby, a po jego ukończeniu kursanci otrzymują certyfikat pierwszej kategorii upoważniający ich do prowadzenia operacji ze źródłami osobowymi. Zasady kursu, takie jak jego szybkie tempo, sposób oceniania czy łączenie teorii z praktyką – wyglądają podobnie jak w przypadku Source Operation Course. Podczas szkolenia poruszane są następujące zagadnienia: pisanie raportów, wykorzystywanie funduszu operacyjnego, kwestie prawne, cykl HUMINT-owski czy prowadzenie i wykrywanie obserwacji. Zajęcia praktyczne odbywają się w różnych warunkach terenowych i geograficznych. Absolwenci powinni być także w stanie samodzielnie prowadzić pracę operacyjną na rzecz brygadowych grup bojowych (BCT – Brigade Combat Team) w warunkach zagrożenia oraz w przypadku kontaku z wrogimi służbami specjalnymi. Kandydaci na tego typu kurs są wybierani przez specjalną komisję, która bierze pod uwagę takie czynniki, jak wcześniej zdobyte doświadczenia, ukończone szkolenia i kursy, a także możliwość przyszłego wykorzystania kandydata. Komisja zbiera się nie później niż 45 dni kalendarzowych przed rozpoczęciem każdej edycji. Następnie wybrani kursanci otrzymują list, w którym zawarte są instrukcje dotyczące przybycia na kurs i przygotowania się do niego[46].

Strategiczny obronny kurs prowadzenia rozmów – jest to najstarszy kurs, prowadzony od 1983 r. Przed powstaniem HT-JCOE był organizowany przez amerykański Departament Obrony (DOD – Department of Defense). Kurs ten trwa pięć tygodni i odbywa się osiem razy w roku. Po jego ukończeniu słuchacze otrzymują certyfikat DOD strategic debriefers. Najważniejszym celem jest nauczenie kursantów sztuki prowadzenia rozmów z osobami, które zazwyczaj dobrowolnie przekazują informacje. Rozmowy te powinny być prowadzone na poziomie strategicznym, a rozmówcami (źródłami informacji) powinni być obywatele amerykańscy lub obcokrajowcy. Celem kursu nie jest nauczanie zwykłego zadawania pytań i pisania notatek po zakończonych spotkaniach. Instruktorom zależy na przedstawieniu całego procesu przygotowania spotkania, prowadzenia rozmowy, budowania relacji, robienia notatek, a także radzenia sobie z całym spektrum niespodziewanych problemów mogących wyniknąć w trakcie spotkania. Z uwagi na rangę kursu i jego przydatność, słuchacze są werbowani niemal

[46] J. Woodward, *Military Source Operation Branch*, „Military Intelligence Professional Bulletin" 2010, s. 9, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

ze wszystkich amerykańskich rodzajów wojsk, agencji i struktur zajmujących się zbieraniem informacji rozpoznawczych.

Już od pierwszego dnia kursu słuchacze są łączeni w zespoły, w których ramach mogą działać żołnierze i cywile mający za sobą praktykę lub tylko ukończone podstawowe szkolenia HUMINT. Dzięki temu kursanci wymieniają się doświadczeniem zarówno bojowym, jak i zdobytym w trakcie pracy na stanowiskach w kraju. W ramach jednego zespołu mogą pracować na przykład doświadczony sierżant z Iraku czy Afganistanu i młody adept DIA (Defense Intelligence Agency). Słuchacze z DIA mogą pomóc w pisaniu raportów młodym operatorom HUMINT, studenci z CENTCOM (US Central Command) natomiast– podzielić się swoim doświadczeniem z zakresu PIR, dzięki czemu inni mogą się dowiedzieć, na czym należy się skupić w trakcie spotkania z potencjalnym źródłem informacji. Interesujące jest to, że w szkoleniu bierze udział coraz więcej kobiet, co także jest wynikiem ostatnich doświadczeń nabytych w Iraku i Afganistanie. Normalnie w ramach każdego kursu 10–15 proc. wszystkich słuchaczy to kobiety. Inną ciekawostką jest uczestnictwo w kursie żołnierzy, którzy odnieśli rany w boju w Iraku i Afganistanie (niektórzy z nich są pozbawieni kończyn). Wzbogacają oni kurs swoim doświadczeniem bojowym, zdobywanym w specyficznych warunkach, zarażają silną motywacją, a jednocześnie zdobywają nowe umiejętności przydatne na stanowiskach związanych z rozpoznaniem[47].

Kurs DSCC podzielony jest na trzy fazy:

1) faza pierwsza zawiera głównie elementy szkolenia teoretycznego, takie jak teoria działalności HUMINT, prowadzenie rozmów oraz system i sposoby meldowania o zdobytych informacjach. Słuchacze szczegółowo poznają techniki i metody zadawania pytań, uczą się robienia notatek w trakcie rozmów, pisania raportów, są także zapoznawani z oprogramowaniem wykorzystywanym przez HUMINT. Następnie sporządzają raporty oraz prowadzą spotkania, w których trakcie ćwiczą wybrane elementy. Na tym etapie wszelkie problemy kursantów są ściśle monitorowane w celu zidentyfikowania dodatkowych elementów, które powinny być omówione lub przećwiczone,
2) w drugiej fazie szkolenia przechodzi się od zajęć teoretycznych do praktycznych. Każdego dnia słuchacze prowadzą spotkania, w których trakcie muszą uzyskać informacje w zależności od możliwości rozmówcy. Na tym etapie słuchacze ćwiczą całą teorię poznaną wcześniej. Etap ten charakteryzuje się także dużą liczbą tzw. role playerów, czyli osób odgrywających role potencjalnych kontaktów. Osobami tymi są instruktorzy, którzy przy okazji mają możliwość dokonania oceny postępów słuchaczy. Duża wagę przywiązuje się do tego, aby słuchacze przećwiczyli jak największą liczbę różnych sytuacji, przechodząc cały proces, tj. planowanie spotkania, przygotowanie się do niego, prowadzenie spotkania i pisanie raportów. Instruktorzy każdorazowo starają się tworzyć dodatkowe epizody, czasem bardzo trudne i wymagające, dzięki którym słuchacze zyskują nowe umiejętności i pewność siebie. Rozmowy są prowadzone z przeróżnymi osobami: od prostych żołnierzy do naukowców, co wymusza odpowiednie przygotowanie, szczególnie jeżeli chodzi o sposób zadawania pytań. Zwracana jest uwaga nie tylko na technikę prowadzenia

[47] J. Parker, D. Russell, T. Pahle, *Debriefing Branch, Defense Strategic Debriefing Course*, „Military Intelligence Professional Bulletin", October–December 2010, s. 19–20, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

spotkania czy zadawania pytań, lecz także na budowanie relacji bez względu na charakter rozmówcy, co ma w przyszłości znacznie poprawić skuteczność pracy[48],

3) trwająca sześć dni faza trzecia, zwana Strategic Operations Exercise (SOX), jest – według słuchaczy – najbardziej efektywną z całego kursu. Na tym etapie kursanci sami aranżują spotkania, planują je, uwzględniając własne obciążenie pracą, realizują spotkania w miejscach publicznych i sporządzają raporty informacyjne[49].

Połączony kurs przesłuchań dla starszych specjalistów trwa 15 dni i jest organizowany w Fort Huachuca w Arizonie. Jest on skierowany do starszych i doświadczonych specjalistów z zakresu przesłuchań i zapewnia dodatkowe umiejętności dotyczące technik, metodologii i strategii podejścia do przesłuchania, przepytywania, pisania i analizowania raportów oraz ich publikowania, a także dodatkowej profesjonalizacji personelu HUMINT. Kurs ma przygotować do prowadzenia przesłuchań na wszystkich szczeblach szkolenia młodszych specjalistów od przesłuchań oraz analizy zachowań ludzkich. Dodatkowo dyskutowane i ćwiczone są takie elementy, jak źródła informacji, systemy i oprogramowanie wykorzystywane w czasie działalności statutowej, eksploatacja otwartych (ogólnodostępnych) źródeł informacji, raporty informacyjne, wykorzystywanie tłumaczy, działalność HUMINT jako wsparcie operacji rozpoznawczych, obserwacja i rozpoznanie oraz rola HUMINT w operacji typu COIN. W trakcie kursu, podobnie jak w przypadku wyżej opisanego szkolenia, słuchacze odbywają praktyczne zajęcia, po których sporządzają odpowiednie raporty. Instruktorzy starają się maksymalnie wykorzystać wszystkie formy i metody nauczania tj. wykłady, praktyczne ćwiczenia elementów i całych przesłuchań czy dyskusje, co ma rozwinąć w słuchaczach krytyczne myślenie. Na zajęcia zapraszani są także goście i specjaliści z zewnątrz, którzy dzielą się swoją wiedzą i doświadczeniem, a także odpowiadają na wszelkie pytania i wątpliwości słuchaczy. Rocznie organizowanych jest dziewięć edycji kursu, każda po 12 osób[50].

Zakończenie

Należy zauważyć, że czym innym jest budowanie struktur 2X i szkolenie personelu odpowiedzialnego za kierowanie tą komórką, a czym innym przygotowanie specjalistów i operatorów z zakresu HUMINT czy KW. Oczywiście, aby sprawnie funkcjonować w ramach komórki 2X, niezbędne jest doświadczenie operacyjne zdobyte w terenie. Dodatkową trudnością bywa to, że operatorzy HUMINT czy KW, doskonale radzący sobie w działalności operacyjnej, nie zawsze sprawdzają się w komórce 2X, która jest komórką sztabową i kieruje się innymi zasadami.

W przypadku niektórych misji (jak ISAF) zmienia ona swój charakter ze stabilizacyjnego na szkoleniowy, co z kolei wymaga od komórki 2X czy operatorów HUMINT i KW wykazania się zdolnościami z zakresu mentoringu afgańskich sił i służb bezpieczeństwa, szczególnie jeżeli chodzi o szkolenie afgańskiego HUMINT i KW. To z kolei wymaga kompetencji instruktorskich, co nie jest takie oczywiste, pomimo posiadania odpowiedniej wiedzy merytorycznej czy doświadczenia. W przypadku Afganistanu

[48] Tamże.

[49] Tamże.

[50] S. Frelke, *Joint Senior Interrogator Course, The Art and Science of Experience* [online], „Military Intelligence Professional Bulletin" 2010, s. 26–27, http://www.fas.org/irp/agency/army/mipb/index.html [dostęp: 26 XII 2012].

niezbędna jest wiedza na temat mentalności Afgańczyków oraz znajomości historii tego kraju. Inaczej bowiem należy postępować z żołnierzami afgańskimi starszej daty, z wiedzą i doświadczeniem przekazanymi im przez wojska radzieckie, a inaczej z młodym pokoleniem, które w większości uzyskuje pierwsze doświadczenia i wiedzę od sił ISAF. Niejednokrotnie w ramach jednej komórki znajdziemy ludzi z dwóch różnych generacji i o dwóch różnych światopoglądach. Kwestia ta jest istotna szczególnie teraz, w związku z zagrożeniem atakami Green on Blue[51]. Nakłada to na KW dodatkowe obowiązki związane nie tylko z odpowiednio wczesnym wykrywaniem zagrożenia, ale także szkoleniem sił afgańskich, aby mogły same radzić sobie z tym wyzwaniem.

Należy w pewnym stopniu podziwiać Amerykanów za szybkość i elastyczność w podejściu do rozpoznania. Wnioski zdobywane w trakcie misji są dyskutowane i uwzględniane natychmiast w trakcie jednej zmiany – jak to miało miejsce w Iraku czy Afganistanie – a nie po kilku latach lub wcale. Dodatkowo jest rozwijany cały system szkolenia oraz wsparcia technicznego i informatycznego działań realizowanych na teatrze.

W epoce zagrożenia atakami terrorystycznymi i konfliktami asymetrycznymi HUMINT i KW pozostają najbardziej elastycznymi i efektywnymi źródłami informacji. Elementy te można przemieścić w dowolnym czasie w dowolny obszar na kuli ziemskiej. W wielu przypadkach, szczególnie na terenie państw Trzeciego Świata, ich przydatność jest ogromna ze względu na ograniczenia w wykorzystaniu technicznych środków rozpoznawczych z powodu słabej infrastruktury technicznej. Elementy HUMINT i KW są niezwykle istotne w przypadku wojny obronnej, gdzie w zależności od rozwoju sytuacji mogą prowadzić czynności związane zarówno ze zbieraniem istotnych informacji o przeciwniku, jak i rozpoznanie elementów dywersyjnych przeciwnika lub neutralizować wysiłek obronny. W przypadku takiej konieczności operatorzy HUMINT czy KW mogą z powodzeniem tworzyć struktury podziemne i prowadzić działania dywersyjne[52].

Abstrakt

W artykule przedstawiono wybrane aspekty działalności rozpoznania osobowego (HUMINT) i kontrwywiadu (KW), opierajac się na doświadczeniach amerykańskich wyniesionych z konfliktów w Iraku i Afganistanie. Działalność obu tych metod rozpoznania została scentralizowana w ramach komórki 2X, która od momentu jej powstania w latach 90. XX wieku odpowiada za kierowanie i koordynację działalnością KW i HUMINT w danym rejonie operacji. Komórka ta z roku na rok zyskuje coraz większe znaczenie głównie z uwagi na skuteczność podporządkowanych jej elementów. W tak szczególnych warunkach, jak prowadzenie konfliktu typu COIN, obie te dyscypliny dostarczają około 80 proc. wszystkich informacji rozpoznawczych. Z uwagi na skuteczność tych metod we wcześniej wspomnianych konfliktach ich rola znacznie wzrosła. W USA, a także w innych państwach NATO, w ostatnim czasie nastąpił znaczny wzrost ilościowy i jakościowy elementów HUMINT i KW. Rozbudowany system szkolenia,

[51] Ataki „Green on Blue" dotyczą sytuacji dokonywania ataków przez przedstawicieli afgańskich sił i służb bezpieczeństwa na przedstawicieli ISAF.

[52] W okresie II RP większość oficerów Oddziału II SG pełniła tam służbę na etatach zewnętrznych przez pięć lat, po czy wracała do jednostek liniowych. W konsekwencji takiej polityki po 20 latach niepodległości w Wojsku Polskim pracowało tysiące osób zapoznanych z zasadami pracy operacyjnej wywiadu czy kontrwywiadu. Można założyć, że był to główny czynnik, który pozwolił błyskawicznie utworzyć z powodzeniem polskie zbrojne struktury podziemne w okresie okupacji.

przy jego niezbyt wysokich kosztach, oraz duża elastyczność wykorzystania tych metod w połączeniu z ich dużą skutecznością, uczyniły je w ostatnim czasie najważniejszym środkiem rozpoznawczym, niezwykle trudnym do zastąpienia. Techniczne środki rozpoznania, takie jak: IMINT, SIGINT, TECHINT czy MASINT stanowią tylko uzupełnienie działań komórek wykorzystujących osobowe źródła informacji.

Abstract

In the article the chosen element of Counterintelligence (CI) and HUMINT have been presented, based on the US experience from Iraq and Afghanistan. The activities of both have been centralized by staff element such as 2X cell, which from the beginning, it means early 90, coordinates and manages all the HUMINT and CI activities in the Area of Responsibility (AOR). The 2X cell from the beginning start to be more and more important because of the HUMINT and CI intelligence value. In the condition of COIN operation about 80% of all intelligence is based on the mentioned intelligence disciplines. Based on the Iraq and Afghanistan experience, the role of HUMINT and CI considerably increased what influenced their training system. Also, other than US, NATO members start to improve the quality and quantity of the HUMINT and CI elements. The quite low cost comparing with the high effectiveness and flexibility made both of the disciplines really difficult to replace. Technical intelligence disciplines such as TECHINT, MASINT, SIGINT or IMINT can only support the leading discipline like HUMINT and CI, which use mainly the human source of information.

Krzysztof Krełowski

Kontratyp w uprawnieniach ABW i MI5

Nie czyni bezprawia, kto spełnia swą powinność

Artykuł 235 kodeksu karnego[1] penalizuje działanie polegające na podstępnym doprowadzeniu do wszczęcia postępowania karnego. Z takiej perspektywy można spojrzeć na ogół czynności operacyjnych podejmowanych przez służby kontrwywiadowcze. Posługiwanie się dokumentami legalizacyjnymi, legendowanie działań, kontrola operacyjna, działanie pod przykryciem itd. to swego rodzaju podstęp ukierunkowany na wszczęcie postępowania karnego. Każde z wymienionych wyżej działań wyczerpuje dodatkowo formalne znamiona odrębnych czynów zabronionych przez kodeks karny, jak np. posługiwanie się dokumentami stwierdzającymi nieprawdę, udział w grupie przestępczej itp.

W tym kontekście rodzi się pytanie, jakie przepisy bądź konstrukcje prawne „przywracają" legalność działań funkcjonariuszy wypełniających formalne znamiona przepisów ustawy karnej.

Okoliczności wyłączające bezprawność czynu noszą w nauce nazwę kontratypów. Czyn noszący formalne znamiona przestępstwa nie jest bezprawny w pewnych, określonych, okolicznościach.

Można więc postawić tezę, że podstawą pracy służb policyjnych i specjalnych w ujęciu prawnokarnym jest konstrukcja kontratypu.

Kontratypy można podzielić na kodeksowe – unormowane przez kodeks karny – oraz pozakodeksowe. Kontratypy kodeksowe to obrona konieczna, stan wyższej konieczności, eksperyment naukowy, udział w zawodach sportowych, błąd co do prawa i błąd, co do okoliczności faktycznych. Jako kontratyp można potraktować także brak winy bądź szkodliwości społecznej czynu. Z punktu widzenia działania służb istotniejsze są jednak kontratypy pozakodeksowe, wśród których pierwszorzędne znaczenie ma kontratyp działania w ramach szczególnych uprawnień i zezwoleń (na ten temat szeroko wypowiedzieli się W. Wolter oraz W. Wróbel i A. Zoll)[2].

Policjant stosujący środki przymusu bezpośredniego, posługujący się na przykład pałką lub paralizatorem, nie popełnia przestępstwa, jeśli działa w warunkach określonych prawem. Odpowiedzialność karną wyłącza tu fakt działania w ramach uprawnień. Ustawy określające uprawnienia funkcjonariuszy są przepisami szczególnymi w stosunku do kodeksu karnego i przez to, na zasadzie *lex specialis derogat legi generali*[3] – wyłączają jego działanie.

---

[1] Ustawa z dn. 6 czerwca 1997 r., Dz.U. Nr 88, poz. 553 ze zm.

[2] W. Wolter, *Zarys systemu prawa karnego. Część ogólna*, Kraków 1933, s. 135 oraz W. Wróbel i A. Zoll, *Polskie prawo karn*e. *Część ogólna*, Kraków 2010, s. 373.

[3] *Lex specialis derogat legi generali* – łac. 'ustawa szczególna uchyla ustawę ogólną'.

W praktyce sprawa ta nie wygląda jednak tak prosto. Kontratyp w ustawie o ABW oraz AW[4] (dalej *Ustawa*) skonstruowany jest w sposób niejednolity.

Nie czyni bezprawia, kto spełnia swą powinność

Przykładem poprawnie skonstruowanego kontratypu są następujące przepisy *Ustawy*:

1) art. 23 – wydawanie poleceń określonego zachowania, zatrzymywanie osób, przeszukanie osób i pomieszczeń, kontrola osobista, przeglądanie bagażu oraz obserwowanie i rejestrowanie zdarzeń,
2) art. 25 – użycie środków przymusu bezpośredniego,
3) art. 26 – użycie broni palnej,
4) art. 27 – kontrola operacyjna.

Ustawa nadaje we wskazanych przepisach określone uprawnienia, które tym samym wyłączają stosowanie kodeksu karnego. Regułę tę wyraża rzymska paremia: *Non facit fraudem, qui facit, quod debet* (nie czyni bezprawia, kto spełnia swą powinność).

Podwójna garda?

Nieprawidłowe z legislacyjnego i logicznego punktu widzenia są przepisy art. 32 ust. 1 i art. 35 ust. 6 *Ustawy*. Artykuł 32 ust. 1 brzmi:

„Nie popełnia przestępstwa, kto, będąc do tego uprawnionym, wykonuje czynności określone w art. 29 ust. 1, jeżeli zostały zachowane warunki określone w art. 29 ust. 3, a także kto wykonuje czynności określone w art. 30 ust. 1".

W art. 29 jest mowa o zakupie kontrolowanym, w art. 30 zaś o przesyłce niejawnie nadzorowanej.

Artykuł 35 dotyczy posługiwania się dokumentami legalizacyjnymi. Ustęp 6 tego przepisu brzmi:

„6. Nie popełnia przestępstwa:
   1) kto poleca sporządzenie lub kieruje sporządzeniem dokumentów, o których mowa w ust. 2 i 3,
   2) kto sporządza dokumenty, o których mowa w ust. 2 i 3,
   3) kto udziela pomocy w sporządzeniu dokumentów, o których mowa w ust. 2 i 3,
   4) funkcjonariusz Agencji lub osoba wymieniona w ust. 3, posługujący się przy wykonywaniu czynności operacyjno-rozpoznawczych dokumentami, o których mowa w ust. 2 i 3".

Konstrukcja polegająca na przyznaniu w jednym przepisie określonych uprawnień, w następnym zaś depenalizująca takie działanie oznacza de facto, że za korzystanie z uprawnień można zostać ukaranym. W państwie prawa to samo działanie nie może być jednocześnie dozwolone przez prawo i nielegalne, a tym bardziej karalne.

Działanie pod przykryciem, czyli udział w grupie przestępczej

Z drugiej strony mamy instytucje niekorzystające z podwójnego zabezpieczenia, a nawet takie, których legalność wynika z ustawy jedynie pośrednio. Legalność funkcjonowania w grupie przestępczej pod przykryciem wynika z przepisów regulujących instytucję zakupu kontrolowanego (art. 29 *Ustawy*). Choć artykuł ten nie zezwala

[4] Ustawa z dn. 24 maja 2002 r., Dz.U. z 2010 r. Nr 29, poz. 154 ze zm.

wprost na prowadzenie pozorowanej działalności przestępczej, to należy konstatować, że przepis prawa musi być możliwy do wykonania, a możliwość taką daje właśnie działanie pod przykryciem. Jest to jednak tylko interpretacja.

Autoryzacja określonych działań

Zgodnie z *Ustawą* zgoda osobnego organu jest wymagana w przypadkach:

1) stosowania kontroli operacyjnej – konieczna jest tu zgoda sądu (art. 27),
2) zakupu kontrolowanego – wymagana jest pisemna zgoda Prokuratora Generalnego (art. 29),
3) przesyłki niejawnie nadzorowanej – w tym przypadku przepis nakłada obowiązek poinformowania Prokuratora Generalnego, który może nakazać zaniechanie tych czynności (art. 30).

Zgoda niezależnego organu jest potrzebna w sytuacji, kiedy określone działania szczególnie głęboko ingerują w konstytucyjne prawa jednostki i jednocześnie nie są to działania nagłe, będące bezpośrednią odpowiedzią na czyn przestępczy. Konieczne są tu dwa elementy: działanie na podstawie ustawy i zgoda podmiotu zewnętrznego. Podmiotem tym będzie sąd lub prokurator.

W polskiej tradycji prawnej istnieje jednak przykład autoryzowania określonych działań przez organ administracji. Legalizację działań pod przykryciem zawierał już przepis art. 2 rozporządzenia prezydenta RP z 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu państwa[5], którego konstrukcja była następująca:

„Art. 2. Działanie nie jest bezprawne wtedy tylko, gdy podjęto je za zezwoleniem udzielonem:

a) przez Ministra Spraw Wojskowych lub upoważnione przez niego organa państwowe – w związku z wykonywaniem zadań ochrony bezpieczeństwa Państwa Polskiego;
b) przez właściwą władzę naczelną lub upoważnione przez nią organa podległe – w związku z wykonywaniem innych zadań państwowych".

Przepis ten, jak widać, nie wyszczególniał działań wypełniających znamiona przestępstwa, które miały być legalizowane przez wydanie zezwolenia. Trzeba jednak zauważyć, że jest on skonstruowany precyzyjnie – nie pozostawia funkcjonariuszom wątpliwości, które działanie jest zgodne z prawem.

Zezwolenie jako podstawa legalizacji określonych działań w legislacji brytyjskiej

Autoryzacja określonych działań przez organ administracji jest podstawą pracy operacyjnej służb brytyjskich. Podstawowym aktem prawnym regulującym tę materię jest *Regulation of Investigatory Powers Act 2000* (*Ustawa o uprawnieniach operacyjnych z 2000 roku,* dalej RIPA). Ustawa ta została uchwalona w odpowiedzi na rozwój nowoczesnych technologii związanych z Internetem i przesyłaniem danych. W miarę precyzyjnie określiła też stosowanie innych, bardziej tradycyjnych metod pozyskiwania informacji, takich jak stosowanie obserwacji, rejestrowanie obrazów i zapisów sytuacji w miejscach publicznych i prywatnych czy prace z osobowymi źródłami informacji. Akt ten jest podstawą pracy operacyjnej przede wszystkim Security Service (MI5),

[5] Dz.U. Nr 94, poz. 851.

Goverment Communications Headquarters (GCHQ) oraz innych formacji, w tym Secret Intelligence Service (MI6), choć ta ostatnia służba działa w pewnej mierze, opierając się na swojej własnej ustawie (*The Intelligence Services Act 1994*), która uwzględnia specyfikę funkcjonowania wywiadu – np. naruszenie własności rzeczy położonej poza terytorium Wielkiej Brytanii. W polskiej ustawie brak takiego zapisu, a miałby on znaczenie istotne – polską ustawę karną stosuje się także wobec obywatela polskiego, który popełnił przestępstwo za granicą (art. 109 kk).

Niniejsze opracowanie dotyczy jedynie uprawnień określonych w RIPA. Jest to tematyka niezmiernie obszerna – RIPA to akt liczący ponad sto stron, do którego dochodzą wydawane na jego mocy przez sekretarzy stanu *Orders*, tj. akty zbliżone do polskich rozporządzeń, zawierające uzupełnienie przepisów ustawy, i wreszcie *Codes of Practice*, tj. *Zasady postępowania* – mające moc prawną dokumenty przeznaczone do praktycznego wykorzystywania przez urzędników dokonujących autoryzacji określonych działań. W sumie jest to kilkaset stron uregulowań dotyczących pracy operacyjnej. W niniejszej publikacji z konieczności ograniczono się jedynie do kilku wybranych kwestii.

Definicja przestępstwa telekomunikacyjnego

Artykuł 1 RIPA definiuje przestępstwo telekomunikacyjne: „Kto umyślnie i bez zgody uprawnionego organu władzy narusza na terenie Zjednoczonego Królestwa tajemnicę komunikowania się…" ("It shall be an offence for a person intentionally and without lawful authority to intercept, at any place in the United Kingdom, any communication…"). Przepis ten sam w sobie zawiera kontratyp, którym jest działanie w ramach uprawnienia. We wcześniejszych uwagach zawartych w niniejszej publikacji został wyrażony pogląd, że działanie w ramach uprawnień w każdym przypadku będzie wyłączać bezprawność czynu. Jak się jednak wydaje, w zapisie tym chodzi o podkreślenie konieczności uzyskania stosownego zezwolenia określonej władzy dla danego działania, co jest istotą RIPA.

Przestępstwo wymienione w artykule 1 RIPA odpowiada czynowi stypizowanemu w art. 267 polskiego kodeksu karnego, ale RIPA opisuje je dużo szerzej i bardziej szczegółowo. Jest to istotne z punktu widzenia zasady zawężającego interpretowania przepisów karnych i zakazu stosowania analogii. Prawo karne jest instrumentem surowym, stąd jego wszelkie interpretacje winny być ograniczane do minimum. Artykuł 1 ust. 3 RIPA stanowi przykładowo, że naruszenie systemu telekomunikacyjnego polegające na uzyskaniu dostępu do przekazu ogólnie dostępnego nie stanowi przestępstwa („References in this Act to the interception of communication do not include references to the interception of any communication broadcast for general reception"). Polska ustawa karna nie zawierała takiego zapisu, a problem był istotny i wymagał ostatecznie rozstrzygnięcia go przez Sąd Najwyższy, co nastąpiło w orzeczeniu z 22 stycznia 2003 r. (IKZP 43/02): „Działanie sprawcy polegające na bezprawnym podłączeniu odbiornika telewizyjnego do sieci kablowej godzi w prawa majątkowe nadawcy programu, nie wyczerpuje jednak znamion przestępstwa określonego w art. 267 kodeksu karnego".

Przestępstwo nieudzielenia informacji uprawnionemu organowi

Instytucją nieznaną w prawie polskim jest przestępstwo polegające na odmowie udzielenia informacji niejawnej funkcjonariuszowi posiadającemu stosowne zezwolenia

– art. 53 *Ustawy*. Informacje niejawne w ujęciu tego przepisu to informacje chronione w sposób dowolny – poprzez zakodowanie itp. Zgodnie z art. 49 tejże *Ustawy* organem wydającym nakaz udzielenia informacji niejawnych jest sąd, co jest pewnego rodzaju wyjątkiem – zasadą bowiem jest wydawanie zezwoleń przez organ administracyjny. Obowiązek ten obejmuje wydanie kodów, programów deszyfrujących itd., tj. narzędzi umożliwiających dostęp do informacji. Skorelowana z tym rozwiązaniem jest konstrukcja przestępstwa nieujawnienia informacji, przewidziana w art. 53. Jest to niewątpliwie narzędzie użyteczne w pracy operacyjnej.

Konstrukcja kontratypu w RIPA

Jak już zostało powiedziane, legalizacja działań służb brytyjskich polega na udzieleniu zezwolenia określanego jako *authorisation* (bądź *warrant* – w najpoważniejszych przypadkach, typu naruszenie własności) przez określony organ administracyjny.

RIPA określa: po pierwsze metodę działania, po drugie cel, któremu ma ona służyć, oraz po trzecie przyporządkowuje tej metodzie rodzaj uprawnienia (ranga podmiotu dokonującego autoryzacji) nadający takiemu działaniu walor legalności. W pewnym uproszczeniu model ten obrazuje poniższa tabela.

Tabela. Konstrukcja kontratypu w RIPA.

Metoda	Cel	Poziom autoryzacji
Kontrola korespondencji i telekomunikacji – *Interception of communication*	Bezpieczeństwo narodowe, prewencja i wykrywanie poważnych przestępstw (definicja poważnego przestępstwa poniżej tabeli), bezpieczeństwo ekonomiczne Wielkiej Brytanii	*Warrant* udzielony przez sekretarza stanu dla Home Office (w Szkocji – Cabinet Secretary for Justice)
Dane telekomunikacyjne (bilingi) – *Use of communication data*	Bezpieczeństwo narodowe, prewencja i wykrywanie przestępstw, zapobieganie zamieszkom, bezpieczeństwo ekonomiczne Wielkiej Brytanii, bezpieczeństwo publiczne, zapobieganie czynnikom niebezpiecznym dla zdrowia powszechnego, odzyskiwanie należności podatkowych i innych danin publicznych, oraz jeśli czyn może skutkować śmiercią lub rozstrojem zdrowia	urzędnik wysokiej rangi danej instytucji (*senior member of that authority*) – RIPA definiuje to pojęcie w odniesieniu do każdej formacji
Obserwacja (śledzenie osób) – *Directed surveillance*	Bezpieczeństwo narodowe, prewencja i wykrywanie przestępstw, zapobieganie zamieszkom, bezpieczeństwo ekonomiczne Wielkiej Brytanii, bezpieczeństwo publiczne, zapobieganie czynnikom niebezpiecznym dla zdrowia powszechnego, odzyskiwanie należności podatkowych i innych danin publicznych	urzędnik wysokiej rangi danej instytucji (*senior member of that authority*)

Osobowe źródła informacji – *Covert human intelligence sources*	Bezpieczeństwo narodowe, prewencja i wykrywanie przestępstw, zapobieganie zamieszkom, bezpieczeństwo ekonomiczne Wielkiej Brytanii, bezpieczeństwo publiczne, zapobieganie czynnikom niebezpiecznym dla zdrowia powszechnego, odzyskiwanie należności podatkowych i innych danin publicznych	urzędnik wysokiej rangi danej instytucji (*senior member of that authority*)
Inwigilacja – ukryta aparatura rejestrująca dźwięk i obraz oraz możliwość naruszania własności – *Intrusive surveillance*	Bezpieczeństwo narodowe, prewencja i wykrywanie poważnych przestępstw, bezpieczeństwo ekonomiczne Wielkiej Brytanii	sekretarz stanu dla Home Office (w Szkocji – Cabinet Secretary for Justice) (możliwość taką posiadają również liczne służby, w pierwszej kolejności policja, a także formacje o charakterze skarbowym lub policji militarnej, najczęściej na podstawie zgody szefa służby, zatwierdzanej przez Komisarza ds. Inwigilacji).

Źródło: Opracowanie własne autora.

RIPA definiuje pojęcie „poważnego przestępstwa" (*serious crime*): zgodnie z tym dokumentem „poważne przestępstwo" wiąże się z użyciem przemocy bądź skutkuje dużymi stratami finansowymi lub jest popełnione przez wiele osób działających we wspólnym celu albo też jest to przestępstwo, w którego przypadku istnieje duże prawdopodobieństwo, że osoba, które je popełniła, mająca ukończone 21 lat, wcześniej nie karana, zostanie skazana na karę co najmniej 3 lat pozbawienia wolności.

Przestępstwo ujawnienia informacji dotyczącej udzielonej autoryzacji

Ustawa brytyjska w odrębny sposób penalizuje czyn polegający na ujawnieniu danych dotyczących autoryzacji, tj. na jaki okres została wydana, komu, w związku z jaką sprawą itd.

Komisarze

RIPA sankcjonuje istnienie niezależnych, choć działających w ramach administracji, organów nadzorczych, którymi są Komisarz ds. Służb Specjalnych oraz Komisarz ds. Ingerencji Telekomunikacyjnych (*Intellegence Services Commissioner* oraz *Interception of Communications Commissioner*). Statuuje też funkcjonowanie Komisarza ds. Uprawnień Operacyjnych dla Irlandii Północnej (*Investigatory Powers Commissioner for Northern Ireland*) oraz rozszerza zakres kompetencji Głównego Komisarza ds. Inwigilacji (*Chief Surveillance Commissioner*) powołanego na mocy ustawy o Policji z 1997 r. Do zadań tych Komisarzy należy nadzór nad wydawaniem zezwoleń dotyczących stosowania określonych metod. W przypadkach ingerencji sięgających najdalej w sferę praw jednostkowych (np. naruszenie własności) zaś konieczne jest uprzednie wyrażenie zgody przez właściwego Komisarza. Komisarze rokrocznie

składają premierowi sprawozdania, które zawierają podstawę prawną i zakres ich kompetencji, opis wykonanych przez nich czynności – liczbę i datę spotkań z przedstawicielami służb, ich przedmiot, liczbę stwierdzonych uchybień (*errors*), studium poszczególnych przypadków i wreszcie ogólną ocenę funkcjonowania służb. Instytucja Komisarzy odgrywa więc istotną rolę w zapewnieniu ochrony praw jednostki przed nieuzasadnioną ingerencją ze strony państwa.

Trybunał do spraw Operacyjnych

RIPA statuuje też istnienie wyspecjalizowanego organu sądowego właściwego w sprawach skarg na czynności operacyjno-rozpoznawcze, które mogłyby naruszyć prawa jednostkowe, w tym zwłaszcza w sprawach związanych z naruszeniem własności bądź tajemnicy telekomunikacyjnej, tj. Investigatory Powers Tribunal (Trybunał do spraw Operacyjnych). Każdy, kto uzna, że jego prawa zostały naruszone, ma prawo wnieść skargę do tego Trybunału. Komisarze obowiązani są świadczyć pomoc w wyjaśnianiu spraw będących przedmiotem prac Trybunału do spraw Operacyjnych.

Zasady postępowania – *Codes of Practice*

Na mocy RIPA oraz innych ustaw (ustawa o Policji z 1997 r.) są wydawane *Zasady postępowania* (*Codes of Practice*). Zgodnie z nazwą mają one wymiar stricte praktyczny – określają przystępnym językiem, w jakich sytuacjach należy wystąpić o jaki rodzaj autoryzacji i jak rozumieć poszczególne terminy. Tekst jest przeplatany przykładami, które jednak, zgodnie z informacją zamieszczoną na początku, nie mają mocy prawnej. *Zasady postępowania* to zbiór publikacji dotyczących naruszania tajemnicy telekomunikacyjnej, tajemnicy korespondencji, naruszania własności nieruchomości i rzeczy ruchomych, stosowania środków umożliwiających rejestrację obrazów miejsc i zdarzeń itd. Są one skierowane do funkcjonariuszy realizujących uprawnienia operacyjne, ale są powszechnie dostępne, w tym na stronach internetowych. Na marginesie mówiąc, zgodnie z informacjami zamieszczonymi na stronach Home Office ambicją tej instytucji jest bycie najbardziej transparentną strukturą o tym charakterze na świecie.

Niejawne osobowe źródła informacji

RIPA inaczej niż art. 36 ustawy o ABW oraz AW definiuje pojęcie osobowych źródeł informacji. Nie ogranicza się w tym jedynie do osób niebędących funkcjonariuszami, jak czyni to *Ustawa*. Rozwiązuje tym samym problem działania funkcjonariuszy działających pod przykryciem. Zgodnie z art. 26 ust. 8 RIPA niejawnym osobowym źródłem informacji (*covert human intelligence source* – dalej CHIS) jest osoba, która:

a) nawiązuje lub utrzymuje osobiste lub inne relacje z drugą osobą w niejawnym celu określonym w punktach „b" lub „c" poniżej,
b) w sposób niejawny wykorzystuje takie relacje do zdobywania informacji lub umożliwienia dostępu do takich informacji innym osobom,
c) w niejawny sposób przekazuje informacje uzyskane przy wykorzystaniu takich relacji.

Zdobywanie informacji poprzez CHIS wymaga zezwolenia. Ustawodawca brytyjski wychodzi z założenia, że kształtowanie relacji międzyludzkich przez organ państwa

jest daleko posuniętą ingerencją w sferę prywatności, wobec czego dopuszczalne jest jedynie w wyjątkowych okolicznościach poprzez autoryzowanie takich działań. Zezwolenie wydawane jest, co do zasady, na okres 12 miesięcy. W szczególnych przypadkach – korzystanie z pomocy osób nieletnich, „podatnych na zranienie" (chodzi o osoby, którym byłaby przynależna pomoc społeczna w związku z niedomaganiem psychicznym lub fizycznym) – autoryzacja jest wydawana wyjątkowo i jedynie na okres jednego miesiąca.

RIPA przewiduje dwa rodzaje autoryzacji w odniesieniu do CHIS, tj. autoryzację wykorzystania osobowego źródła informacji, która ma znaczenie dla władzy publicznej sięgającej po taki środek (*use of a covert human intelligence source*) oraz autoryzację poszczególnych działań (*conduc tof a covert human intelligence source*), która ma znaczenie dla CHIS, jako akt kontratypizujący określone działania. Autoryzacja działania (*conduct authorisation*) nie musi się przy tym odnosić do każdej czynności. Chodzi tu bardziej o autoryzację działań w określonym celu. CHIS nie może więc być wykorzystywane w każdym celu. Nawiasem mówiąc, w pewnych sytuacjach funkcjonariusze sami mogą autoryzować swoje działania. W takich jednak przypadkach obowiązani są umieścić stosowną notatkę w rejestrze autoryzacji prowadzonym przez każdą z upoważnionych formacji. Tego typu autoryzacje podlegają szczególnemu nadzorowi ze strony Komisarzy.

Ograniczenia w korzystaniu z CHIS

System brytyjski nie zawiera ograniczeń podmiotowych dotyczących funkcjonariuszy państwa, z którymi współpraca jest zabroniona. Katalog taki zawiera natomiast art. 37 ustawy o ABW oraz AW. Zbiór ten jest szeroki i obejmuje przedstawicieli wszystkich trzech władz oraz mediów. Zwłaszcza ta ostatnia kwestia, a mianowicie zakaz tajnej współpracy z dziennikarzami, nastręcza wielu problemów. Czy osoba sporadycznie publikująca teksty w czasopiśmie hobbistycznym jest dziennikarzem, czy nie? Sprawa jest o tyle istotna, że ustawa o ABW oraz AW przewiduje sankcję karną za nieuprawnione podejmowanie tajnej współpracy z dziennikarzami.

Ustawodawstwo brytyjskie idzie w innym kierunku. RIPA kładzie nacisk na ochronę jednostki przed działaniem służb. Przykładowo *The Regulation of Investigatory Powers (Juveniles) Order 2000* – akt prawny wydany przez sekretarza stanu – określa warunki wykorzystania nieletnich CHIS. Zgodnie z nim dozwolone jest korzystanie z pomocy CHIS, które ukończyły 16 rok życia. W wyjątkowych sytuacjach możliwe jest wykorzystanie CHIS poniżej tej granicy. W takim wypadku konieczne jest zapewnienie udziału dorosłego opiekuna w jego spotkaniach z funkcjonariuszem. W odniesieniu do CHIS poniżej 18 roku życia na pierwszy plan wysuwa się kwestia uniknięcia „zranień psychicznych" takiej osoby oraz wyczerpującego przedstawienia różnego rodzaju ryzyka związanego z taką działalnością. Niedopuszczalne jest zdobywanie od CHIS informacji dotyczących jego rodziców i najbliższej rodziny.

Możliwość wykorzystania informacji zdobytych przez CHIS w postępowaniu karnym

RIPA dopuszcza wykorzystywanie informacji zdobytych przez CHIS w postępowaniu karnym, wprowadzając przy tym jednak wiele ograniczeń. Będą one dotyczyły np. informacji uzyskanych od nieletnich CHIS czy poufnych materiałów

dziennikarskich. Szeroki opis „wrażliwych" informacji wyłączonych z wykorzystania w procesie karnym zawiera rozdział 4 *Zasad postępowania* dotyczący niejawnej inwigilacji i naruszeń własności (*Codes of Practice – Covert Surveilance and Property Interference*).

Działanie pod przykryciem

Wracając zaś do funkcjonariuszy działających pod przykryciem, należy zaznaczyć, że zarówno sam ich udział w grupie przestępczej, jak i możliwość dokonywania przez nich określonych działań są legalizowane poprzez kombinacje autoryzacji ich wykorzystania (*use*) i działania (*conduct*) w określonych kierunkach.

Kontratyp cywilny

RIPA wyłącza odpowiedzialność cywilną CHIS za szkody będące przypadkową konsekwencją ich działania na podstawie wydanej autoryzacji lub innego działania zgodnego z prawem.

Luki w systemie

Prawo brytyjskie reguluje kwestie dotyczące pracy operacyjnej znacznie obszerniej i bardziej wyczerpująco niż legislacja polska. Pomimo to, co jakiś czas są podnoszone postulaty na temat dopracowywania systemu. Jako ciekawostkę można przytoczyć sprawę Marka Kennedy'ego, funkcjonariusza Metropolitan Police, działającego przez wiele lat pod przykryciem w środowisku ekologów – ekstremistów, których działania nierzadko miały charakter przestępczy. Kennedy wszedł w to środowisko i głęboko je rozpracowywał, często utrzymując zażyłe kontakty z wieloma działaczami. Mając żonę i dwoje dzieci, żył na przykład w bliskim związku z jedną z aktywistek tego środowiska (według niektórych miał zresztą wiele romansów). Wreszcie wraz z kilkudziesięcioma innymi osobami został podczas jednej z akcji aresztowany i zdekonspirowany (pozostali uczestnicy zdarzenia chcieli wspólnie skorzystać z usług jednego adwokata, a tylko Kennedy domagał się innego prawnika. To wzbudziło podejrzenia grupy). Po różnych perypetiach odmówił jednak składania zeznań na niekorzyść ekologów. Sprawa odbiła się szerokim echem nie tylko w Wielkiej Brytanii. Również w Polsce ukazało się kilka artykułów prasowych na ten temat. Ich mottem przewodnim było pytanie o aspekt moralny i legalność takiego postępowania. Działanie Kennedy'ego było przedmiotem raportu Głównego Komisarza ds. Inwigilacji, który badał, czy i jakich autoryzacji mu udzielono i czy jego działanie mieściło się w ich zakresie.

Sprawa okazała się jednak bardziej kłopotliwa. Kennedy pozwał Metropolitan Police o to, że ta, będąc obowiązana do opieki nad CHIS, nie zapobiegła jego zaangażowaniu się w głęboki związek uczuciowy z jedną z aktywistek – przełożeni akceptowali fakt utrzymywania przez niego intymnych relacji. Po ujawnieniu szczegółów jego działalności rozpadło się jego małżeństwo, a on sam utracił cześć i dobre imię. Na fali doniesień prasowych do Metropolitan Police wpłynęły kolejne pozwy, tym razem od kobiet, które twierdziły, że oficerowie działający pod przykryciem utrzymywali z nimi długie i w efekcie wyniszczające je psychicznie intymne stosunki. Jedna ze spraw okazała się szczególnie bulwersująca, ponieważ w wyniku takich relacji jedna z aktywistek zaszła w ciążę, po czym ojciec dziecka zniknął z jej życia. Na podstawie znanych jej danych

osobowych tego mężczyzny dotarła do jego, jak sądziła, rodziny. Wówczas okazało się, że Metropolitan Police, budując legendę dla swoich funkcjonariuszy, wykorzystała dane zmarłych dzieci. W wyniku tych incydentów obecnie są podnoszone postulaty dotyczące zmiany prawa regulującego działanie funkcjonariuszy pod przykryciem, w celu uniknięcia podobnych sytuacji. Dnia 1 marca 2013 r. w „The Guardian" ukazał się artykuł autorstwa Roba Evansa i Paula Lewisa pod tytułem: *Konieczne nowe prawo dla policji pod przykryciem – Metropolitan Police* (*New law needed for undercover police – MPs*).

Pozwy wniesione w sprawach podobnych do wyżej opisanych są badane przez Trybunał ds. Operacyjnych.

Różnice między legislacją polską a brytyjską

Różnice między legislacją polską a brytyjską w zakresie stosowania poszczególnych metod operacyjnych (oprócz różnic przedstawionych powyżej) przedstawiają się następująco:

1. Zasadą RIPA jest autoryzowanie działań przez organ administracji. Ustawa brytyjska nie przewiduje (poza wydawaniem nakazu ujawnienia informacji) wydawania zezwolenia przez niezawisły sąd bądź prokuratora. Na pierwszy rzut oka może się zdawać, że model polski zabezpiecza prawa jednostki w sposób pełniejszy. RIPA wymaga jednak autoryzacji dla zdecydowanie większej liczby działań, nadzór prowadzony w trybie administracyjnym zaś pozwala na bieżąco modyfikować bądź cofać autoryzacje w razie ustania takiej potrzeby. A należy pamiętać, że każde działanie operacyjne jest związane z naruszaniem praw jednostkowych. Ingerencja w te sfery powinna ograniczać się do niezbędnego minimum. Niezawisły sąd czy prokurator mają mniejsze możliwości prowadzenia bieżącego nadzoru nad faktycznym wykorzystaniem danego instrumentu.
2. Obserwowanie i rejestrowanie obrazu i dźwięku zdarzeń w miejscach publicznych jest w polskim i brytyjskim porządkach prawnych uregulowane ustawowo. Przepisy brytyjskie jednak oprócz zdefiniowania podmiotu uprawnionego do podejmowania decyzji w tym zakresie szczegółowo określają w *Code of Practice*, jakie miejsca należy uznać za publiczne. Będą to np. klatki schodowe. W przypadku jednak, gdy w takim miejscu zamieszka bez tytułu prawnego jakakolwiek osoba (np. bezdomny), to miejsce takie staje się pomieszczeniem prywatnym i umieszczenie tam aparatury rejestrującej obraz i dźwięk wymaga już uzyskania stosownego zezwolenia.
3. RIPA reguluje kwestie związane z wykorzystaniem dodatkowych informacji uzyskanych w trakcie prowadzenia czynności operacyjnych w postępowaniach sądowych i innych.
4. Istotną różnicą między legislacją polską a brytyjską jest możliwość naruszania własności (bądź ograniczonych praw rzeczowych – najem, posiadanie, użytkowanie rzeczy) nieruchomości i ruchomości w trakcie prowadzenia czynności operacyjno-rozpoznawczych. Ustawa o ABW oraz AW nie przewiduje takiej możliwości. Tym samym brak jest ustawowego kontratypu dla przestępstwa określonego w art. 193 kk („Kto wdziera się do cudzego mieszkania, lokalu, pomieszczenia albo ogrodzonego terenu albo wbrew żądaniu uprawnionej osoby miejsca takiego nie opuszcza podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku") oraz dla przepisów karnych chroniących mienie. Brak takiej regulacji często uniemożliwia wykonanie postanowienia sądowego dotyczącego zgody na

zastosowanie kontroli operacyjnej, co jest przecież ważnym instrumentem walki z przestępczością. Trzeba tu podkreślić, że *Codes of Practice* reguluje tę materię bardzo szczegółowo. Przykładowo, zdjęcie odcisków palców z telefonu publicznego nie wymaga autoryzacji. Pozyskanie telefonu prywatnego w tym celu zaś wymaga już jednak stosownej zgody. Naruszenie nieruchomości wymaga *warrantu*, ale w razie ryzyka zdekonspirowania obserwacji jest możliwe chwilowe naruszenie nieruchomości sąsiedzkiej bez autoryzacji.

5. RIPA definiuje jako niejawne osobowe źródła informacji zarówno funkcjonariuszy działających pod przykryciem, jak i osoby niebędące funkcjonariuszami. Działanie obu tych kategorii źródeł wymaga autoryzacji. RIPA narzuca ograniczenia w zakresie korzystania z CHIS będących osobami niepełnoletnimi lub ułomnymi. Przewiduje też wprost możliwość wykorzystania w procesie karnym informacji i materiałów uzyskanych przez CHIS z określonymi wyjątkami. Ustawa o ABW oraz AW nie określa procedury autoryzacji wykorzystania osobowych źródeł informacji, tak w zakresie samej współpracy, jak i w zakresie poszczególnych działań.
6. Artykuł 37 ustawy o ABW oraz AW jest jedynym ograniczeniem dotyczącym podmiotów współpracujących ze służbami. Zawiera on szeroki katalog osób, z którymi podejmowanie współpracy jest zabronione z uwagi na ochronę państwa przed wpływem służb. Ustawa brytyjska nie zawiera takich ograniczeń, kładzie natomiast nacisk na ochronę jednostki.

Wnioski końcowe

1. Przepisy art. 32 oraz art. 35 ust. 6 *Ustawy* winny zostać usunięte. Ustęp 2 w art. 35 powinien otrzymać brzmienie: „Przy wykonywaniu czynności operacyjno-rozpoznawczych funkcjonariusze Agencji mogą **sporządzać** dokumenty, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza oraz środków, którymi posługuje się przy wykonywaniu zadań służbowych, i posługiwać się nimi".
2. *Ustawa* powinna regulować działania pod przykryciem poprzez szersze zdefiniowanie osobowego źródła informacji bądź poprzez dopuszczenie expressis verbis prowadzenia pozorowanej działalności przestępczej w celu realizacji zadań ustawowych służb. Przy tej okazji należałoby wprowadzić instytucję kontratypu cywilnego.
3. *Ustawa* powinna szczegółowo określać sposób postępowania z wszelkimi materiałami uzyskanymi w trakcie działań operacyjno-rozpoznawczych (a nie tylko zgromadzonymi podczas kontroli operacyjnej) tak w procesie karnym dotyczącym danego zagadnienia, jak i w innych działaniach procesowych i operacyjnych.
4. Zasadne wydaje się wskazanie w *Ustawie* podmiotów wydających zgodę na podjęcie określonych działań (np. że na działanie pod przykryciem zgodę wydaje szef służby, na prowadzenie obserwacji – szef bądź upoważniony przez niego kierownik jednostki organizacyjnej itd.).
5. *Ustawa* powinna przewidywać możliwość naruszania własności (bądź ograniczonego prawa rzeczowego) w celu realizacji kontroli operacyjnej oraz w innych celach (np. pobranie odcisków palców). Przepis taki winien być skonstruowany podobnie do regulacji dotyczącej kontroli operacyjnej. W sytuacji zagrożenia poważnymi przestępstwami zgodę na naruszenie własności powinien wydawać sąd (lub inny organ, np. minister spraw wewnętrznych lub minister koordynator).
6. Kodeks karny dzieli przestępstwa na występki i zbrodnie. Można więc przyjąć, że naruszenie, o którym mowa wyżej, jest możliwe tylko w przypadku zbrodni.

Powinien to być jednak instrument ostateczny – zgoda byłaby udzielana tylko w sytuacji, gdyby określonego celu nie można było osiągnąć inaczej. Pewną odrębność musiałby jednak zachować wywiad. Naruszenie własności poza granicami kraju powinno być autoryzowane przez szefa służby.

7. Duże znaczenie miałoby opracowanie dokumentów na wzór *Codes of Practice*, które szczegółowo przedstawiałyby praktyczne rozumienie pojęć i procedur ustawowych, a przy tym miałyby charakter aktu prawnego. Regulacje dotyczące uprawnień operacyjnych powinny być zrozumiałe przede wszystkim dla funkcjonariuszy wykonujących przepisy, ale także dla reszty obywateli.

Przedstawiona problematyka ma znaczenie fundamentalne. Prawidłowe określenie sfery działań funkcjonariuszy to z jednej strony gwarancja ich bezpieczeństwa określona przepisami karnymi, z drugiej zaś gwarancja ochrony praw jednostki. Służby realizujące zadania z zakresu bezpieczeństwa powinny być wyposażone w instrumentarium odpowiednie do znaczenia takich zadań. Jako przykład szerokich uprawnień przy jednoczesnym zapewnieniu transparentnej i głębokiej (choć w pewnych aspektach niepełnej) kontroli nad służbami może posłużyć model brytyjski.

Sprawa ma dodatkowe znaczenie w świetle toczących się aktualnie dyskusji nad wprowadzeniem regulacji dyskwalifikującej możliwość wykorzystania w procesie karnym dowodów pozyskanych w wyniku czynu zabronionego (tzw. owoce trującego drzewa – *fruits of poisoneous tree*). W judykaturze amerykańskiej przykładem takich praktyk jest nieuprawnione przeszukanie pomieszczeń, w którego trakcie uzyskano dowód popełnienia przestępstwa. Dowód taki, podobnie jak i dowody pochodne – „trujące drzewo" i jego „owoce" – nie będą brane pod uwagę w postępowaniu sądowym. Prace nad nowelizacją są w toku i trudno wyrokować, jak materia ta zostanie ostatecznie uregulowana. Niemniej jednak przy niniejszych rozważaniach kwestii tej nie można tracić z pola widzenia.

Abstrakt

Artykuł ma postać felietonu prawniczego. Jako cel stawia sobie zrozumiałe zaprezentowanie uprawnień ABW i MI5 jako kontratypu, czyli okoliczności wyłączających odpowiedzialność karną za działania noszące formalne znamiona przestępstwa. Większość metod pracy operacyjnej, których istotę można ująć jako podstępne doprowadzanie do wszczęcia postępowania karnego, oraz metod pracy śledczej, takich jak zatrzymanie, stosowanie środków przymusu bezpośredniego itd., to działania wypełniające formalne znamiona przestępstwa. Rodzi się wobec tego pytanie, jakie przepisy bądź konstrukcje prawne przywracają legalność takich działań funkcjonariuszy. Analiza tego typu konstrukcji zawartych w ustawie o ABW oraz AW stanowi pierwszą część artykułu.

W części drugiej artykuł przedstawia uregulowania dotyczące czynności operacyjno-rozpoznawczych w legislacji brytyjskiej, koncentrując się przy tym na przepisach zawartych w *Regulation of Investigatory Powers Act 2000*, ustawy będącej podstawą pracy operacyjnej wielu brytyjskich służb, między innymi MI5. Model brytyjski opiera się na autoryzacji określonych działań przez określone podmioty. Tak więc uzyskanie stosownego zezwolenia będzie okolicznością przywracającą legalność działaniu noszącemu formalne znamiona przestępstwa.

W artykule zanalizowano również zakres uprawnień służb brytyjskich i sposób ich nadzorowania. Wskazano, że istotną rolę w zakresie nadzoru pełnią tu Komisarze:

do spraw Służb, Inwigilacji oraz Naruszeń Komunikacyjnych. W systemie brytyjskim funkcjonuje wreszcie wyspecjalizowany organ sądowy, którego zadaniem jest rozpatrywanie skarg osób uważających, że ich prawa jednostkowe zostały poprzez działania służb naruszone. Uprawnienia służb brytyjskich są zdecydowanie szersze niż uprawnienia służb polskich, ale jednocześnie są zrównoważone ich pełnym i transparentnym nadzorowaniem.

Na koniec porównano legislację polską i brytyjską oraz postawiono wnioski *de lege ferenda*.

Abstract

The aim of the article is to analyze the powers of special services from the point of view of the penal law. The article presents a view that most operational work methods that might be referred to as deceitful attempts to launch criminal proceedings, as well as most investigative methods, such as arrest, use of coercive measures, etc., are activities that fit the definition of a crime. This raises a question about the provisions of law or legal measures that would reestablish the legitimacy of such activities performed by officers. The first section of the article offers an analysis of such provisions contained in the Act on ABW and AW.

The second section of the article provides an overview of regulations on surveillance and investigation operations in the British law based on the provisions of the Regulation of Investigatory Powers Act 2000. The Act is the basis for operation of many British services, including MI5. The analysis of the regulations shows that the British model is based on the authorization of specific operational activities carried out by specific bodies. Authorization of specific activities makes those actions that formally fit the definition of a crime legitimate.

The author also examines the scope of powers granted to British services and how they are controlled. The analysis indicates that Commissioner play an important role in the supervision. There are commissioners responsible for the affairs of the service, surveillance, and communications violations. The British system includes a judicial court unit that is responsible for examining complaints of persons who believe that activities taken by services infringed upon their rights. The powers of British services are much more extensive than the powers of Polish services. However, they are subject to comprehensive and transparent control system.

The last section of the article contains a comparison of the Polish and English legislation and conclusions *de lege ferenda*.

Piotr Wojtunik

Pojęcie, źródła i przedmiot prawa stosunków służbowych

I. Pojęcie prawa stosunków służbowych

1. Uwagi ogólne

Przeciętne roczne zatrudnienie w administracji publicznej obejmuje ponad 400 tysięcy osób[1]. Liczba ta dotyczy zawierania różnego rodzaju stosunków służbowych. Są to stosunki prawne oparte zarówno na przepisach prawa pracy, jak i prawa administracyjnego. W literaturze przedmiotu przeważa pogląd, że prawo stosunków służbowych to: (...) *akty prawne regulujące zatrudnienie w sektorze publicznym, znamienne ustaleniem zaostrzonych kryteriów zatrudnieniowej zdolności prawnej* (...)*, szczególnym systemem rekrutacji kandydatów* (…), *statusem prawnym zatrudnionych* (…) *Termin „zatrudnienie" dotyczy zarówno szczególnych stosunków pracy regulowanych przepisami zawartymi w pracowniczych pragmatykach służbowych, np. w urzędach państwowych (służbie cywilnej), w szkolnictwie, szkolnictwie wyższym, Najwyższej Izbie Kontroli, Państwowej Inspekcji Pracy, sądownictwie, prokuraturze, instytutach badawczych i in., jak i niepracowniczych stosunków zatrudnienia typu administracyjnoprawnego, regulowanych przepisami zawartymi w niepracowniczych pragmatykach odnoszących się do służb mundurowych (zmilitaryzowanych)*[2]. Prawo stosunków służbowych jest utożsamiane z pojęciem pragmatyki służbowej (zawodowej, urzędniczej). „Pragmatyka" to termin języka prawniczego wypracowany przez doktrynę oraz przez osoby stosujące i interpretujące przepisy prawne. Rozumiana jest jako zbiór aktów prawnych regulujących całokształt poszczególnych kategorii stosunków służbowych w administracji publicznej.

2. Pojęcie „stosunku służbowego"

Pomimo tego, że „stosunek służbowy" i „służba" to terminy prawne, to w polskim systemie prawnym brak ich definicji legalnej. Językoznawcy wywodzą oba te pojęcia ze słowa „służyć", rozumianego jako poświęcanie pracy jakiejś idei, dobru, sprawie. Współczesna polszczyzna łączy z tymi pojęciami działalność w instytucjach publicznych. „Służba" oznacza pracę *w urzędzie państwowym, instytucji użyteczności publicznej, wojsku itp.*[3], a „służbowy" to *dotyczący pracy w urzędzie, instytucji, wojsku*[4]. Rozważania te są istotne dla ustalenia zakresu odniesienia stosunku służbowego

[1] Zob. dane statystyczne za lata 2009–2011, www.stat.gov.pl.

[2] T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy*, w: *System prawa administracyjnego. Tom 11*, R. Hauser, Z. Niewiadomski, A. Wróbel (red.), Warszawa 2011, C.H. Beck, s. 104–105.

[3] *Słownik języka polskiego*, E. Sobol (oprac.), Warszawa 2005, PWN, s. 933.

[4] Tamże.

jako stosunku prawnego, czyli więzi (relacji) prawnej pomiędzy instytucją państwową a osobą w niej zatrudnioną i realizującą zadania publiczne.

W aktach prawnych pojawiają się różne pojęcia nawiązujące do terminu „służba". Obok „służby publicznej", „służby państwowej" czy „służby cywilnej" znajdziemy takie kategorie, jak: „służba medycyny pracy", „służba bezpieczeństwa i higieny pracy", „służba porządku publicznego" i inne. Powszechnie mówi się także o „służbach państwa". Każde z tych określeń jest przedmiotem zainteresowania doktryny i jest charakteryzowane przez trzy gałęzie prawa – prawo konstytucyjne, administracyjne i prawo pracy. Na uwagę zasługuje również stanowisko Trybunału Konstytucyjnego, który w wyroku z dnia 7 maja 2002 r. wskazał, że „służbą publiczną" jest kadra wykonująca zadania aparatu państwowego na warunkach ustalonych jednostronnie przez państwo w ramach posiadającego cechę trwałości stosunku publicznoprawnego, charakteryzującego się daleko idącym podporządkowaniem służbowym urzędnika i wzmocnioną odpowiedzialnością zawodową[5]. Warto w tym miejscu zauważyć, że wśród różnych teoretycznych koncepcji określenia pojęcia i granic „służby publicznej" („państwowej") w nauce o administracji wyróżniono termin „prawo urzędnicze", obejmujące swym zakresem przedmiotowym charakterystykę pojęcia „stosunek służbowy". Większość przedstawicieli nauki zajmujących się tą tematyką wskazuje, że „stosunek służbowy" obejmuje osoby zatrudnione na stanowiskach urzędniczych w:

- administracji rządowej (członkowie korpusu służby cywilnej i służby zagranicznej),
- innych urzędach państwowych (poza korpusem służby cywilnej, np.: pracownicy ABW),
- administracji samorządowej[6].

Niektórzy autorzy[7] rozszerzają powyższy krąg podmiotów charakteryzowanego stosunku prawnego o:

- osoby pełniące funkcje organów władzy państwowej,
- funkcjonariuszy służb zmilitaryzowanych,
- prokuratorów,
- sędziów,
- nauczycieli,
- pracowników socjalnych innych państwowych jednostek organizacyjnych.

W literaturze przedmiotu pojęcie „stosunek służbowy" jest definiowane różnie, jego charakterystyka zależy w głównej mierze od przyjętych przez autora założeń teoretycznych. Analiza pragmatyk zawodowych wskazuje na funkcjonowanie w administracji publicznej kilku typów więzi prawnych. Znalezienie dla nich wspólnego mianownika sprowadza się do *ogólnego stwierdzenia, że stosunek służbowy to kategoria stosunku prawnego zachodzącego między określonymi podmiotami, którego treść jest regulowana przepisami prawa publicznego (administracyjnego, konstytucyjnego), ale również przepisami prawa pracy. Jego treścią są prawa i obowiązki stron, a przedmiotem zachowanie wymagane od osoby zobowiązanej, odniesione do treści służby*[8]. Ujęcie to z oczywistych względów należy doprecyzować poprzez odniesienie

[5] SK 20/00, OTK-A 2002, nr 3, poz. 29.

[6] Zob. T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy...,* s. 7*;* E. Ura, *Prawo urzędnicze*, Warszawa 2007, s. 19 i in.; P. Winczorek, *Komentarz do Konstytucji Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 roku*, Warszawa 2008, Liber, s. 144–145.

[7] T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy…*, s. 7.

[8] Tamże.

uprawnień i obowiązków osób w ramach stosunku służbowego do interesu państwa lub utożsamianego z nim interesu służby. To pozwala wskazać, że w ramach interesujących nas stosunków prawnych osoba zatrudniona występuje w roli podmiotu wykonującego funkcję publiczną, a w konsekwencji realizującego zadania państwa i służby.

3. Charakterystyka stosunku służbowego

Najpowszechniejszym podziałem stosunków służbowych w obecnym stanie prawnym jest ich rozróżnienie na „stosunki służbowe służb mundurowych" (zmilitaryzowanych) oraz na „pracownicze stosunki służbowe". Te ostatnie, z uwagi na sposób ich powstania, można podzielić na „stosunki służbowe nominacyjne" (pozaumowne) i „stosunki służbowe kontraktowe" (umowne). Podstawa prawna dotycząca przyjęcia do „służby" lub „pracy" bezpośrednio wpływa na występowanie w konkretnym rodzaju zatrudnienia cech zarówno administracyjnoprawnych, jak i cywilnoprawnych. W ustawach pragmatycznych prawodawca, konstytuując dany typ stosunku służbowego, decyduje o jego charakterze poprzez zaakcentowanie tylko pewnych jego cech (publicznoprawnych bądź prywatnoprawnych). W konsekwencji, kryterium różnicującym stosunki służbowe jest intensywność nasycenia ich elementami zapożyczonymi z prawa administracyjnego i cywilnego (prawa pracy). Dlatego przy rozważaniu interesującego nas zagadnienia jest istotne, aby wskazać, jakie cechy przeważają w konstrukcji poszczególnych stosunków służbowych. Warto w tym miejscu podkreślić, że dany akt prawny odnoszący się do konkretnego typu służby czy pracy zawiera dodatkowe unormowania odrębnych form zatrudnienia. I tak, w zakresie dotyczącym służb zmilitaryzowanych i specjalnych można znaleźć (poza systemowym ujęciem służby żołnierzy zawodowych i funkcjonariuszy) przepisy prawne dotyczące zatrudniania pracowników cywilnych i kierowników służb. Analizując pragmatyki, można wskazać cechy wspólne dla stosunku służbowego administracyjnego i pracowniczego. W obu przypadkach występuje szczególne podporządkowanie zwane podległością służbową, charakteryzujące się m.in. dyspozycyjnością i obowiązkiem wykonywania poleceń służbowych. Ponadto część stosunków służbowych prawa pracy powstaje w wyniku aktu mianowania, co jest charakterystyczne dla służby typu administracyjnego. Akt mianowania jest określony w ustawach pragmatycznych służb mundurowych oraz wymieniany jako sposób pozaumownego nawiązania stosunku zatrudnienia w prawie pracy[9]. Nominacja wpływa na większą trwałość zatrudnienia, gdyż tak powstały stosunek prawny może zostać zmieniony lub rozwiązany tylko w sytuacjach enumeratywnie wskazanych w ustawie. Akt mianowania powoduje również, że *urzędnicy służby cywilnej, jak i funkcjonariusze służb mundurowych czy żołnierze zawodowi uzyskują w wyniku nominacji określone uprawnienia do wykonywania działań w imieniu i na rzecz państwa*[10].

W nauce prawa administracyjnego, jak już wspomniano wyżej, mianowanie jest traktowane jako akt administracyjny, jednostronnie rozstrzygający w indywidualnej sprawie, powodujący powierzenie stanowiska i nawiązanie stosunku służby. Warto w tym miejscu przypomnieć, że w Polsce w okresie międzywojennym dominowała moni-

[9] Art. 76 *Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy* (tekst jednolity – Dz.U. z 1998 r. Nr 21, poz. 94 ze zm.)

[10] P. Szustakiewicz, *Stosunki służbowe funkcjonariuszy służb mundurowych i żołnierzy zawodowych jako sprawa administracyjna*, Warszawa 2012, Difin, s. 21.

styczna – publicznoprawna – koncepcja urzędniczego stosunku pracy[11]. Współcześnie przepisy prawne oraz ich wykładnia skłaniają do przyjęcia pluralistycznego charakteru mianowania jako źródła powstania pracowniczych stosunków służbowych. W konsekwencji pozaumowne podstawy zatrudnienia – mianowanie i powołanie[12] – rodzą stosunki prawne mieszane, tj. wywołujące skutki w sferze prawa administracyjnego (co jest związane ze specyfiką pracy w administracji) i prawa pracy.

3.1. Stosunki służbowe służb zmilitaryzowanych

W polskich służbach zmilitaryzowanych: Policji, Straży Granicznej, Państwowej Straży Pożarnej, Biurze Ochrony Rządu, Służbie Więziennej, Służbie Celnej, Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu, Służbie Kontrwywiadu Wojskowego, Służbie Wywiadu Wojskowego i Centralnym Biurze Antykorupcyjnym dominują administracyjne stosunki służbowe. Oprócz funkcjonariuszy obejmują one również żołnierzy zawodowych pełniących służbę w polskich siłach zbrojnych oraz w wyżej wymienionych wojskowych służbach specjalnych. Administracyjne stosunki służbowe w swojej konstrukcji prawnej wyróżniają się trzema elementami: obowiązkiem poświęcenia, podporządkowania (w tymwyjątkową dyspozycyjnością) oraz przyznaniem szczególnych uprawnień.

Na temat specyfiki służby w formacjach zmilitaryzowanych wypowiedział się Trybunał Konstytucyjny w wyroku z 23 września 1997 r. (sygn. akt K 25/96). Skład orzekający podkreślił, że charakteryzuje się ona obowiązkiem wykonywania zadań w nielimitowanym czasie pracy i trudnych warunkach, wymagających narażania życia i zdrowia. Osoby decydujące się służyć jako funkcjonariusze wymienionych służb lub żołnierze zawodowi składają rotę ślubowania, w której zobowiązują się do poświęcenia zdrowia, a nawet życia w imię ochrony wartości nadrzędnych. Aksjologiczne odwołania w ustawach pragmatycznych dotyczą szeroko rozumianego bezpieczeństwa państwa. Szczególnie istotnym aspektem składania przyrzeczenia, o którym mowa, jest to, że nie można się uchylić od skutków złożonej przysięgi. Takiego elementu stosunku służbowego nie ma w przypadku pracowniczych stosunków służbowych w zakresie dotyczących służby celnej, cywilnej, dyplomatycznej itp.

Element ofiarności w publicznoprawnych stosunkach służbowych łączy się z dyspozycyjnością jako warunkiem sprawnego wykonywania zadań doniosłych dla państwa i jego obywateli. Wyjątkowość tej cechy w porównaniu z podległością służbową pozostałych stosunków zatrudnieniowych wyraża się w pełnym podporządkowaniu poleceniom służbowym oraz uprawnieniu organów administracyjnych do jednostronnego kształtowania warunków służby w zależności od potrzeb danej formacji mundurowej. *Cechą charakterystyczną formacji umundurowanych jest obowiązek wykonywania rozkazów lub poleceń. Przepisy, które zezwalają funkcjonariuszom na niewykonanie rozkazu są absolutnym wyjątkiem i nie mogą być nadużywane. Charakter służb zmilitaryzowanych nie pozwala na dyskusję lub głosowanie nad rozkazami. Takie postępowanie byłoby zaprzeczeniem mechanizmu funkcjonowania tych formacji*[13]. Kolejnymi wyróżnikami

[11] Zob. *Ustawa z dnia 17 lutego 1922 r. o państwowej służbie cywilnej* (tekst jedn. Dz. U. z 1949 r. Nr 11, poz. 72 ze zm.)

[12] Pozaumownym sposobem nawiązania stosunku pracy jest również wybór. Z uwagi na odrębny charakter tak powstałych stosunków prawnych nie będą one omawiane w ramach niniejszego opracowania.

[13] P. Szustakiewicz, *Stosunki służbowe funkcjonariuszy służb mundurowych*…, s. 28.

dyspozycyjności w administracyjnych stosunkach służbowych są: możliwość przeniesienia żołnierza zawodowego i funkcjonariusza na inne stanowisko służbowe, nawet w innej miejscowości, elastyczne określanie czasu służby oraz ograniczenie w zakresie ustalania terminu zakończenia stosunku służbowego na wniosek nominata. Tak ukształtowana treść stosunku służbowego, wpływa również na wysokie wymagania wobec osób kandydujących do formacji zmilitaryzowanych oraz uzasadnia przyznanie funkcjonariuszom i żołnierzom zawodowym szeregu przywilejów wzmacniających ich stabilność zawodową.

3.2. Pracownicy zatrudnieni w służbach zmilitaryzowanych

Odrębną kwestią, o której należy wspomnieć, jest sprawa wyznaczania obowiązków na stanowiskach szefów (kierowników) omawianych służb. W sytuacji niejednolitych regulacji prawnych dotyczących tego typu stosunków służbowych należy wskazać dwie koncepcje odnoszące się do tej sytuacji. Pierwsza z nich obejmuje desygnowanie szefa formacji spośród funkcjonariuszy danej służby. Powołanie takiej osoby skutkuje wyłącznie powierzeniem funkcji organizacyjnej, bez nawiązywania nowego stosunku prawnego. Druga dotyczy objęcia funkcji kierownika urzędu centralnego i nawiązania w ten sposób stosunku pracy z powołania przez osobę nieposiadającą statusu funkcjonariusza. Osoba taka otrzymuje status innych pracowników urzędów państwowych i staje się pracownikiem kierowanego przez siebie urzędu. *Pozostawanie w takim stosunku wynika z natury aktu powołania, prowadzącego do nawiązania między tą osobą a organem powołującym stosunku podległości służbowej o charakterze organizacyjnym*[14]. Odwołanie kierownika urzędu centralnego wywołuje skutki w postaci pozbawienia stanowiska kierowniczego oraz rozwiązania stosunku pracy.

Poszczególne ustawy pragmatyczne zawierają bardziej (jak w przypadku Służby Więziennej) lub mniej precyzyjne unormowania dotyczące zatrudniania osób we wskazanych formacjach na podstawie umowy o pracę. Dla potrzeb niniejszego opracowania wystarczy wskazać, że tego typu pracowniczy stosunek służbowy obejmuje zatrudnienie na różnych stanowiskach o charakterze administracyjnym, technicznym i gospodarczym. Kategoria obejmująca trzy wyżej wymienione rodzaje stanowisk pracowniczych jest wewnętrznie zróżnicowana ze względu na charakter wykonywanej pracy oraz ze względu na odmienne konstrukcje prawne zawarte w pragmatykach i ustawach regulujących status członków korpusu służby cywilnej i pracowników urzędów państwowych, jak również w przepisach prawa pracy.

3.3. Pracownicze stosunki służbowe

Punktem wyjścia do scharakteryzowania zatrudnienia pracowników merytorycznych administracji publicznej są zastosowane przez prawodawcę, wspomniane już wyżej, podstawy nawiązywania stosunku pracy – nominacyjne i kontraktowe. Ta grupa stosunków służbowych jest również niejednolita. Obejmuje ona zarówno osoby mające status pracowników mianowanych, pracowników powołanych, pracowników umownych wykonujących zadania służby oraz pozostałych pracowników umownych. W większości pragmatyk dotyczących tej kategorii stosunków służbowych zastosowano instytucje prawne i rozwiązania typu administracyjnego. Chodzi tu przede wszystkim

[14] T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy...*, s. 15–16.

o jednostronne ustawowe ustalenie indywidualnych warunków zatrudnienia, co przekłada się na wyłączenie możliwości kształtowania praw i obowiązków pracowniczych w drodze zawierania zbiorowych układów pracy i innych porozumień zbiorowych.

Kolejnym elementem charakterystycznym dla interesujących nas stosunków służbowych jest stabilizacja zatrudnienia, która nabiera szczególnego znaczenia w kontekście władzy dyspozytywnej przełożonego w zakresie kształtowania treści stosunku pracowniczego[15]. Obowiązki pracowników są tu utożsamiane z powinnością wobec Państwa, a interesy osobiste są podporządkowane interesom publicznym. Przekłada się to na ustawowe ograniczenia, w ramach więzi służbowej, części uprawnień obywatelskich typu politycznego (apolityczność), pracowniczego (np. zakaz uczestniczenia w strajkach), osobistego (np. składanie oświadczeń majątkowych), ekonomicznego (np. zakaz podejmowania dodatkowej pracy zarobkowej). Ponadto w przypadku stosunków prawnych, o których mowa, jest widoczny wzmocniony rygor odpowiedzialności dyscyplinarnej, która jest jednym z wyróżników uprawnień władczych zatrudniającego wobec zatrudnionego.

3.3.1. Pracownicy mianowani

Charakter prawny nominacji (mianowanie, powołanie) wpływa na wewnętrzne zróżnicowanie omawianych tu stosunków służbowych. W tym przypadku akt mianowania nie będzie miał cech wyłącznie aktu administracyjnego, jak miało to miejsce w przypadku stosunków służbowych służb zmilitaryzowanych. *W kwestii stosunku prawnego powstałego w wyniku mianowania w nauce prawa pracy przeważa tak czy inaczej uzasadniany pogląd o jego międzygałęziowym: administracyjnym i prawnopracowniczym uwarunkowaniu. Wyrażają to ogólne sformułowania, stwierdzające, że* (…) *stosunki służbowe z nominacji należy zaliczyć do stosunków pracy zawierających wyraźne elementy administracyjnoprawne, wreszcie że w stosunkach tych występuje różny zakres element*ów *o charakterze administracyjnoprawnym, odróżniającym je od umownego stosunku pracy*[16]. Natura prawna nominacji będzie każdorazowo zależała od ujęcia aspektów podmiotowych i przedmiotowych w ustawach pragmatycznych. Wspólną cechą tych stosunków prawnych jest to, że status podmiotów składa się z norm wyznaczających publicznoprawną sferę zatrudnienia (akt powierzenia, pozbawienia, zmiany miejsca pracy, instytucja zawieszenia w obowiązkach, odpowiedzialność dyscyplinarna) oraz z norm wyznaczających sferę pracowniczą (ochrona pracy, regulacja wynagrodzenia, organizacja czasu pracy, stosowanie odpowiedzialności materialnej).

Mianowanie stosuje się wobec m.in. prokuratorów i asesorów prokuratury, sędziów wszystkich rodzajów sądów, asesorów w sądach administracyjnych, referendarzy sądowych, radców Prokuratorii Generalnej Skarbu Państwa, etatowych członków samorządowych kolegiów odwoławczych i zawodowych kuratorów sądowych. W przypadku mianowania istotne jest to, że organem mianującym jest organ usytuowany poza strukturą jednostki zatrudniającej pracownika. Pozwala to na stworzenie więzi służbowej pomiędzy nominatem a organem nadrzędnym, mającym kompetencje do wyznaczania stanowiska służbowego. W tych przypadkach akt mianowania może zawierać zarówno oświadczenie w rozumieniu art. 11 kodeksu pracy,

[15] Stabilność zatrudnienia w mniejszym stopniu dotyczy umownych stosunków służbowych, dla których pragmatyki nie przewidują katalogu przesłanek rozwiązania stosunku pracy.

[16] T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy*..., s. 24.

powodujące skutek nawiązania stosunku pracy, jak i oświadczenie będące elementem treści aktu administracyjnego, a tym samym powodujące skutki publicznoprawne. W celu podkreślenia statusu przewagi cech służby w tych stosunkach prawnych ustawodawca w pragmatykach stosuje takie zwroty, jak: „stosunek służbowy", „uposażenie", „zwolnienie ze służby". Nominacja jest wówczas formalnym jednostronnym rozstrzygnięciem o charakterze służbowym i jednocześnie podstawą piastowania stanowiska, tj. pełnienia funkcji w ramach powstałego stosunku pracy. Taka konstrukcja stosunków służbowych wiąże się z przyznaniem mianowanemu pracownikowi uprawnień do przygotowywania, wydawania i wykonywania rozstrzygnięć (decyzji), co jest istotne przy realizacji zadań publicznych z zakresu wymiaru sprawiedliwości, orzecznictwa administracyjnego itp. Charakterystyczne jest tu rozgraniczenie stosunku pracy i stanowiska, którego dopiero objęcie wiąże się z uzyskaniem władzy jurysdykcyjnej, orzeczniczej lub egzekucyjnej.

Oprócz wyżej opisanej konstrukcji stosunków służbowych istnieją rozwiązania, w których organ administracyjny zajmujący stanowisko kierownika jednostki organizacyjnej dokonuje aktu nominacyjnego w celu nawiązania stosunku pracy. Dotyczy to m.in. pracowników nadzorujących lub wykonujących czynności kontrolne Najwyższej Izby Kontroli, Państwowej Inspekcji Pracy, nauczycieli mianowanych i dyplomowanych oraz nauczycieli akademickich[17]. Akt nawiązania stosunku pracy może ponadto prowadzić do udzielenia zatrudnionemu określonego władztwa typu administracyjnego. Mianowanie ma wówczas charakter wyłącznie formalny, a zgoda pracownika jest warunkiem jego ważności i skuteczności, co skutkuje nadaniem tym stosunkom służbowym cech wzajemnej więzi zobowiązaniowej właściwej dla stosunków służbowych z zakresu prawa pracy. Podkreślenie przewagi cech charakterystycznych dla pracy w przypadku tych stosunków prawnych następuje w warstwie semantycznej, poprzez zastosowanie w pragmatykach zwrotów: „stosunek pracy", „wynagrodzenie", „rozwiązanie stosunku pracy". *Postępowanie nominacyjne jest postępowaniem w sprawie nawiązania stosunku pracy,* (…) *podmiotami powstałego stosunku prawnego są pracownik i pracodawca zdolny do nawiązania stosunku pracy przez własną czynność prawną, którego przedmiot dotyczy statusu stron tego stosunku. Ze wskazanych powodów wydany w tych okolicznościach akt mianowania powinien być rozpatrywany w kategoriach czynności prawa pracy, wywierającej skutki materialnoprawne* (…)[18].

Pewną hybrydą omawianych stosunków służbowych jest zatrudnianie urzędników służby cywilnej. Stosunki te powstają w wyniku aktu mianowania przez szefa służby cywilnej[19]. W wyniku mianowania pracownika służby cywilnej stosunek pracy przekształca się z umownego stosunku służbowego w nominacyjny, skutkujący zwiększeniem poziomu stabilności pracy oraz uzyskaniem dodatkowych uprawnień pracowniczych. Status zawodowy urzędnika służby cywilnej jest mimo to nasycony pierwiastkami charakterystycznymi dla więzi zobowiązaniowej.

---

[17] Od połowy lat 90. XX wieku orzecznictwo sądowe, analizując mianowanie na stanowisko nauczyciela czy pracownika samorządowego, traktuje to mianowanie jako czynność prawa pracy o charakterze materialnoprawnym. Zob. wyrok SN z 10.04.1997 r., I PKN 57/96, OSNAPiUS 1998, nr 4, poz. 112 i z 23.11.2004 r., I PK 35/04, OSNP 2005, nr 11, poz. 160.

[18] T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy...*, s. 37.

[19] Art. 48 ustawy z dnia 21.11.2008 r. o służbie cywilnej (Dz.U. z 2008 r. Nr 227, poz. 1505 ze zm.)

3.3.2. Pracownicy powołani

Analizując rozwiązania prawne dotyczące powołania osoby na stanowisko związane z funkcją kierowniczą, należy zwrócić uwagę, że nominacja może skutkować nawiązaniem z powołanym stosunku organizacyjnego lub stosunku pracy. Jest to sytuacja analogiczna do opisanej wyżej kwestii wyznaczania kierowników służb formacji zmilitaryzowanych. W przypadku pracowniczych stosunków służbowych istotne jest również to, czy osoba została desygnowana spośród osób zatrudnionych w danej jednostce organizacyjnej. Powierzenie stanowiska kierowniczego osobie z grona pracowników danej służby lub zawodu (np.: prezes sądu, rektor uczelni publicznej, kurator okręgowy) jest podstawą do przekształcenia dotychczasowego stosunku pracy w zakresie poszczególnych obowiązków i uprawnień związanych ze sprawowaniem funkcji kierowniczej. W takich sytuacjach akt powołania będzie powodował skutki organizacyjne, odwołanie z funkcji nie wpłynie więc na ciągłość stosunku służbowego i najczęściej będzie oznaczało powrót na stanowisko zajmowane przed datą desygnowania.

Odmiennym przypadkiem jest powierzenie stanowiska kierownika urzędu osobie nieposiadającej statusu pracownika danej jednostki. Powołanie skutkuje wówczas nawiązaniem stosunku pracy (który trwa do momentu odwołania ze stanowiska) traktowanego jako wypowiedzenie umowy o pracę lub rozwiązanie bez wypowiedzenia.

3.3.3. Umowne stosunki służbowe

Umowne źródło stosunku służbowego jest charakterystyczne dla zatrudniania większości pracowników i urzędników sfery budżetowej. Oprócz wskazanych wyżej cech publicznoprawnych pracowniczych stosunków służbowych, status pracowników służby cywilnej, pracowników samorządowych, urzędników sądów i prokuratur, pracowników Najwyższej Izby Kontroli, Państwowej Inspekcji Pracy oraz nauki i oświaty wskazuje na sądowy tryb rozpatrywania sporów wynikających ze stosunku pracy.

Pragmatyki dotyczące powyższych grup pracowniczych regulują ich status w sposób niejednorodny. Jeśli chodzi o dyspozycyjność, to znajdziemy rozwiązania zbliżone zarówno do konstrukcji dotyczących pracowników mianowanych (pracownicy Najwyższej Izby Kontroli czy Państwowej Inspekcji Pracy), jak i dla typowych stosunków pracowniczych (pracownicy służby cywilnej, urzędnicy sądów i prokuratur). W przepisach regulujących umowne stosunki służbowe nie znajdziemy mechanizmów zapewniających taką trwałość zatrudnienia, jaka występuje w przypadku pracowników mianowanych. Możemy, co prawda, wskazać pewne ustawowe instytucje mające wpływ na długość ochrony zatrudnienia bądź dające pracodawcy możliwość zwolnienia pracownika z pełnienia obowiązków w okresie wypowiedzenia, ale co do zasady w tych przypadkach będzie miał zastosowanie kodeks pracy. Odrębności w regulacji statusu poszczególnych przedstawicieli stosunków kontraktowych można odnaleźć m.in. w katalogu kar dyscyplinarnych, możliwości zawieszenia w obowiązkach czy różnego ujęcia obowiązków służbowych. W przypadku pracowników oświaty i nauki ustawodawca zezwolił na układową metodę regulacji warunków zatrudnienia.

Reasumując, należy podkreślić, że interesujące nas stosunki służbowe mają w przeważającej mierze charakter zobowiązaniowy, zbliżony do rozwiązań przyjętych w prawie pracy. W ramach szczegółowych rozwiązań instytucjonalnych znajdujemy natomiast elementy służbowe, podkreślające związek z władztwem administracyjnym.

Do grupy stosunków służbowych mających charakter zobowiązaniowy zostanie zaliczone również zatrudnienie pracowników na stanowiskach administracyjnych, pomocniczych i obsługi, o których była mowa przy okazji omawiania stosunków służbowych w formacjach zmilitaryzowanych. Ta szeroka, niejednolita grupa pracowników podlega przepisom prawa pracy w zakresie nieuregulowanym przez ustawy pragmatyczne oraz przez ustawę o pracownikach urzędów państwowych[20]. Rozwiązania formalne zastosowane dla tego typu zatrudnienia nie zawierają istotnych kwestii dotyczących elementu „służbowego", wobec czego w niniejszym opracowaniu nie zostaną poddane głębszej analizie.

II. Źródła prawa stosunków służbowych

1. Źródła prawa powszechnie obowiązujące

Źródła prawa (źródła pochodzenia, powstawania prawa) to oznaczone rodzaje aktów prawnych zawierające w swej treści przepisy prawne ustanowione przez kompetentne w tym zakresie organy państwa i ogłoszone w określonym trybie. *W znaczeniu formalnym należy rozumieć przez nie formę powstawania i egzystowania prawa, jego przejawiania się i istnienia. W znaczeniu materialnym są to czynniki rodzące prawo jako zjawisko społeczne*[21] Konstytucja RP w rozdziale III oraz w art. 234 ust. 2[22] wskazuje, że ustawodawca wyróżnia trzy rodzaje źródeł prawa: akty powszechnie obowiązujące, akty prawa wewnętrznego niebędące źródłami prawa powszechnie obowiązującego oraz akty prawa miejscowego[23]. Ustawa zasadnicza w art. 87 zalicza do źródeł powszechnie obowiązujących: Konstytucję, ustawy, ratyfikowane umowy międzynarodowe, rozporządzenia oraz akty prawa miejscowego[24].

W odniesieniu do prawa stosunków służbowych najistotniejszą rolę regulacyjną odgrywają ustawy i rozporządzenia. Przyjęty w nich sposób normowania treści stosunku służbowego uwzględnia kierunek wyznaczony przez nadrzędne normy konstytucyjne o charakterze ustrojowym. Uregulowania międzynarodowe w interesującej nas sferze dotyczą przede wszystkim praw obywatelskich związanych z dostępem do służby publicznej oraz pracowniczych praw człowieka.

1.1. Konstytucja

Ustawa zasadnicza zawiera szereg norm odnoszących się do szeroko rozumianych stosunków służbowych. Najważniejsze z nich obejmują zasady konstytucyjnej ochrony pracy oraz określają system organów państwa i realizowane przez nie zadania publiczne. W zakresie ważnym dla niniejszego artykułu istotne znaczenie mają unormowania konstytucyjne dotyczące państwowego nadzoru nad warunkami wykonywania pracy. Jeśli chodzi o zatrudnienie, to najważniejsze są regulacje przewidujące wolność

[20] Ustawa z dnia 16.09.1982 r. o pracownikach urzędów państwowych (tekst jednolity – Dz.U. z 2001 r. Nr 86, poz. 953 ze zm.).

[21] *Polskie prawo konstytucyjne*, D. Górecki (red.), Warszawa 2008, Wolters Kluwer, s. 29.

[22] Ustawa z dnia 2.04.1997 r. Konstytucja Rzeczypospolitej Polskiej (Dz.U. z 1997 r. Nr 78, poz. 483 ze zm.).

[23] *Polskie prawo konstytucyjne...*, s. 29.

[24] Te ostatnie mają moc powszechnie obowiązującą, ale wyłącznie na obszarze działania organów, które je ustanowiły.

pracy, ochronę godności człowieka oraz dotyczące: zasady równości, praw i wolności zbiorowych, a także bezpiecznych i higienicznych warunków pracy. Konstytucja jako podstawa polskiego systemu prawnego nie zawiera rozbudowanych przepisów bezpośrednio odnoszących się do stosunków służbowych. Wpływ na ukształtowanie poszczególnych instytucji w ustawach pragmatycznych będą miały unormowania z zakresu organizacji i funkcjonowania aparatu państwowego. Najważniejsze z nich to: zasady funkcjonowania służby cywilnej (art. 153 Konstytucji RP), prawo obywateli polskich do równego dostępu do służby publicznej (art. 60 Konstytucji RP), prawo do informacji o działalności organów państwowych (art. 61 Konstytucji RP) i prawo do wynagrodzenia szkody wyrządzonej przez niezgodne z prawem działanie organu władzy publicznej (art. 77 Konstytucji RP). Jednocześnie w ustawie zasadniczej znajdziemy wiele ograniczeń praw obywatelskich i pracowniczych osób pełniących służbę publiczną, jak np.: przewidziane w art. 178 ust. 3 wyłączenie uprawnień związkowych sędziów czy określoną w art. 103 zasadę incompatibilitas, *której istota polega na wskazaniu tych funkcji i stanowisk, których nie można łączyć z wykonywaniem mandatu przedstawicielskiego*[25].

1.2. Prawo międzynarodowe

Prawo stosunków służbowych bez wątpienia stanowi domenę krajowych unormowań prawnych. Z oczywistych względów państwa autonomicznie decydują o systemie funkcjonowania władzy publicznej, a tym samym o statusie zawodowym osób zatrudnionych w administracji publicznej. Akty prawa międzynarodowego dotyczące tematyki niniejszego opracowania zawierają głównie postanowienia z zakresu praw obywatelskich, a konkretnie dostępu do służby publicznej. I tak, w Powszechnej Deklaracji Praw Człowieka z 10.12.1948 r. oraz w Międzynarodowym Pakcie Praw Obywatelskich i Politycznych z 19.12.1966 r. (Dz.U. z 1977 r. Nr 38, poz. 167) podkreślono prawo do równego dostępu do służby publicznej w swoim kraju, bez żadnej dyskryminacji i bez nieuzasadnionych ograniczeń. Kwestia ta została również uwzględniona w Konwencji Międzynarodowej Organizacji Pracy Nr 151 z 27.06.1978 r. (Dz.U. z 1994 r. Nr 22, poz. 78), w której wskazano na ochronę prawa do organizowania się oraz na procedury określania warunków zatrudnienia w służbie publicznej. W tym miejscu należy zwrócić uwagę, że z prawa unijnego dotyczącego swobody przepływu osób została wyłączona kwestia zatrudnienia w sferze publicznej. Co więcej, w art. 45 ust. 4 traktatu o funkcjonowaniu Unii Europejskiej (Dz.U. z 2004 r. Nr 90, poz. 864 ze zm.) dokonano ograniczenia wolności pracy w odniesieniu do zatrudnionych w służbie publicznej. W praktyce przekłada się to na możliwość ustanawiania przez kraje członkowskie ograniczenia w dostępie do służby publicznej dla osób bez obywatelstwa danego państwa. Kwestia ta została poruszona również w orzecznictwie Trybunału Sprawiedliwości, w którym widnieje zapis, że *zatrudnienie w służbie publicznej musi ograniczać się jedynie do stanowisk istotnych dla ochrony ważnych interesów państwa. Chodzi tu o interesy, które z istoty swej wymagają istnienia szczególnej więzi pomiędzy funkcjonariuszami a państwem, opartej na lojalności, jakiej można oczekiwać od własnych obywateli*[26]. Ponadto, bez wchodzenia w szczegóły, należy tu wspomnieć o Europejskim Kodeksie Dobrej Administracji, mimo że nie jest on źródłem prawa

[25] *Polskie prawo konstytucyjne*..., s. 131.

[26] T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy*..., s. 133.

dla państw UE. Jest to w istocie zbiór reguł, wyznaczający standardy organizowania i funkcjonowania administracji publicznej w kontekście praw obywatelskich.

1.3. Pragmatyki służbowe służb zmilitaryzowanych

Wszystkie służby funkcjonujące w Polsce mają oddzielne regulacje prawne rangi ustawowej, zwane pragmatykami służbowymi. Tworzą one autonomiczne podsystemy normatywne, których podstawą są następujące akty prawne:

1) ustawa z 6.04.1990 r. o Policji (tekst jedn. Dz.U. z 2011 r. Nr 287, poz. 1687 ze zm.),
2) ustawa z 12.10.1990 r. o Straży Granicznej (tekst jedn. Dz.U. z 2011 r. Nr 116, poz. 675 ze zm.),
3) ustawa z 24.08.1991 r. o Państwowej Straży Pożarnej (tekst jedn. Dz.U. z 2009 r. Nr 12, poz. 68 ze zm.),
4) ustawa z 21.08.1997 r. Prawo o ustroju sądów wojskowych (tekst jedn. Dz.U. z 2012 r., poz.952),
5) ustawa z 16.03.2001 r. o Biurze Ochrony Rządu (tekst jedn. Dz.U. z 2004 r. Nr 163, poz. 1712 ze zm.),
6) ustawa z 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tekst jedn. Dz.U. z 2010 r. Nr 29, poz. 154 ze zm.),
7) ustawa z 11.09.2003 r. o służbie wojskowej żołnierzy zawodowych (tekst jedn. Dz.U. z 2010 r. Nr 90, poz. 593 ze zm.),
8) ustawa z 9.06.2006 r. o Centralnym Biurze Antykorupcyjnym (tekst jedn. Dz.U. z 2012 r. poz. 621 ze zm.),
9) ustawa z 9.06.2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego (Dz.U. z 2006 r. Nr 104, poz. 710 ze zm.),
10) ustawa z 27.08.2009 r. o Służbie Celnej (Dz.U. z 2009 r. Nr 168, poz. 1323 ze zm.),
11) ustawa z 9.04.2010 r. o Służbie Więziennej (Dz.U. z 2010 r. Nr 79, poz. 523 ze zm.).

Wszystkie wymienione ustawy pragmatyczne posługują się instytucją stosunku służbowego dla określenia więzi prawnej pomiędzy żołnierzami i funkcjonariuszami a daną formacją. W każdym z tych aktów prawnych znajdziemy odrębne uregulowania – bardziej lub mniej szczegółowe – odnoszące się do nawiązywania, kształtowania i rozwiązywania stosunków służbowych oraz określania ich treści (tj. praw i obowiązków podmiotów). Poszczególne ustawy nie tworzą jednego, spójnego systemu. Co prawda można zauważyć zbieżność w ich konstrukcji przy określaniu stosunku służbowego, ale należy wskazać, że istnieje dyferencja statusu funkcjonariuszy w zakresie ich praw i obowiązków, wynikająca choćby z faktu, że pragmatyki te pochodzą z różnych okresów. *Co więcej, poza nielicznymi przypadkami brak jest odesłań między pragmatykami służbowymi, paradoksalnie w każdej z nich znajdują się odesłania do przepisów prawa pracy, a nie do innych – zdawałoby się – „pokrewnych" aktów prawnych, regulujących zbliżone co do charakteru prawnego materie*[27].

Istotną cechą wspólną norm prawnych zawartych w wymienionych aktach jest to, że mają one charakter bezwzględnie obowiązujący, czyli ich stosowanie nie może być wyłączone na mocy porozumienia stron stosunku służbowego.

Bardziej syntetycznie uregulowaną kwestią jest sprawa zaopatrzenia emerytalnego funkcjonariuszy tych formacji. W tym zakresie obowiązuje ustawa z 18.02.1994 r. o zaopatrzeniu emerytalnym funkcjonariuszy Policji, Agencji Bezpieczeństwa

[27] Tamże, s. 135.

Wewnętrznego, Agencji Wywiadu, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego, Centralnego Biura Antykorupcyjnego, Straży Granicznej, Biura Ochrony Rządu, Państwowej Straży Pożarnej i Służby Więziennej oraz ich rodzin (tekst jedn. Dz.U. z 2004 r. Nr 8, poz. 67 ze zm.) oraz ustawa z 10.12.1993 r. o zaopatrzeniu emerytalnym żołnierzy zawodowych oraz ich rodzin (tekst jedn. Dz.U. z 2004 r. Nr 8, poz. 66 ze zm.). Wyjątek stanowią tu funkcjonariusze Służby Celnej, których ustawodawca przyporządkował do powszechnego systemu ubezpieczeń społecznych.

Na podstawie charakterystyki stosunków służbowych opisanych w poszczególnych pragmatykach doktryna dokonuje prób usystematyzowania prawa tych stosunków. Jedną z ciekawszych koncepcji jest podział na pragmatyki typu wojskowego, policyjnego oraz pragmatyki cywilnych służb specjalnych. Pierwszą grupę, obejmującą ustawy o służbie wojskowej żołnierzy zawodowych, o SKW i SWW oraz o BOR, cechuje służba o największym natężeniu dyspozycyjności i ograniczeniu uprawnień obywatelskich. Do kolejnego typu zalicza się ustawy o Policji, SG, SW, PSP i SC, które wykazują najwięcej cech zbliżonych do regulacji pracowniczych. Ostatnia, skupiająca ustawy o ABW i AW oraz o CBA, zawiera elementy pośrednie i wyróżnia się m.in. mniejszym zakresem dyspozycyjności osób pełniących służbę w porównaniu z wojskową koncepcją służby.

Licznymi źródłami prawa w tej dziedzinie są również rozporządzenia. Są to akty prawne wykonawcze wydawane przez ministrów, Radę Ministrów lub Prezesa Rady Ministrów na podstawie norm kompetencyjnych. Uszczegóławiają one rozwiązania zawarte w ustawach pragmatycznych. Omawianie ich w szerszym zakresie nie jest celowe, ponieważ nie mają one decydującego wpływu na charakter poszczególnych stosunków służbowych.

1.3.4. Źródła prawa o charakterze wewnętrznym, dotyczące stosunków służbowych służb zmilitaryzowanych

Art. 93 Konstytucji RP wymienia następujące akty prawa wewnętrznego: uchwały Rady Ministrów oraz zarządzenia Prezesa Rady Ministrów i ministrów. Nie są to źródła prawa o charakterze powszechnym. Przepisy tych regulacji obowiązują jednostki organizacyjne podległe organowi wydającemu dany akt i mają doniosłe znaczenie dla sprawności funkcjonowania i realizacji zadań publicznych przez zhierarchizowane struktury służb. Część pragmatyk zawiera przepisy ustrojowo służbowe, dotyczące upoważnienie Prezesa Rady Ministrów, ministrów lub szefów służb do regulowania w drodze zarządzeń struktur organizacyjnych poszczególnych formacji. Treścią wewnętrznych aktów prawnych są zagadnienia dotyczące: organizacji i pełnienia służby, obiegu informacji służbowej, prowadzenia dokumentacji, ceremoniału musztry, mianowania na wyższe stanowiska oraz stopnie służbowe itp.

Oprócz zarządzeń istotne z punktu widzenia prawa stosunków służbowych są statuty i regulaminy. Te wewnętrzne akty prawne są wprost wymienione w części ustaw pragmatycznych i często doprecyzowują warunki korzystania z praw oraz wypełniania obowiązków przez żołnierzy i funkcjonariuszy służb państwowych.

1.4. Pragmatyki pracownicze

Na wstępie omawiania pragmatyk pracowniczych należy wspomnieć o różnorodnym charakterze pracowników administracji publicznej. Trzeba pamiętać, że regulacje prawne dotyczące stosunków pracowniczych, podobnie jak dotyczące stosunków służ-

bowych, nie stanowią jednego spójnego systemu. Każda z pragmatyk pracowniczych to autonomiczne unormowanie prawne. W odróżnieniu od administracyjnych stosunków służbowych można tu wskazać wspólny punkt odniesienia dla ogółu pracowników sfery publicznej w postaci przepisów prawa pracy. Konstrukcja stosunku pracy jest kompleksowa i jednorodna we wszystkich omawianych tu aktach prawnych. Przepisy te są traktowane, zgodnie z art. 5 kodeksu pracy, jako przepisy szczególne wobec norm generalnych powszechnego prawa pracy.

Odwołując się do omówionej wyżej systematyki pracowniczych stosunków służbowych, można wyróżnić trzy grupy pragmatyk pracowniczych[28]. Do pierwszej, obejmującej tzw. stosunki służbowo-pracownicze charakteryzujące się występowaniem cech właściwych dla służby, należy zatrudnianie sędziów i prokuratorów na podstawie: ustawy z 27.07.2001 r. prawo o ustroju sądów powszechnych (Dz.U. z 2001 r. Nr 98, poz. 1070 ze zm.), ustawy z 20.06.1985 r. o prokuraturze (tekst jedn. Dz.U. z 2011 r. Nr 270, poz. 1599 ze zm.), ustawy z 23.11.2002 r. o Sądzie Najwyższym (Dz.U. z 2002 r. Nr 240, poz. 2052 ze zm.) i ustawy z 25.07.2002 r. prawo o ustroju sądów administracyjnych (Dz.U. z 2002 r. Nr 153, poz. 1269 ze zm.).

Kolejna grupa pragmatyk dotyczy stosunków pracowniczo-służbowych i obejmuje nominacyjne zatrudnienie w administracji publicznej. Do tej grupy są przyporządkowani urzędnicy mianowani na podstawie ustawy o służbie cywilnej, a także członkowie służby zagranicznej, których stosunek pracy jest oparty na ustawie z 27.07.2001 r. o służbie zagranicznej (Dz.U. z 2001 r. Nr 128, poz. 1403 ze zm.), inspektorzy pracy mianowani na podstawie ustawy z 13.04.2007 r. o Państwowej Inspekcji Pracy (tekst jedn. Dz.U. z 2012 r., poz. 404) oraz kontrolerzy NIK zatrudnieni na podstawie ustawy z 23.12.1994 r. o Najwyższej Izbie Kontroli (tekst jedn. Dz.U. z 2012 r., poz. 82).

Ostatnia, najliczniejsza, grupa pragmatyk dotyczy stosunków pracy z elementami służbowymi, uregulowanych w: ustawie z 21.11.2008 r. o pracownikach samorządowych (Dz. U. z 2008 r. Nr 223, poz. 1458 ze zm.), ustawie z 16.09.1982 r. o pracownikach urzędów państwowych (tekst jedn. Dz.U. z 2001 r. Nr 86, poz. 953 ze zm.), ustawie z 18.12.1998 r. o pracownikach sądów i prokuratury (tekst jedn. Dz.U. z 2011 r. Nr 109, poz. 639 ze zm.), ustawie z 26.01.1982 r. Karta Nauczyciela (tekst jedn. Dz.U. z 2006 r. Nr 97, poz. 674 ze zm.), ustawie z 27.07.2005 prawo o szkolnictwie wyższym (tekst jedn. Dz.U. z 2012 r., poz. 572), ustawie z 30.04.2010 r. o instytutach badawczych (Dz.U. z 2010 r. Nr 96, poz. 618 ze zm.), ustawie z 30.04.2010 r. o Polskiej Akademii Nauk (Dz.U. z 2010 r. Nr 96, poz. 619 ze zm.) oraz ustawie z 27.07.2001 o kuratorach sądowych (Dz.U. z 2001 r. Nr 98, poz. 1071). Do tej grupy należy także ustawa o służbie cywilnej, dotycząca pracowników tej służby.

Innym podziałem pragmatyk pracowniczych wypracowanym przez doktrynę, jest wyróżnienie pragmatyk urzędniczych, nauczycielskich i sędziowskich.

Regulacja treści stosunków pracy we wskazanych wyżej aktach prawnych ma znaczenie dla określenia charakteru prawnego norm w nich zawartych, w kontekście rozwiązań systemowych prawa pracy. Zgodnie z art. 18 kodeksu pracy postanowienia umów o pracę oraz innych aktów, na których mocy powstaje stosunek pracy, nie mogą być mniej korzystne dla pracownika niż przepisy prawa pracy. Wpływa to na uznanie za nieważne mniej korzystnych dla pracownika unormowań prawnych oraz wynikających ze stypulacji postanowień, a tym samym na zastosowanie rozwiązań kodeksowych. *W praktyce jednak niezmiernie rzadko dochodzi w sferze publicznej do kształtowania*

[28] Tamże, s. 141.

treści stosunków pracy w sposób odmienny od wynikającego z treści norm prawnych. Semidyspozytywność norm pragmatycznych nie oznacza bowiem, że kierownicy urzędów i innych jednostek są zwolnieni z rygorów dyscypliny budżetowej[29].

Wśród źródeł prawa pracowniczych stosunków służbowych dużą rolę odgrywają również rozporządzenia. Upoważnienia ustawowe w zakresie wydawania aktów wykonawczych są zawarte w każdej pragmatyce pracowniczej. W odniesieniu do regulacji treści stosunków służbowych odgrywają one taką samą rolę, jak w przypadku unormowań stosunków publicznoprawnych, i z tych samych względów nie wymagają szerszego omawiania.

1.4.1. Źródła prawa o charakterze wewnętrznym, dotyczące pracowniczych stosunków służbowych

Akty prawa wewnętrznego są istotne dla treści stosunków pracy tylko w rozbudowanych strukturach organizacyjnych (służba cywilna, NIK, PIP, sądy i prokuratury). W tych przypadkach ich formy i role są tożsame z formą i rolą zarządzeń wydawanych przez organy służb zmilitaryzowanych. W pozostałych przypadkach mamy do czynienia z sytuacją, w której między pracownikiem a organem centralnym nie zachodzi bezpośrednia zależność organizacyjna. Wówczas akty prawne wydawane przez kierownictwo wewnętrzne mogą być pośrednim źródłem praw pracowniczych.

1.4.2. Specyficzne źródła prawa pracy w zakresie pracowniczych stosunków służbowych

W przypadku prawa pracy istotną rolę odgrywają źródła charakterystyczne dla tej gałęzi prawa. Zgodnie z art. 9 kodeksu pracy są to układy zbiorowe pracy, inne porozumienia zbiorowe, regulaminy oraz statuty. Obok najważniejszej funkcji – regulacyjnej – przy realizacji grupowych interesów pracowniczych mają one znaczenie praktyczne. W sektorze publicznym ich funkcja jest ograniczona lub zupełnie wyłączona. Wynika to albo z ustawowych ograniczeń niektórych praw pracowniczych, albo z kompleksowej regulacji treści stosunku pracy w danej pragmatyce i rozporządzeniach. W zakresie dotyczącym tematyki niniejszego artykułu najczęściej mamy do czynienia z regulaminami wewnętrznymi. Najważniejsze spośród nich to regulamin pracy (organizacyjny) oraz regulamin wynagradzania i premiowania. Określają one organizację i porządek pracy oraz związane z nimi prawa i obowiązki stron stosunku pracy.

III. Przedmiot prawa stosunków służbowych

Przedmiotem prawa stosunków służbowych są stosunki służbowe o charakterze formalnym i instytucjonalnym. Te ostatnie odnoszą się do spraw wynikających z więzi pomiędzy pracodawcą a pracownikiem wykonującym zadania na rzecz państwa. Specyficzny charakter tego stosunku prawnego wynika z podporządkowania i dyspozycyjności zatrudnionego, jak również z jednostronnie ustalonych przez państwo warunków oraz obowiązków wykraczających poza zobowiązaniową sferę stosunku pracy. *W ramach stosunków służbowych o charakterze formalnym podmioty służbowe, działając jako organy lub pełnomocnicy władzy publicznej, mogą w prawem*

[29] Tamże, s. 144.

przewidzianych przypadkach, w związku ze świadczeniem przez funkcjonariusza lub pracownika służby (pracy) dobrowolnie podporządkowanej, związanej z realizacją zadań publicznych państwa, wykonywanej osobiście, w celach zarobkowych, jednostronnie kształtować ich całościowo ujmowany status służbowy z uwagi na kryterium interesu (dobra) służby[30]. Publicznoprawny charakter przedmiotu tych stosunków wynika z tego, że sprawa należy do sfery działania administracji i jest regulowana w trybie nakazów administracyjnych. W odróżnieniu od treści dotyczących stosunku cywilnego, przedmiot określony w treści odnoszącej się do stosunków publicznoprawnych musi wynikać bezpośrednio z przepisów materialnego prawa administracyjnego. W związku z powyższym prawa i obowiązki w tym przypadku wynikają z ustaw pragmatycznych, wyznaczając nakazy i zakazy związane ze służbą. Konsekwencją tego jest to, że przełożeni, *kształtując sytuację prawną funkcjonariuszy i żołnierzy, nie mogą wyjść poza przepisy ustawowe, a funkcjonariusze i żołnierze zawodowi nie mogą żądać większych uprawnień niż te, jakie są dla nich określone w ustawach pragmatycznych*[31]. W formacjach zmilitaryzowanych przedmiotem stosunku służbowego jest obowiązek poddania się rygorowi wynikającemu ze służby, a wyrażający się w poświęceniu się i dyspozycyjności. Ma to swoje konsekwencje w sposobie wykonywania owej służby (rozkazy, polecenia, umundurowanie, wyposażenie) oraz w zakresie uprawnień wpływających na stabilność zatrudnienia.

Przedstawienie problematyki przedmiotu prawa stosunków służbowych wymaga również przybliżenia problematyki dotyczącej postępowań kwalifikacyjnych (konkursowych, egzaminacyjnych i weryfikacyjnych), które są uregulowane we wszystkich pragmatykach służbowych. Przystąpienie osób do tych postępowań skutkuje powstaniem stosunków prawnych: poprzedzających nawiązanie stosunku służbowego (np.: postępowanie kwalifikacyjne w sprawie przyjęcia na aplikację ogólną w Krajowej Szkole Sądownictwa i Prokuratury, postępowanie rekrutacyjne do Krajowej Szkoły Administracji Publicznej), dotyczących włączenia do służby (np.: procedura powoływania sędziów, prokuratorów i etatowych członków Samorządowego Kolegium Odwoławczego) oraz obejmujących awans zawodowy (np.: postępowanie kwalifikacyjne dla osób ubiegających się o mianowanie do służby cywilnej i postępowanie kwalifikacyjne na stopień awansu zawodowego nauczycieli). Ponadto w treści stosunków służbowych zawiera się wiele praw i obowiązków związanych z zakończeniem więzi służbowej (np.: dotyczących świadczeń i należności pieniężnych, obowiązku dochowania tajemnicy służbowej czy uprawnień honorowych).

Przedmiot stosunków służbowych obejmuje również stosunki prawne będące konsekwencją czynności o charakterze dyrektywnym, świadczeniowym, dystrybutywnym i dyscyplinarnym, podejmowanych przez przełożonego. Czynności dyrektywne mogą dotyczyć procesu organizacji pracy w ramach podporządkowania służbowego bądź procesu przekształcania zatrudnienia w ramach dyspozycyjności służbowej. Kolejne czynności – świadczeniowe – są związane z realizacją uprawnień funkcjonariusza publicznego do uzyskania prawnie wskazanych należności, takich jak: świadczenia uposażeniowe, urlopowe, socjalne itp. W relacjach przełożony–podwładny szczególny charakter mają czynności dystrybutywne, które mają wpływ na rozdział świadczeń związanych z wykonywaniem pracy czy pełnieniem służby. W odróżnieniu od czynności świadczeniowych czynności te są zależne od decyzji kierownika służby

[30] Tamże, s. 47.

[31] P. Szustakiewicz, *Stosunki służbowe funkcjonariuszy służb mundurowych*..., s. 42.

lub upoważnionego przełożonego i konstytuują nową sytuację prawną, np. przyznanie wyższego stopnia służbowego, mianowanie na stanowisko służbowe, przyznanie urlopu dla podratowania zdrowia itp. Ostatnie z wymienionych czynności, tj., czynności dyscyplinarne, a konkretnie rozstrzygnięcia dyscyplinarne, mogą wpływać na status zawodowy funkcjonariusza, urzędnika lub pracownika poszczególnych instytucji publicznych[32].

Abstrakt

W polskim systemie prawnym występuje szereg unormowań regulujących zagadnienie stosunków służbowych. Niniejszy artykuł w sposób ogólny charakteryzuje poszczególne rodzaje stosunków prawnych będących podstawą do wyodrębnienia prawa stosunków służbowych i jest próbą usystematyzowania pojęć i instytucji prawnych oraz przybliżenia relacji występujących w ramach więzi prawnej pomiędzy pracownikami, urzędnikami, funkcjonariuszami i żołnierzami a organami administracji publicznej.

W opracowaniu wskazano na problem utożsamienia „interesu służby" z „interesem państwa", jako na element łączący stosunki służbowe o różnorodnym charakterze. Z drugiej strony, w celu usystematyzowania niejednolitej grupy stosunków prawnych, dokonano rozróżnienia na „stosunki służbowe publicznoprawne" i „stosunki służbowe prywatnoprawne".

Artykuł zawiera ponadto omówienie podstawowych źródeł prawa dotyczących problematyki zawartej w tytule z uwzględnieniem uregulowań międzynarodowych.

Abstract

In the Polish legal system there are plenty of regulations concerning employment relationships. This article describes the general terms of individual legal relationships as a legal basis for the development of an independent law of employment relationships. The publication is an attempt at systematizing legal terms and institutions as well as presenting relations which develop in terms of the legal dependencies between employees, clerks, public officers, soldiers and the public administration authorities. This article indicates the problem of considering "the interests of service" and "interests of state" as two equivalent notions, which is a common element of employment relationships of various nature.

On the other hand, in order to systematize a non-uniform group of legal relationships the author has differentiated between: "public law employment relationships" and "private law employment relationships".

Moreover, the article contains an overview of basic sources of law concerning the presented issue including international legal regulations.

[32] T. Kuczyński, E. Mazurczak-Jasińska, J. Stelina, *Stosunek służbowy...*, s. 48–52.

Przemysław Szustakiewicz

Postępowanie dyscyplinarne w służbach specjalnych w świetle orzecznictwa sądów administracyjnych

1. Uwagi wstępne

Służby specjalne są wyspecjalizowanymi organami państwa powołanymi do zwalczania szczególnych zagrożeń dla funkcjonowania kraju. W odróżnieniu od innych formacji zmilitaryzowanych charakteryzują się one tym, że działają w sposób niejawny, a ich działalność obejmuje również wykonywanie czynności poza terytorium Rzeczypospolitej Polskiej. Ponadto część tych służb ma szczególną pozycję w ustroju państwa, ponieważ ich szefowie podlegają bezpośrednio Prezesowi Rady Ministrów, a ich funkcjonowanie jest przedmiotem kontroli parlamentarnej dokonywanej za pośrednictwem Sejmowej Komisji ds. Służb Specjalnych.

Obecnie w Polsce funkcjonuje pięć służb specjalnych: Agencja Bezpieczeństwa Wewnętrznego (dalej: ABW), Agencja Wywiadu (dalej: AW), Służba Kontrwywiadu Wojskowego (dalej: SKW), Służba Wywiadu Wojskowego (dalej: SWW) oraz Centralne Biuro Antykorupcyjne (dalej: CBA).

Charakter zadań postawionych przed służbami specjalnymi powoduje, że szczególnego znaczenia nabiera sposób wypełniania przez funkcjonariuszy obowiązków służbowych, które powinny być wypełniane jak najlepiej. Należy przypomnieć, że funkcjonariusze służb mundurowych pełnią swoje obowiązki w ramach specyficznego stosunku prawnego łączącego ich z daną służbą – stosunku służbowego. Jego cechą jest to, że funkcjonariusze podlegają prawu administracyjnemu, a nie prawu pracy[1], a *na treść tych stosunków, jak się przyjmuje, składają się wzajemne prawa i obowiązki stron nie mające charakteru zobowiązaniowego*[2]. Zadania wykonywane przez funkcjonariuszy służb specjalnych są podporządkowane celom, dla których te formacje zostały powołane. Wiążą się one z zapewnieniem bezpieczeństwa publicznego, rozumianego jako *państwo ze swoim ustrojem i innymi urządzeniami oraz obywatele, ich życie, zdrowie i mienie*[3]. Tak ważne zadania postawione przed służbami specjalnymi powodują, że ich funkcjonariusze muszą pełnić swoje obowiązki w sposób szczególny, wykazując się dużą starannością i szczególnym podporządkowaniem się poleceniom przełożonych. Charakter stosunku służbowego w służbach specjalnych sprawia, że konieczne jest stworzenie systemu prawnego chroniącego prawidłowość wykonywania przez nie zadań. Elementem tego systemu jest swoisty rodzaj odpowiedzialności, której podlegają funkcjonariusze – odpowiedzialność dyscyplinarna. Podniósł to Trybunał Konstytucyjny w wyroku z 8 października 2002 r. (sygn. akt K 36/00) wydanym na podstawie prze-

[1] Więcej na temat istoty stosunku służbowego w służbach mundurowych zob. P. Szustakiewicz, *Stosunki służbowe funkcjonariuszy służb mundurowych i żołnierzy zawodowych*, Warszawa 2012, Difin, s. 17–53.

[2] M. Liwo, *Status służb mundurowych i funkcjonariuszy w nich zatrudnionych*, Warszawa 2013, LexisNexis, s. 288.

[3] S. Pieprzny, *Administracja bezpieczeństwa i porządku publicznego*, Rzeszów 2012, Wydawnictwo Uniwersytetu Rzeszowskiego, s. 14–15.

pisów dyscyplinarnych dotyczących policjantów. Trybunał Konstytucyjny wskazał, że objęcie funkcjonariuszy *odpowiedzialnością dyscyplinarną uzasadnia społeczna rola tej formacji, charakter powierzonych zadań i kompetencji oraz związane z działalnością policji publiczne zaufanie. Służyć ma również przeciwdziałaniu takim zachowaniom, które mogłyby pozbawić ją wiarygodności w oczach opinii publicznej, zwłaszcza, że wiele uprawnień przyznanych policji pozwala na ingerowanie w sferę obywatelskich wolności i praw*[4]. Orzeczenie to, choć nie dotyczy funkcjonariuszy omawianych formacji, lecz innej służby mundurowej, znakomicie uchwyciło cel postępowania dyscyplinarnego w służbach mundurowych, w którym jest ochrona prawidłowości działania danej służby, w tym także jej funkcjonowania w otoczeniu społecznym. Oczywiste jest bowiem, że w demokratycznym państwie, w którym wszystkie instytucje publiczne podlegają nieustannej kontroli społeczeństwa, nie może dobrze działać instytucja, w której zadania wykonują osoby niecieszące się zaufaniem i szacunkiem obywateli.

Należy jednak podkreślić, że pomimo podobieństwa zadań i stosowanych metod działania służb specjalnych, ustawodawca niejednolicie określił zakres i przebieg postępowań dyscyplinarnych w nich obowiązujących. Postępowania dyscyplinarne dla każdej z pięciu służb specjalnych zostały uregulowane w odrębny sposób, bez względu na to, że niektóre z nich mają wspólne uregulowania ustawowe dotyczące ich kompetencji i regulacji związanych ze stosunkiem służbowym funkcjonariuszy służb mundurowych. W poszczególnych służbach specjalnych postępowania dyscyplinarne są uregulowane w następujących aktach prawnych:

- ABW – rozdział 10 *Ustawy z dnia 25 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[5], dalej: uoABWoAW oraz *Rozporządzenie Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego*[6],
- AW – rozdział 10 *Ustawy z dnia 25 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu,* a także *Rozporządzenie Prezesa Rady Ministrów z dnia 20 sierpnia 2003 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu*[7],
- SKW – rozdział 6 *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[8], dalej: uoSKWoSWW i *Rozporządzenie Ministra Obrony Narodowej z dnia 29 września 2006 r. w sprawie postępowania dyscyplinarnego w stosunku do funkcjonariuszy Służby Kontrwywiadu Wojskowego*[9],
- SWW – rozdział 6 *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* i *Rozporządzenie Ministra Obrony Narodowej z dnia 29 września 2006 r. w sprawie postępowania dyscyplinarnego w stosunku do funkcjonariuszy Służby Wywiadu Wojskowego*[10],

[4] OTK ZU nr 5/A/2002, poz. 63.

[5] Dz.U. z 2010 r. Nr 29, poz. 154 ze zm.

[6] Dz.U. Nr 272, poz. 2690 ze zm.

[7] Dz.U. Nr 160, poz. 1557 ze zm.

[8] Dz.U. Nr 104, poz. 710 ze zm.

[9] Dz.U. Nr 188, poz. 1391.

[10] Dz.U. Nr 188, poz. 1392.

- CBA – rozdział 7 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*[11], dalej: uoCBA oraz *Rozporządzenie Prezesa Rady Ministrów z dnia 6 listopada 2006 r. w sprawie szczegółowego trybu wykonywania czynności związanych z postępowaniem dyscyplinarnym w stosunku do funkcjonariuszy Centralnego Biura Antykorupcyjnego*[12].

2. Zakres przedmiotowy odpowiedzialności dyscyplinarnej

We wszystkich służbach specjalnych ustalono ogólną klauzulę odpowiedzialności dyscyplinarnej. Zgodnie z art. 145 ust. 1 uoABWoAW, art. 106 ust. 1 uoSKWoSWW oraz art. 107 ust. 1 uoCBA funkcjonariusze ponoszą odpowiedzialność dyscyplinarną za dwa rodzaje czynów: za naruszenie dyscypliny służbowej oraz w innych przypadkach określonych w ustawach.

Ustawy nie określają definicji przewinienia dyscyplinarnego. Jest ono natomiast definiowane przez określenie w kolejnych przepisach katalogu czynów, za które funkcjonariusz może zostać ukarany. W tym wypadku jednak ustawodawca sformułował różne katalogi czynów, które są przewinieniami dyscyplinarnymi w poszczególnych służbach specjalnych. Mamy tutaj dwa rozwiązania:

- przewinienia dyscyplinarne stanowią zamknięty katalog czynów – w odniesieniu do AW, CBA,
- wymienione przewinienia dyscyplinarne nie stanowią zamkniętego katalogu czynów, a podane w przepisach wyliczenie ma jedynie charakter przykładowy – i w odniesieniu do ABW, wojskowych służb specjalnych).

Nawet w przypadku służb, których status został określony w jednym akcie prawnym, a więc ABW i AW, ustawodawca w różny sposób określił zakres przedmiotowy odpowiedzialności dyscyplinarnej funkcjonariuszy.

Zgodnie z treścią § 4 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 sierpnia 2003 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu* przewinieniem dyscyplinarnym jest:

1) niedopełnienie obowiązków służbowych,
2) odmowa wykonania albo niewykonanie rozkazu lub polecenia służbowego, z wyjątkiem przypadku, o którym mowa w art. 79 ust. 2 uoABWoAW, oraz gdy odmowa dotyczy wykonania polecenia służbowego, które nie pozostaje w związku z pełnieniem służby,
3) zaniechanie wykonania czynności służbowej albo wykonanie jej w sposób niedbały lub niezgodny z rozkazem lub poleceniem służbowym,
4) świadome wprowadzenie w błąd przełożonego lub innego funkcjonariusza, jeżeli spowodowało to lub mogło spowodować szkodę dla służby, funkcjonariusza bądź innej osoby,
5) nadużycie zajmowanego stanowiska do osiągnięcia korzyści majątkowej lub osobistej,
6) wprowadzenie się w stan ograniczający zdolność wykonywania zadania służbowego lub uniemożliwiający jego wykonanie,
7) utrata służbowej broni palnej, amunicji lub legitymacji służbowej,
8) utrata dokumentu stanowiącego tajemnicę państwową lub służbową,

[11] Dz.U. z 2012 r. Nr 0, poz. 621.

[12] Dz.U. Nr 203, poz. 1495.

9) porzucenie służby,
10) samowolne oddalenie się z rejonu zakwaterowania bądź nieusprawiedliwione opuszczenie lub niestawienie się do miejsca pełnienia służby,
11) umyślne naruszenie dóbr osobistych innego funkcjonariusza w czasie pełnienia służby.

Z kolei wedle treści art. 107 ust. 2 uoCBA funkcjonariusz CBA popełnienia przewinienie dyscyplinarne wtedy, gdy:

1) odmawia wykonania polecenia przełożonego, lub nie wykonuje polecenia przełożonego, względnie organu, który jest uprawniony na podstawie ustawy do wydawania poleceń funkcjonariuszom CBA, z wyłączeniem poleceń, o których mowa w art. 71 ust. 2 uoCBA,
2) zaniecha czynności służbowej albo wykona ją w sposób nieprawidłowy,
3) niedopełni obowiązków służbowych albo przekroczy uprawnienia określone w przepisach prawa,
4) wprowadzi w błąd przełożonego lub innego funkcjonariusza, jeżeli spowoduje to lub może spowodować szkodę dla służby, funkcjonariusza lub innej osoby,
5) będąc przełożonym działa w sposób przyczyniający się do rozluźnienia dyscypliny służbowej w podległej jednostce organizacyjnej lub komórce organizacyjnej CBA,
6) stawi się do służby w stanie po spożyciu alkoholu lub po użyciu podobnie działającego środka odurzajacego oraz spożywa alkohol lub używa podobnie działającego środka w czasie służby albo w obiektach lub na terenach zajmowanych przez CBA,
7) utraci służbową broń palną, amunicję lub legitymację służbową,
8) utraci przedmiot stanowiący wyposażenie służbowe, którego wykorzystanie przez osoby nieuprawnione wyrządziło szkodę obywatelowi lub stworzyło zagrożenie dla porządku publicznego lub bezpieczeństwa powszechnego,
9) utraci materiał zawierający informacje niejawne,
10) ujawni informacje pozostające w związku z wykonywaniem czynności służbowych.

Zgodnie z § 8 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* przewinienie dyscyplinarne polega w szczególności na:

1) odmowie wykonania albo niewykonaniu rozkazu lub polecenia służbowego, z wyjątkiem przypadku, o którym mowa w art. 79 ust. 2uoABWoAW, oraz gdy odmowa dotyczy wykonania polecenia, które nie pozostaje w związku z pełnieniem służby,
2) zaniechaniu wykonania czynności służbowej albo wykonaniu jej w sposób niedbały lub niezgodny z rozkazem lub poleceniem służbowym,
3) świadomym wprowadzeniu w błąd przełożonego lub innego funkcjonariusza, jeżeli spowodowało to lub mogło spowodować szkodę dla służby, funkcjonariusza albo innej osoby,
4) umyślnym naruszeniu dóbr osobistych innego funkcjonariusza albo innej osoby, w czasie pełnienia służby lub w związku z jej pełnieniem,
5) wprowadzeniu się w stan ograniczający zdolność wykonywania obowiązków służbowych albo uniemożliwiający ich wykonywanie,
6) zawinionej utracie broni służbowej lub amunicji, legitymacji służbowej, a także dokumentu zawierającego informacje stanowiące tajemnicę państwową albo służbową,
7) nadużyciu zajmowanego stanowiska lub służby dla osiągnięcia korzyści majątkowej lub osobistej,

8) samowolnym oddaleniu się z rejonu zakwaterowania, jeżeli funkcjonariusz pełni służbę w systemie skoszarowanym, a także nieusprawiedliwionym opuszczeniu lub niestawieniu się w miejscu pełnienia służby,
9) porzuceniu służby.

Według art. 106 ust. 2 uoSKWoSWW naruszeniem dyscypliny służbowej jest w szczególności:

1) odmowa wykonania albo niewykonanie rozkazu lub polecenia służbowego, z wyjątkiem przypadku, o którym mowa w art. 38 ust. 2, oraz gdy odmowa dotyczy wykonania polecenia służbowego, które nie pozostaje w związku z pełnieniem służby,
2) zaniechanie wykonania czynności służbowej albo wykonanie jej w sposób nieprawidłowy,
3) niedopełnienie obowiązków służbowych albo przekroczenie uprawnień określonych w przepisach prawa,
4) wprowadzenie w błąd przełożonego lub innego funkcjonariusza, jeżeli spowodowało to lub mogło spowodować szkodę dla służby, funkcjonariusza lub innej osoby,
5) postępowanie przełożonego w sposób przyczyniający się do rozluźnienia dyscypliny służbowej w podległej jednostce organizacyjnej lub komórce organizacyjnej,
6) stawienie się do służby w stanie po użyciu alkoholu lub podobnie działającego środka odurzającego oraz spożywanie alkoholu lub podobnie działającego środka w czasie służby albo w obiektach lub na terenach zajmowanych przez SKW albo SWW,
7) utrata służbowej broni palnej, amunicji lub legitymacji służbowej, a także materiału zawierającego informacje niejawne,
8) utrata przedmiotu stanowiącego wyposażenie służbowe, którego wykorzystanie przez osoby nieuprawnione wyrządziło szkodę obywatelowi lub stworzyło zagrożenie dla porządku publicznego lub bezpieczeństwa powszechnego,
9) nadużycie zajmowanego stanowiska lub służby dla osiągnięcia korzyści majątkowej lub osobistej,
10) samowolne oddalenie się funkcjonariusza z rejonu zakwaterowania, jeżeli pełni służbę w systemie skoszarowanym, a także nieusprawiedliwione opuszczenie lub niestawienie się w miejscu pełnienia służby,
11) porzucenie służby.

Zamknięty lub otwarty katalog przewinień dyscyplinarnych oznacza, że (w przypadku AW i CBA) jeśli czyn zarzucony funkcjonariuszowi nie mieści się w katalogu określonym w § 4 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 sierpnia 2003 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu* albo art. 107 ust. 2 uoCBA, to wówczas funkcjonariusz nie może być pociągnięty do odpowiedzialności dyscyplinarnej. Z kolei funkcjionariusze ABW, SKW i SWW mogą być pociągnięci do odpowiedzialności dyscyplinarnej nie tylko za czyny określone w § 8 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* albo art. 106 ust. 2 uoSKWoSWW, ale też za każdy czyn, który narusza dyscyplinę służbową. W tym wypadku należy przyjąć, że katalog określony w powołanych przepisach wyróżnia dobra, które mogą być naruszone na skutek zachowania funkcjonariusza. T. Kuczyński uważa, że w takim wypadku strona przedmiotowa odpowiedzialności dyscyplinarnej

obejmuje różne zachowania, które, najogólniej rzecz ujmując, mogą polegać na: 1) naruszeniu obowiązków służbowych sensu stricto, określanych jako naruszenie dyscypliny służbowej, 2) uchybieniu godności służby (etyki zawodowej), 3) popełnieniu przestępstwa lub wykroczenia[13]. Tak więc przewinieniem dyscyplinarnym będzie nie tylko czyn wymieniony w § 8 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* albo w art. 106 ust. 2 uoSKWoSWW, lecz także taki, który narusza istotę stosunku służbowego, jaką jest mająca wyjątkowy charakter dyspozycyjność, obowiązek podporządkowania czy zasady etyki zawodowej albo też taki postępek, który jest przestępstwem lub wykroczeniem.

W orzeczeniach sądów administracyjnych dotyczących postępowań dyscyplinarnych w służbach specjalnych przewinieniem, które najczęściej jest zarzucane funkcjonariuszom, jest odmowa wykonania lub niewykonanie polecenia przełożonego. Jak zauważył WSA w Warszawie w wyroku z 4 grudnia 2012 r., sygn. akt II SA/Wa 1441/07[14], w sprawie dotyczącej odpowiedzialności dyscyplinarnej funkcjonariusza ABW, jeżeli polecenie służbowe pozostaje w związku ze służbą, to powinno być wykonane bezwzględnie, a obwiniony nie może zasłaniać się argumentem, że w jego przekonaniu forma polecenia była niewłaściwa. Z kolei w wyroku z 27 kwietnia 2010 r., sygn. akt II SA/Wa 239/10, wydanym również w sprawie dotyczącej funkcjonariusza ABW, podkreślono, że charakter podobny do poleceń mają regulacje wewnętrzne, które są opublikowane w dzienniku urzędowym służby specjalnej, a zatem im również powinien się podporządkować funkcjonariusz. Sąd przyjął tutaj, że opublikowanie aktu wewnętrznego w „Dzienniku Urzędowym ABW" oznacza, że jego *postanowienia były wiążące dla skarżącego w sposób przyjęty w danej służbie. Skoro więc przyjętą zasadą jest publikowanie tego rodzaju pism okólnych w Dzienniku Urzędowym ABW, to od chwili dokonania takiej publikacji (...), skarżącego wiązały wszystkie postanowienia w nim zawarte*[15], tak więc obwiniony funkcjonariusz nie może zasłaniać się nieznajomością takiego aktu prawnego jako podstawą do umorzenia postępowania. W przypadku, gdy akt wewnętrzny nie był opublikowany we właściwym dzienniku urzędowym, to, jak wskazano w wyroku WSA w Warszawie z 17 grudnia 2008 r., sygn. akt II SA/Wa 1081/08[16], wydanym w sprawie dotyczącej funkcjonariusza SKW, obwinionemu należy udowodnić, że istotnie zapoznał się z jego treścią. W przypadku braku w aktach personalnych obwinionego aktu wewnętrznego z adnotacją, że skarżący istotnie zapoznał się z treścią aktu, nie można mu skutecznie postawić zarzutu niewykonania polecenia służbowego. Należy również zauważyć, że dla ustalenia czynu ważne jest określenie, czy do obowiązków obwinionego należało wykonanie czynności, którego brak jest mu zarzucany. Wskazał na to NSA w wyroku z 2 września 2010 r., sygn. akt I OSK 24/10[17], uznając, że nie można skutecznie postawić funkcjonariuszowi ABW zarzutu

[13] T. Kuczyński, *Odpowiedzialność porządkowa i dyscyplinarna*, w: *System prawa administracyjnego. Stosunek służbowy,* t. 11, R. Hauser, Z. Niewiadomski, A. Wróbel (red.) Warszawa 2011, C.H. Beck, s. 450.

[14] Niepublikowany.

[15] Opublikowany w CBOSA.

[16] Niepublikowany.

[17] Niepublikowany.

niewykonania obowiązku służbowego polegającego na niezarejestrowaniu dokumentu w sytuacji, gdy organy nie ustaliły, czy taki obowiązek na obwinionym spoczywał.

Warto również wskazać na wyrok NSA z 18 lutego 2011 r., sygn. akt I OSK 1473/10[18], w którym wskazano, że do obowiązków funkcjonariusza służby specjalnej należy stałe bycie w kontakcie z przełożonymi, co oznacza, że jest on zobowiązany do odbierania od nich telefonów nawet w trakcie urlopu.

Przypadki, w których przeciwko funkcjonariuszom może być wszczęte postępowanie dyscyplinarne za czyny niebędące przewinieniami dyscyplinarnymi są dwojakiego rodzaju: popełnienie czynu karalnego lub niewykonanie prawnego obowiązku. Postępowanie dyscyplinarne wobec funkcjonariuszy wszystkich służb może być wszczęte wtedy, gdy popełnią oni przestępstwo lub wykroczenie. Ponadto w przypadku osób pełniących służbę w ABW, AW oraz w wojskowych służbach specjalnych może być wszczęte postępowanie dyscyplinarne, jeżeli inne organy, spoza służb, nałożyły na nie karę pieniężną, np. za niewłaściwe zachowanie na rozprawie administracyjnej – art. 96 kpa – lub grzywnę w celu przymuszenia, np. w celu wykonania egzekucji niepieniężnej – art. 119 § 1 *Ustawy z dnia 17 czerwca 1966 r. o postępowaniu egzekucyjnym w administracji*[19]. W sytuacji popełnienia takiego czynu właściwy organ z urzędu zawiadamia przełożonego dyscyplinarnego, który powinien podjąć czynności procesowe.

W postępowaniu dyscyplinarnym zasadnicze znaczenie ma prawidłowość zarzutów stawianych obwinionemu. Jak wskazano w wyroku WSA w Warszawie z 4 kwietnia 2006 r., sygn. akt II SA/Wa 179/06, dotyczącym funkcjonariusza ABW, niedopuszczalne jest wydanie decyzji o ukaraniu funkcjonariusza, która *nie pozwala na ustalenie, czy, kiedy i w jakich okolicznościach zostały popełnione czyny zarzucone skarżącemu. Brak szczegółowego opisu zarzucanych mu czynów* (podobnie: wyrok WSA w Warszawie z 22 września 2010 r., sygn. akt II SA/ Wa 435/10). Opis czynu powinien być dokładny. W sytuacji, w której czyn zarzucany funkcjonariuszowi jest opisany w sposób lakoniczny i ogólny, ocena materiału dowodowego zebranego w toku postępowania dyscyplinarnego nie jest możliwa, ponieważ nie bardzo wiadomo, jakiego przewinienia dotyczy postępowanie. Taka sytuacja niewątpliwie pogarsza pozycję procesową samego obwinionego, który nie bardzo wie, przed jakimi zarzutami powinien się bronić.

Przedmiotowej materii dotyczy również wyrok NSA z 16 grudnia 2005 r., sygn. akt I OSK 499/05, dotyczący funkcjonariusza ABW, w którym podkreślono, że opis czynu powinien szczególnie wskazywać na datę jego popełnienia, gdyż wymóg ustalenia *czasu popełnienia czynu i zamieszczenie tego w decyzji jest istotny ze względu na wprowadzone w art. 147 ustawy z 24 maja 2002 o ABW i AW instytucje przedawnienia ścigania i przedawnienia karalności*[20]. Wskazanie w opisie przewinienia dokładnej daty popełnienia przewinienia dyscyplinarnego ma duże znaczenie dla określenia prawidłowości toczącego się postępowania, ponieważ powinno być ono umorzone, jeżeli do jego wszczęcia lub ukarania obwinionego upłynął termin przedawnienia.

[18] Opublikowany w CBOSA.

[19] Dz.U. z 2005 r. Nr 229, poz. 1954 ze zm.

[20] Opublikowany w CBOSA. Podobnie wyrok NSA z 24 maja 2007 r., sygn. akt I OSK 1094/06, opublikowany w CBOSA i wyrok NSA z 2 września 2010 r., sygn. akt I OSK 24/10, niepublikowany.

3. Tryb postępowania dyscyplinarnego

Przebieg postępowania dyscyplinarnego w służbach specjalnych również został uregulowany w sposób niejednolity. Dotyczy to zarówno czynności w postępowaniu, jak i sposobu uregulowania. W ABW, AW i wojskowych służbach specjalnych ustawy pragmatyczne lakonicznie odnoszą się do czynności postępowania dyscyplinarnego. Czynności postępowania, w tym także prawa i obowiązki obwinionego, zostały natomiast szczegółowo uregulowane w rozporządzeniach wykonawczych. Inaczej określono przepisy o postępowaniu dyscyplinarnym w CBA. W przypadku tej służby całość czynności postępowania dyscyplinarnego została uregulowana w ustawie pragmatycznej, a *Rozporządzenie Prezesa Rady Ministrów z dnia 6 listopada 2006 r. w sprawie szczegółowego trybu wykonywania czynności związanych z postępowaniem dyscyplinarnym w stosunku do funkcjonariuszy Centralnego Biura Antykorupcyjnego* zawiera jedynie rozstrzygnięcia dotyczące formy dokumentów tworzonych w trakcie postępowania.

Postępowanie dyscyplinarne we wszystkich służbach specjalnych ma charakter inkwizycyjny, w którym dominującą rolę odgrywa przełożony dyscyplinarny. Przełożonym dyscyplinarnym dla wszystkich funkcjonariuszy jest szef danej służby specjalnej. Kierownik jednostki organizacyjnej służby jest natomiast przełożonym dyscyplinarnym w stosunku do podległych mu funkcjonariuszy. Przełożony dyscyplinarny decyduje o wszczęciu postępowania, ocenia zebrany przez rzecznika dyscyplinarnego materiał dowodowy oraz wymierza karę dyscyplinarną. Przełożony dyscyplinarny może, na podstawie art. 268a *Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego*[21], dalej kpa, upoważnić innego funkcjonariusza do dokonywania w jego imieniu czynności w toku postępowania, przy czym upoważnienie to nie musi być imienne, ale tylko wtedy, gdy *w danej jednostce organizacyjnej występowało tylko jedno takie stanowisko, co niewątpliwie pozwalało na zidentyfikowanie upoważnionego funkcjonariusza* (wyrok NSA z 10 stycznia 2012 r., sygn. akt I OSK 1563/11[22]). Tak więc upoważnienie wydane w trybie art. 268a kpa, jeśli identyfikuje upoważnionego przez podanie jego stanowiska, ale takich stanowisk w jednostce organizacyjnej jest więcej – jest nieprawidłowe, ponieważ nie określa się kogo dokładnie upoważniono do wydawania orzeczeń w toku postępowania. Czynności dowodowe przeprowadza bezpośrednio rzecznik dyscyplinarny będący wyspecjalizowanym organem, którego zadaniem jest prowadzenie postępowania wyjaśniającego, zebranie dowodów w toku postępowania, postawienie zarzutów obwinionemu oraz przedstawienie wyników postępowania właściwemu przełożonemu. Rzecznicy są powoływani przez szefa służby w jednostkach organizacyjnych lub, jak to określono w § 14 *Rozporządzenia Prezesa Rady Ministrów w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego,* w specjalnym zespole rzeczników poległym jednostce organizacyjnej ABW zajmującej się sprawami kadrowymi. Rzecznicy w toku postępowania są niezależni, a ich niezależność jest chroniona przez wyznaczenie okresu, na który są powoływani – w CBA na cztery lata, w pozostałych służbach specjalnych na dwa lata. Przepisy pragmatyczne w służbach specjalnych w większości nie określają przesłanek, jakie musi spełniać funkcjonariusz powołany na stanowisko rzecznika. Wydaje się to błędem, gdyż

[21] Dz.U. z 2000 r. Nr 98, poz. 1071 ze zm.

[22] Opublikowany w CBOSA.

charakter spraw dyscyplinarnych powoduje, że tego typu postępowania powinny być prowadzone przez doświadczonych funkcjonariuszy, dysponujących szeroką wiedzą z zakresu funkcjonowania służby i znajomości prawa. Wyjątkiem jest tu ABW, gdzie w § 15 ust. 2 *Rozporządzenia Prezesa Rady Ministrów w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* wskazano, że rzecznik dyscyplinarny powinien spełniać łącznie cztery warunki: mieć stopień oficerski, charakteryzować się niekaralnością sądową i dyscyplinarną, posiadać pozytywną opinię służbową i nie zajmować stanowiska służbowego zastępcy lub doradcy szefa ABW, kierownika lub zastępcy kierownika jednostki organizacyjnej służby. Rzecznicy dyscyplinarni i przełożeni dyscyplinarni podlegają wyłączeniu z postępowania, gdy:

– sprawa bezpośrednio ich dotyczy,
– są małżonkami, krewnymi lub powinowatymi obwinionego lub osoby przez niego pokrzywdzonej w rozumieniu przepisów *Ustawy z dnia 6 czerwca 1997 r. Kodeks postępowania karnego*, dalej kpk[23],
– byli świadkami czynu,
– między nimi a obwinionym lub osobą pokrzywdzoną przez obwinionego zachodzi stosunek osobisty mogący wywołać wątpliwości co do ich obiektywizmu.

Przełożony może odwołać rzecznika dyscyplinarnego również wtedy, gdy utraci on przymioty pozwalające mu pełnić tę funkcję. Dotyczy to sytuacji, gdy rzecznik przestanie pełnić służbę lub zostanie ukarany dyscyplinarnie.

Stroną postępowania dyscyplinarnego jest obwiniony i jego obrońca. Obwinionym jest osoba, której postawiono zarzuty w postanowieniu o wszczęciu postępowania dyscyplinarnego. Ma on prawo do odmowy składania wyjaśnień, składania własnych wniosków dowodowych, przeglądania akt i sporządzania z nich odpisów (chyba, że ze względu na dobro postępowania rzecznik dyscyplinarny ograniczy to prawo) i składania środków procesowych zmierzających do wzruszenia wydanych w toku postępowania orzeczeń. Obrońcą w postępowaniu dyscyplinarnym może być inny funkcjonariusz, a także adwokat lub radca prawny. Zgodnie z art. 125 ust. 3 uoCBA, art. 129 ust. 3 uoSKWoSWW, § 22 *Rozporządzenia Prezesa Rady Ministrów w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* oraz § 23 *Rozporządzenia Prezesa Rady Ministrów w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu* obrońca jest ustanowiony przez obwinionego pisemnie, posiada te same co on uprawnienia, z wyjątkiem sytuacji, gdy obwiniony ograniczył je w pełnomocnictwie.

Postępowanie dyscyplinarne we wszystkich służbach specjalnych jest regulowane przez dwa akty prawne: przepisy pragmatyczne i przepisy kpk dotyczące wezwań, terminów, doręczeń i świadków, z wyłączeniem możliwości nakładania kar porządkowych oraz zatrzymywania i doprowadzania świadków.

Postępowanie dyscyplinarne jest wszczynane przez organ wtedy, gdy istnieje uzasadnione przypuszczenie, że funkcjonariusz popełnił przewinienie. W takich sytuacjach organ wszczyna postępowanie z inicjatywy własnej, inicjatywy przełożonego funkcjonariusza albo też inicjatywy sądu albo prokuratora prowadzącego postępowanie w danej sprawie. W CBA i wojskowych służbach specjalnych przewidziano fakultatywną

[23] Dz.U. Nr 89, poz. 555 ze zm.

możliwość wszczęcia postępowania na wniosek osoby pokrzywdzonej przewinieniem funkcjonariusza.

Wszczęcie postępowania może być poprzedzone czynnościami wyjaśniającymi. Takie postępowanie quazi-wyjaśniające wszczyna się zgodnie z art. 120 ust. 3 uoCBA, art. 124 ust. 3 uoSKWoSWW, § 11 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* oraz § 11 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 sierpnia 2003 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu*, gdy otrzymano informację o czynie funkcjonariusza, ale jednocześnie otrzymana wiadomość budzi wątpliwości, w szczególności co do popełnienia tego czynu lub jego kwalifikacji prawnej albo co do osoby sprawcy. Podejmowane wówczas czynności służą wyjaśnieniu wątpliwości związanych z otrzymanymi informacjami na temat czynu. Postępowanie to nie jest sformalizowane. Prowadzi je rzecznik dyscyplinarny, jego działanie *sprowadza się do sprawdzenia określonych faktów i sporządzenia notatek urzędowych*[24]. W toku postępowania nie prowadzi się zatem czynności dowodowych, choć po wszczęciu postępowania rzecznik może dołączyć zebrany materiał do materiału dowodowego. Przepisy dotyczące postępowania wyjaśniającego w większości określają, że czynności te powinny się zakończyć w terminie trzydziestu dni. W Agencji Wywiadu termin ten określono na czternaście dni, ma on jednak ma charakter instrukcyjny, a więc jego przekroczenie nie powinno mieć wpływu na decyzję o wszczęciu postępowania. Jedynym ograniczeniem są tu terminy przedawnienia postępowania.

Wszczynając postępowanie dyscyplinarne przełożeni dyscyplinarni powinni mieć na względzie treść art. 147 uoABWoAW, art. 111 UoCBA i art. 118 uoSKWoSWW. Przepisy te wprowadzają terminy „przedawnienia ścigania" i „przedawnienia karalności czynu". Nie wszczyna się postępowania dyscyplinarnego po upływie 90 dni od dnia otrzymania przez przełożonego wiadomości o popełnieniu przewinienia lub naruszeniu dyscypliny służbowej. Przedawnienie karalności natomiast następuje po upływie roku od dnia popełnienia czynu. W sytuacji, gdy popełniony czyn zawiera w sobie znamiona przestępstwa lub wykroczenia, przedawnienie deliktu dyscyplinarnego nie może nastąpić przed upływem terminu przedawnienia tego przestępstwa lub wykroczenia. Terminy w postępowaniu dyscyplinarnym mają znaczenie gwarancyjne, dlatego też nie mogą być one wydłużane ani tym bardziej ignorowane. Podkreślono to w wyroku NSA z 24 maja 2007 r., sygn. akt I OSK 1094/06, w którym stwierdzono, że *wyjaśnienie kwestii daty powiadomienia właściwego przełożonego o popełnieniu przez skarżącego przewinienia ma zasadnicze znaczenie dla oceny możliwości wszczęcia postępowania dyscyplinarnego. Kwestia ta powinna być jednoznacznie wyjaśniona i udokumentowana zanim doszło do wszczęcia postępowania*[25]. Sąd uznał tu, że już na etapie wszczęcia postępowania przełożony dyscyplinarny powinien dysponować pewną wiedzą o tym, kiedy został poinformowany o popełnionym przewinieniu, a co za tym idzie, czy już w dacie wszczęcia nie nastąpiła okoliczność, która wyklucza dalsze prowadzenie postępowania. Upływ terminu przedawnienia oraz śmierć funkcjonariusza, zapadnięcie prawomocnego orzeczenia dyscyplinarnego lub toczące się postępowanie dyscyplinarne w tej samej sprawie oraz brak przesłanek wskazujących, że zostało

[24] S. Maj, *Postępowanie dyscyplinarne w służbach mundurowych,* Warszawa 2008*,* LexisNexis, s. 59.

[25] Opublikowany w CBOSA.

popełnione przewinienie dyscyplinarne są okolicznościami, na których podstawie przełożony dyscyplinarny wydaje postanowienie o odmowie wszczęcia postępowania, a w przypadku, gdy postępowanie się toczy – orzeczenie o jego umorzeniu. Należy podkreślić, że okoliczność, iż dana osoba nie pełni już służby w danej formacji, nie jest przesłanką umorzenia postępowania, co w sprawie funkcjonariusza SKW podkreślił WSA w Warszawie w wyroku z 11 marca 2011 r., sygn. akt II SA/Wa 1347/10[26].

Wszczęcie postępowania następuje w drodze postanowienia wydanego przez przełożonego dyscyplinarnego. Postanowienie to nie podlega zaskarżeniu. Treść postanowienia jest dokładnie określona w art. 120 ust. 5 uoCBA, art. 124 ust. 5 uoSKWoSWW, § 13 ust. 3 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* oraz § 13 ust. 3 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 sierpnia 2003 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu*. W postanowieniu powinno wskazać się osobę, przeciwko której toczy się postępowanie, określić zarzucany jej czyn oraz wskazać jego kwalifikację prawną oraz przedstawić uzasadnienie.

Czas trwania postępowania jest określony w różny sposób. W ABW i AW obejmuje on 30 dni, przy czym przełożony dyscyplinarny może w drodze postanowienia przedłużyć postępowanie do trzech miesięcy. Jest to maksymalny okres, w którym może trwać postępowanie w tych służbach. W CBA i wojskowych służbach specjalnych czynności dowodowe powinny być zakończone w terminie miesiąca od dnia wszczęcia postępowania. Okres ten może być przedłużony o dalsze 30 dni przez przełożonego dyscyplinarnego. Po tym okresie przedłużenie czynności postępowania na dalszy czas oznaczony następuje na podstawie postanowienia szefa danej służby.

Zbierając materiał dowodowy rzecznik dyscyplinarny ma obowiązek badać okoliczności przemawiające zarówno na korzyść jak i niekorzyść obwinionego. Obwiniony nie jest uprawniony do udziału w czynnościach dowodowych, a jego uprawnienia w postępowaniu dyscyplinarnym są we wszystkich ustawach pragmatycznych ograniczone do: odmowy składania wyjaśnień, pisemnego zgłaszania wniosków dowodowych, ustanowienia obrońcy, przeglądania akt postępowania dyscyplinarnego oraz sporządzania z nich notatek. Podkreślił to WSA w Warszawie w wyroku z 29 czerwca 2012 r., sygn. akt II SA/Wa 674/12 wskazując, że *postępowanie dyscyplinarne funkcjonariuszy ABW nie jest ukształtowane na wzór postępowania sądowego, a obwiniony nie ma zapewnionego bezpośredniego udziału we wszystkich czynnościach tego postępowania, w tym przesłuchaniu świadków*[27], a zatem w postępowaniu dyscyplinarnym obwiniony ma inicjatywę dowodową, ale nie ma prawa do uczestniczenia w czynnościach postępowania dowodowego prowadzonych przez rzecznika. Rzecznik nie jest związany wnioskiem dowodowym obwinionego. Dowód zgłaszany przez obwinionego jest przeprowadzony jedynie wówczas, gdy ma on istotne znaczenie dla sprawy. Nie przeprowadza się dowodów, które są sprzeczne z prawem, jeśli okoliczność, która ma być udowodniona, została już ustalona lub nie jest istotna dla sprawy lub gdy przeprowadzenie dowodu nie jest istotne dla sprawy. Wniosek dowodowy ulega oddaleniu postanowieniem, na które nie przysługuje zażalenie.

[26] Niepublikowany.

[27] Opublikowany w CBOSA.

Postępowanie dyscyplinarne zawiesza się z powodu długotrwałej przeszkody uniemożliwiającej prowadzenie postępowania lub jeżeli wynik postępowania dyscyplinarnego zależy od innego toczącego się postępowania karnego.

W sytuacji, gdy rzecznik dyscyplinarny zbierze materiał dowodowy, który w jego przekonaniu wystarczy do rozstrzygnięcia sprawy, to zapoznaje obwinionego i jego obrońcę z aktami postępowania dyscyplinarnego. Z czynności zapoznania się z aktami postępowania dyscyplinarnego jest sporządzany protokół. Odmowa zapoznania się z aktami postępowania lub złożenia podpisu stwierdzającego tę okoliczność nie wstrzymuje postępowania. Obwiniony ma prawo w terminie 3 dni od dnia zapoznania się z aktami postępowania dyscyplinarnego zgłosić wniosek o ich uzupełnienie. Na wydane przez rzecznika dyscyplinarnego postanowienie o odmowie uzupełnienia akt postępowania dyscyplinarnego obwinionemu przysługuje prawo złożenia zażalenia. Po uzupełnieniu materiału dowodowego obwiniony ponownie ma prawo do zapoznania się z aktami postępowania i ponownie może złożyć wniosek o ich uzupełnienie, ale tylko w zakresie wynikającym z przeprowadzonych czynności dowodowych uzupełniających akta tego postępowania. Po czynnościach związanych z zapoznaniem obwinionego z aktami postępowania rzecznik sporządza sprawozdanie, w którym określa sposoby zakończenia postępowania.

Przełożony dyscyplinarny po przedstawieniu mu sprawozdania wydaje orzeczenie dyscyplinarne. Orzeczeniem tym można uniewinnić obwinionego, umorzyć postępowanie w sprawie lub uznać go winnym, ale odstąpić od ukarania, lub też ukarać obwinionego. Wydanie orzeczenia dyscyplinarnego kończy postępowanie wyjaśniające. Orzeczenie dyscyplinarne powinno być sporządzone w wymaganej przez przepisy pragmatyczne formie i zawierać uzasadnienie, które przedstawia w sposób niebudzący wątpliwości dowody potwierdzające rozstrzygnięcie. Uzasadnienie ogólnikowe, *nie poparte dogłębną oceną i analizą materiału dowodowego, co wywołuje wątpliwości, że organ w sposób wystarczający udokumentował fakt popełnienia przez skarżącego zarzucanego mu czynu*[28], nie może być uznane za prawidłowe, świadczy bowiem o tym, że zebrany materiał ma luki lub w ogóle nie udowadnia przyjętego rozstrzygnięcia. W wyroku WSA w Warszawie z 8 lutego 2011 r., sygn. akt II SA/Wa 1665/10 wskazano na wzór prawidłowego uzasadnienia, które *musi wiązać się z przyjętym w osnowie rozstrzygnięciem. Powinno zatem przytaczać i wyjaśniać przepisy prawa mające zastosowanie (uzasadnienie prawne), a także omawiać fakty i dowody odnoszące się do przypisywanego funkcjonariuszowi czynu oraz wymierzonej kary (uzasadnienie faktyczne). Uzasadnienie nie może pozostać w sprzeczności z sentencją orzeczenia*[29]. Uzasadnienie orzeczenia dyscyplinarnego powinno zawierać dwie części: prawną, będącą wykładnią zastosowanych w postępowaniu przepisów, oraz faktyczną – opisującą fakty, które zostały udowodnione w toku postępowania. Uzasadnienie powinno odpowiadać treści rozstrzygnięcia, a więc niedopuszczalne jest, aby treść rozstrzygnięcia orzeczenia dyscyplinarnego nie odpowiadała treści uzasadnienia.

Zgodnie z art. 130 ust. 1 uoCBA, art. 134 ust. 1 uoSKWoSWW, § 32 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy*

[28] Wyrok WSA w Warszawie z 28 września 2007 r., sygn. akt II SA/Wa 524/07, niepublikowany, podobnie wyrok WSA w Warszawie z 27 lutego 2008 r., sygn. akt II SA/Wa 1817/07, opublikowany w CBOSA oraz wyrok WSA w Warszawie z 5 stycznia 2011 r., sygn. akt II SA/Wa 1747/10, opublikowany w CBOSA.

[29] Opublikowany w CBOSA.

Agencji Bezpieczeństwa Wewnętrznego oraz § 32 ust. 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 sierpnia 2003 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu* od orzeczenia dyscyplinarnego wydanego w pierwszej instancji obwiniony lub jego obrońca może wnieść pisemne odwołanie w terminie siedmiu dni od dnia doręczenia orzeczenia. Postępowanie odwoławcze toczy się przed właściwym organem drugiej instancji. Odwołanie składa się do organu pierwszej instancji, który ma obowiązek w terminie siedmiu dni od dnia doręczenia odwołania przesłać akta sprawy wraz z odwołaniem do organu drugiej instancji. Przepisy o postępowaniu dyscyplinarnym nie przewidują możliwości zmiany wydanego orzeczenia przez organ pierwszej instancji. Organ drugiej instancji ma ograniczone uprawnienia do przeprowadzenia odrębnego postępowania dowodowego. Dowody przeprowadza się jedynie wyjątkowo i mają one charakter uzupełniający. W CBA i wojskowych służbach specjalnych szef służby wydaje postanowienie o odmowie przyjęcia odwołania, jeżeli jest ono niedopuszczalne lub zostało złożone przez osobę nieuprawnioną. W tych samych służbach organ odwoławczy powołuje komisję złożoną z trzech funkcjonariuszy, której zadaniem jest ocena zgromadzonego w sprawie materiału dowodowego. W ramach swoich uprawnień komisja może wysłuchać rzecznika dyscyplinarnego, obwinionego lub jego obrońcę. Ze swoich prac przedstawia sprawozdanie, które organ odwoławczy powinien wziąć pod uwagę wydając orzeczenie, ale nie jest nim związany. Organ odwoławczy nie może orzekać na niekorzyść obwinionego. Przepisy o postępowaniu dyscyplinarnym wskazują, że organ odwoławczy może orzec jedynie o:

– utrzymaniu w mocy orzeczenia,
– zmianie orzeczenia w całości lub w części i w tym zakresie wymierza inną karę lub środek dyscyplinarny albo odstępuje od ukarania,
– uchyleniu orzeczenia w całości lub w części i w tym zakresie uniewinnia obwinionego albo umarza postępowanie dyscyplinarne.

Organ odwoławczy nie może wydać orzeczenia o innej sentencji niż to jest określone w przepisach, co podniósł WSA w Warszawie w wyroku z 11 maja 2010 r., sygn. akt II SA/Wa 1898/09[30] w sprawie dotyczącej funkcjonariuszy ABW. Sąd podkreślił, że wyjście poza dyspozycje przepisu statuującego rodzaje orzeczeń stanowi jego istotne naruszenie. Wydanie orzeczenia przez organ odwoławczy zamyka postępowanie odwoławcze. Orzeczenie dyscyplinarne staje się z tą chwilą ostateczne. Orzeczenie dyscyplinarne staje się także ostateczne, jeśli upłynie termin wniesienia odwołania od orzeczenia organu pierwszej instancji.

We wszystkich służbach specjalnych przepisy znają tylko jeden sposób wzruszenia prawomocnego orzeczenia dyscyplinarnego – poprzez wznowienie postępowania. Nie jest dopuszczalne stosowanie posiłkowo w tym zakresie przepisów kpa, dotyczących zmiany ostatecznej decyzji administracyjnej. W tym wypadku, jak podkreślono w wyroku WSA w Warszawie z 27 stycznia 2006 r., sygn. akt II SA/Wa 1780/05[31], przepisy dotyczące postępowania dyscyplinarnego wskazują, że w sprawach nieuregulowanych stosuje się rozwiązania zawarte w kpk, który nie przewiduje instytucji prawnej „stwierdzenia nieważności wyroku", wyłączone jest natomiast posiłkowe stosowanie przepisów procedury administracyjnej, a zatem funkcjonariusz, wobec którego wydano ostateczne orzeczenie dyscyplinarne, nie może żądać jego zmiany na podstawie art. 156

[30] Niepublikowany.

[31] Niepublikowany.

kpa. Warto w tym miejscu zauważyć, że orzecznictwo sądów administracyjnych konsekwentnie wskazuje, iż byli funkcjonariusze służb specjalnych Polski Ludowej nie mogą żądać stwierdzenia nieważności decyzji dyscyplinarnych wydanych w stosunku do nich przed 1990 r. Podniósł to NSA w wyroku z 24 lutego 2009 r., sygn. akt I OSK 479/08. Zdaniem Sądu *nie ulega bowiem najmniejszej wątpliwości, że oba kwestionowane przez skarżącego akty nie zostały wydane w trybie postępowania administracyjnego regulowanego przepisami kpa. Należy bowiem pamiętać, że w dacie ich wydania, zarówno do spraw dyscyplinarnych (art. 3 § 2 pkt 3 kpa), jak i do postępowania w sprawach wynikających z podległości służbowej pracowników organów (art. 3 § 3 pkt 2 kpa) przepisy tego kodeksu nie miały zastosowania, bo nie było przepisu szczególnego, który by stanowił inaczej. W rozpoznawanej sprawie oznacza to, że nie jest możliwe badanie ich legalności w trybie stwierdzenia nieważności dotyczącym decyzji administracyjnych, ponieważ akty te w dacie ich wydania nie były decyzjami w rozumieniu kodeksu postępowania administracyjnego*[32], a więc sprawy dyscyplinarne byłych funkcjonariuszy Służby Bezpieczeństwa nie były w dniu ich wydania decyzjami administracyjnymi, wobec czego nie można ich wzruszyć stosując przepisy kpa.

Postępowanie dyscyplinarne może być wznowione z urzędu lub na wniosek ukaranego lub obwinionego funkcjonariusza lub, w przypadku jego śmierci, na wniosek członka jego rodziny uprawnionego do otrzymania renty rodzinnej. Termin złożenia wniosku o wznowienie jest ograniczony dwoma warunkami. Po pierwsze, wnosi się go w terminie 30 dni od dnia, w którym ukarany dowiedział się o okoliczności stanowiącej podstawę do wznowienia, a po drugie, postępowania dyscyplinarnego nie wznawia się po upływie 5 lat od dnia uprawomocnienia się orzeczenia. Określone przedziały czasowe są terminami materialnoprawnymi, a z ich upływem następuje wygaśnięcie kompetencji organu do wznowienia postępowania dyscyplinarnego[33]. W wyroku z 28 sierpnia 2007 r., sygn. akt II SA/Wa 832/07[34] podkreślono, że w przypadku, kiedy funkcjonariusz wywodzi wniosek o wznowienie postępowania z treści ogłoszonego orzeczenia sądu, to w sytuacji, gdy był on obecny w trakcie ogłoszenia orzeczenia, termin na złożenie wniosku o wznowienie postępowania rozpoczyna się w dniu ogłoszenia.

Postępowanie dyscyplinarne zakończone prawomocnym orzeczeniem wznawia się, jeżeli:

- dowody, na podstawie których ustalono istotne dla sprawy okoliczności, okazały się fałszywe,
- zostały ujawnione istotne dla sprawy okoliczności, które nie były znane w toku postępowania dyscyplinarnego,
- orzeczenie wydano z naruszeniem obowiązujących przepisów, jeżeli mogło to mieć wpływ na treść orzeczenia,
- orzeczenie zostało wydane na podstawie innego rozstrzygnięcia, które zostało następnie uchylone lub zmienione,
- w wyniku orzeczenia Trybunału Konstytucyjnego stracił moc lub uległ zmianie przepis prawny będący podstawą wydania orzeczenia dyscyplinarnego (tylko w CBA, SKW i SWW).

---

[32] Niepublikowany. Podobnie wyrok NSA z 4 listopada 2005 r., sygn. akt I OSK 192/05, opublikowany w CBOSA.

[33] Takie stanowisko zajął WSA w Warszawie w wyroku z 30 listopada 2007 r., sygn. akt II SA/Wa 1461/07, niepublikowany.

[34] Opublikowany w CBOSA.

Na tle przesłanek wznowienia pojawił się problem, czy umorzenie postępowania karnego lub uniewinnienie funkcjonariusza jest przesłanką wznowienia postępowania i uchylenia orzeczenia dyscyplinarnego. W przypadku funkcjonariuszy ABW sądy administracyjne stoją konsekwentnie na stanowisku, że samo uniewinnienie czy umorzenie postępowania karnego przeciwko ukaranemu nie stanowi samoistnej przesłanki wznowienia postępowania. Podkreśla się bowiem dwoistość odpowiedzialności karnej i dyscyplinarnej. Sądy wskazują tu, że odpowiedzialność dyscyplinarna ma szerszy zakres niż odpowiedzialność karna, a zatem czyn, który w świetle prawa karnego nie jest przestępstwem lub wykroczeniem może być uznany za przewinienie dyscyplinarne[35].

Postępowanie wznowieniowe nie polega na ponownym przeprowadzeniu postępowania dyscyplinarnego, ponieważ rozpatrywana jest jedynie problematyka istnienia podstaw do wznowienia postępowania, a nie kwestia odpowiedzialności dyscyplinarnej, a zatem nie mamy tu do czynienia ze szczególną, kolejną instancją w postępowaniu dyscyplinarnym, ale z postępowaniem ograniczonym jedynie do ustalenia tego, czy rzeczywiście istnieją podstawy do wznowienia postępowania. Po zakończeniu postępowania, stosownie do poczynionych ustaleń, wydaje się jedno z trzech rodzajów orzeczeń:

– uchylające dotychczasowe orzeczenie i stwierdzające uniewinnienie ukaranego lub umorzenie postępowania dyscyplinarnego,
– zmieniające dotychczasowe orzeczenie i wymierzające inną karę dyscyplinarną,
– odmawiające uchylenia dotychczasowego orzeczenia.

4. Katalog kar

Kary dyscyplinarne są odpłatą za popełnione przewinienie dyscyplinarne. Orzeczenie kary dyscyplinarnej oznacza, że dokonano całościowej oceny czynu obwinionego. Ocena taka powinna prowadzić do tego, aby wymierzona kara była adekwatna do wagi czynu, ale także uwzględniała inne uwarunkowania związane z osobą obwinionego i okolicznościami popełnienia czynu.

W art. 119 ust. 1–3 uoCBA, art. 117 ust. 1–3 uoSKWoSWW, § 28 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 grudnia 2004 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego* oraz § 29 ust. 1 i 2 *Rozporządzenia Prezesa Rady Ministrów z dnia 20 sierpnia 2003 r. w sprawie udzielania wyróżnień i przeprowadzania postępowań dyscyplinarnych wobec funkcjonariuszy Agencji Wywiadu* określono zasady wymiaru kary, w tym przede wszystkim katalog okoliczności wpływających na jej zaostrzenie lub złagodzenie. Okoliczności te, jak podkreślił NSA w wyroku z 29 lutego 2012 r., sygn. akt I OSK 995/11, powinny być zawsze uwzględnione przy określaniu wymierzanej obwinionemu kary, błędne jest zatem działanie organu polegające na tym, że *nie wykazał on faktu rozważenia i oceny elementów zawartych w tym przepisie. Wymiar kary powinien uwzględniać dyrektywy jej nakładania oraz okoliczności przemawiające tak na korzyść jak i niekorzyść obwinionego*[36]. Uzasadnienie orzeczenia dyscyplinarnego nie może zatem odnosić się tylko do okoliczności związanych z czynem obwinionego, ale powinno także zawierać obszerne omówienie przesłanek wymiaru kary.

[35] Por. wyroki NSA z 5 maja 2011 r. sygn. akt I OSK 53/11 i I OSK 165/11 opublikowane w CBOSA.

[36] Niepublikowany.

Przesłanki wymiaru kary dyscyplinarnej możemy podzielić na trzy grupy:
– dotyczące okoliczności popełnienia samego czynu – rodzaj i waga czynu, okoliczności jego popełnienia, podjęcie przez funkcjonariusza działań w celu zmniejszenia jego skutków, dobrowolne ujawnienie popełnienia czynu przed wszczęciem postępowania dyscyplinarnego, działanie w obecności podwładnego lub wspólnie z nim albo na jego szkodę;
– cech obwinionego – rodzaj winy, popełnienie czynu w okresie, gdy nie została zatarta kara za poprzednio popełnione przewinienie dyscyplinarne, działanie z motywacji zasługującej na szczególne potępienie, działanie w stanie po spożyciu alkoholu lub zażyciu środka odurzającego,
– wpływu na wykonywanie zadań przez daną służbę – poważne skutki czynu wpływające na wykonywanie zadań przez służbę.

Katalog kar dyscyplinarnych jest w służbach specjalnych niejednolity. Przepis art. 146 ust. 1 uoABWoAW i art. 109 ust. 1 uoSKWoSWW określają dziesięć kar dyscyplinarnych. Karą dyscyplinarną jest: upomnienie, nagana, surowa nagana, nagana z ostrzeżeniem, ostrzeżenie o niepełnej przydatności do służby na zajmowanym stanowisku, wyznaczenie na niższe stanowisko służbowe, obniżenie stopnia, pozbawienie stopnia oficerskiego, ostrzeżenie o niepełnej przydatności do służby, a także wydalenie ze służby. Z kolei art. 113 ust. 1 uoCBA przewiduje, że funkcjonariuszom CBA wymierza się tylko cztery kary: naganę, ostrzeżenie o niepełnej przydatności do służby na zajmowanym stanowisku, wyznaczenie na niższe stanowisko służbowe i wydalenie ze służby.

Ze względu na charakter popełnionego czynu i wynikające z niego skutki dla obwinionego kary dyscyplinarne można podzielić na trzy grupy:
• kary będące wytknięciem niewłaściwego postępowania. Takimi karami będą upomnienie, nagana, surowa nagana i nagana z ostrzeżeniem. Kary określają jak duże były uchybienia obwinionego w realizacji zadań wynikających ze stosunku służbowego;
• kary wskazujące, że czyn obwinionego pozbawia go przymiotów, które są potrzebne do pełnienia służby na określonym stanowisku służbowym. Zaliczyć do nich należy: ostrzeżenie o niepełnej przydatności do służby na zajmowanym stanowisku, wyznaczenie na niższe stanowisko służbowe, obniżenie stopnia, pozbawienie stopnia oficerskiego oraz ostrzeżenie o niepełnej przydatności do służby. Wymierzenie tego rodzaju kary wskazuje na to, że obwiniony nie potrafi unieść ciężarów służby wynikających z określonego stanowiska;
• kary rozwiązujące stosunek służbowy. Tego rodzaju kara jest tylko jedna – wydalenie ze służby. Wskazuje na to, że czyn obwinionego był tak poważny, iż pozbawił go wszelkich przymiotów, które wskazywałyby na to, że może on nadal być stroną stosunku służbowego.

Za popełnione przewinienie dyscyplinarne wymierza się tylko jedną karę dyscyplinarną. Jeżeli obwiniony popełnił więcej przewinień dyscyplinarnych, to wymierza mu się jedną karę dyscyplinarną za wszystkie przewinienia. Kara ta powinna być odpowiednio surowsza. Warto wskazać, że w przypadku funkcjonariuszy CBA przepis art. 113 ust. 2 uoCBA przewiduje możliwość wymierzenia im kary dodatkowej, którą jest czasowe pozbawienie premii.

Pragmatyki służbowe w służbach specjalnych przewidują, że po upływie określonego czasu kary dyscyplinarne ulegają zatarciu. Karę, która została zatarta uważa się za niebyłą, a więc nie wpływa ona na treść stosunku służbowego łączącego funkcjonariusza z daną służbą. Okres zatarcia zależy do rodzaju kary. Im poważniejsze było przewinienie,

a zatem dotkliwsza była kara, tym okres jej zatarcia jest dłuższy. W przypadku nienagannej służby okresy te mogą ulec skróceniu o połowę, a ponadto w nadzwyczajnych wypadkach, gdy obwiniony wykazał się męstwem i odwagą lub ma duże osiągnięcia w służbie, właściwy organ może znacznie wcześniej orzec o zatarciu kary.

5. Uwagi końcowe

Postępowanie dyscyplinarne w służbach mundurowych nie jest uregulowane w sposób jednolity, choć większość instytucji procesowych jest we wszystkich służbach podobna. Takie rozwiązanie ustawodawcy nie wydaje się racjonalne. Omawiane służby mundurowe mają zbliżone zadania, działają w podobny sposób i są podobnie zorganizowane. Stąd zaskakująca jest niekonsekwencja ustawodawcy, który nawet wtedy, gdy elementy stosunku służbowego dwóch służb są określone w jednej ustawie, wprowadza w tym zakresie różnice.

Absolutnie nie zasługuje na aprobatę sposób określenia w przepisach postępowania dyscyplinarnego. Funkcjonariusz służby specjalnej, mimo związania stosunkiem służbowym z daną formacją zmilitaryzowaną, nie traci statusu obywatela, do którego w pełni odnoszą się przepisy Konstytucji. Tymczasem w większości służb specjalnych tak ważne postępowanie decydujące o prawach funkcjonariusza, jakim jest postępowanie dyscyplinarne, jest określone w przepisach wykonawczych. Wyjątkiem są przepisy dotyczące funkcjonariuszy CBA. W tym przypadku postępowanie dyscyplinarne zostało w całości uregulowane w ustawie.

Orzeczenia wydane w toku postępowania dyscyplinarnego w służbach specjalnych podlegają kontroli sądów administracyjnych. Niewątpliwie sprzyja to praworządności. Orzecznictwo Wojewódzkiego Sądu Administracyjnego w Warszawie oraz Naczelnego Sądu Administracyjnego porządkuje i wyjaśnia treść przepisów dyscyplinarnych. Jednak konieczne wydaje się zniwelowanie różnic, które istnieją w służbach specjalnych dotyczących postępowań dyscyplinarnych. Należałoby zatem poważnie rozpatrzyć postawiony kilka lat temu postulat, aby stworzyć jeden akt prawny regulujący postępowanie dyscyplinarne w służbach mundurowych[37].

Abstrakt

Służby specjalne są wyspecjalizowanymi organami państwa powołanymi do zwalczania szczególnych zagrożeń dla funkcjonowania kraju. W odróżnieniu od innych formacji zmilitaryzowanych charakteryzują się one tym, że działają w sposób niejawny, a ich działalność obejmuje również czynności dokonywane poza terytorium Rzeczypospolitej Polskiej. Jednak mimo podobieństw w działalności służb specjalnych ustawodawca uregulował w odmienny sposób procedurę postępowania w sprawach dyscyplinarnych.

We wszystkich służbach specjalnych ustalono ogólną klauzulę odpowiedzialności dyscyplinarnej. Ustawy nie określają definicji przewinienia dyscyplinarnego. Przewinienie dyscyplinarne jest natomiast definiowane przez określenie w kolejnych przepisach katalogu czynów, za które funkcjonariusz może zostać ukarany. Jednak w tym wypadku ustawodawca sformułował w różny sposób katalog czynów, które są przewinieniami dyscyplinarnymi w służbach specjalnych. Mamy tutaj dwa rozwiązania:

[37] Por. S. Maj, *Postepowanie* ..., s. 406–407.

- przewinienia dyscyplinarne stanowią zamknięty katalog czynów (AW, CBA)
- wymienione przewinienia dyscyplinarne nie stanowią zamkniętego katalogu czynów, a podane w przepisach wyliczenie ma jedynie charakter przykładowy (ABW, wojskowe służby specjalne).

Postępowanie dyscyplinarne we wszystkich służbach specjalnych ma charakter inkwizycyjny, w którym dominującą rolę odgrywa przełożony dyscyplinarny. Przełożonym dyscyplinarnym dla wszystkich funkcjonariuszy jest szef danej służby specjalnej. Kierownik jednostki organizacyjnej służby jest natomiast przełożonym dyscyplinarnym w stosunku do podległych mu funkcjonariuszy. Przełożony dyscyplinarny decyduje o wszczęciu postępowania, ocenia zebrany przez rzecznika dyscyplinarnego materiał dowodowy oraz wymierza karę. Kary dyscyplinarne są natomiast odpłatą za popełnione przewinienie dyscyplinarne. Orzeczenie kary dyscyplinarnej oznacza, że dokonano całościowej oceny czynu obwinionego. Ocena taka powinna prowadzić do tego, aby wymierzona kara była adekwatna do wagi czynu, ale także uwzględniała inne uwarunkowania związane z osobą obwinionego i okolicznościami popełnienia czynu.

Abstract

Special services are specialized state bodies established to counteract specific threats to the state. Unlike military institutions, they typically operate covertly and perform actions outside the territory of the Republic of Poland. However, despite some similarities between the methods of operation of particular services, the law-makers have distinguished between disciplinary procedures in various services.

All services are subject to a general clause of disciplinary liability. The legal acts do not provide any definition of a disciplinary violation. The disciplinary violation can only be defined on the basis of all the acts specified in the provisions, for which an officer may be punished. However, the legal provisions stipulate various catalogues of disciplinary violations that officers of particular services may be held accountable for. There are two possibilities:

- disciplinary violations are contained in a closed list (AW, CBA);
- disciplinary violations are not contained in any closed list of acts, whereas those specified in legal provisions are only examples (ABW, military special services).

Disciplinary proceedings in all special services are of inquisitorial nature, where the key role is played by the disciplinary superior. The disciplinary superiors to all officers are heads of special services. Heads of organizational units within the service are disciplinary superiors to all officers that are subordinate to them. It is the disciplinary superior who decides on launching disciplinary proceedings, evaluates the materials gathered by disciplinary assistant and imposes punishment. Disciplinary punishment is retribution for a disciplinary violation. When disciplinary punishment is imposed, it means that the violation has been thoroughly investigated. The investigation should result in imposing punishment that matches the seriousness of the violation. It should also take into consideration other circumstances connected with the specific officer and the general circumstances of the violation.

III
RECENZJE

Sławomir Suchecki

Katarzyna Witkowska-Rozpara, *Przestępczość, środki masowego przekazu a polityka karna*[1]

Monografia zatytułowana *Przestępczość, środki masowego przekazu a polityka karna* autorstwa Katarzyny Witkowskiej-Rozpary, opublikowana przez wydawnictwo C.H. Beck, składa się z wprowadzenia oraz siedmiu rozdziałów, z których ostatni stanowi podsumowanie obejmujące uwagi i wnioski końcowe autorki. Rozważania ujęte w recenzowanej publikacji, zgodnie z deklaracją zawartą we wprowadzeniu, odzwierciedlają oraz pogłębiają tezy zawarte w jej rozprawie doktorskiej.

Wprowadzenie służy określeniu obszaru badawczego, którym zajęła się K. Witkowska-Rozpara. Analiza jego zakresu, dokonana na podstawie przedstawionej we wprowadzeniu systematyki, zmierza do ujęcia opisu obrazu przestępczości w dwóch systemach: demokratycznym i niedemokratycznym. Cel, zarówno rozważań dotyczących „przedpola" historycznego problemów ujętych w publikacji, jak i badań przeprowadzonych przez autorkę, jest jednak inny. K. Witkowska-Rozpara dąży, poprzez analizę zależności pomiędzy mediami, przestępczością i polityką karną, do uzyskania odpowiedzi na pytania dotyczące poziomu wpływu mediów na kształtowanie założeń polityki karnej, oddziałujących na nią czynników politycznych oraz rzetelności prezentowania przestępczości w środkach masowego przekazu.

W rozdziale I, zatytułowanym *Źródła wiedzy o przestępczości*, autorka dokonuje szczegółowej analizy pojęcia „przestępczość". Zgodnie z zawartą we wstępie rozdziału definicją „przestępczość" jest zjawiskiem społecznym, a nie terminem o charakterze ustawowym. K. Witkowska-Rozpara wyraźnie eksplikuje, za powoływaną przez siebie prof. Janiną Błachut, pozycję wiedzy teoretycznej i praktycznej w opisie tego zjawiska społecznego, umożliwiającą jego dobre rozpoznanie, co, niezależnie od strategii oddziaływania, pozwala na prowadzenie spójnej i racjonalnej polityki kryminalnej. Rozdział ten przedstawia zasady tworzenia statystyki dotyczącej przestępczości i jej znaczenie. Statystyka przestępczości jest prowadzona przez organy ścigania oraz organy wymiaru sprawiedliwości. Autorka zestawia w formie ujęć graficznych i tabelarycznych strukturę i charakterystykę przestępczości. Posługuje się przy tym szczegółowymi danymi odnoszącymi się do Polski, obejmującymi przestrzeń do roku 2010, które dotyczą wybranych kategorii przestępstw i wszczynanych w ich zakresie postępowań. Rozważania odnoszące się do przywołanych statystyk otwierają autorce pole do przedstawienia przestępczości ujawnionej i nieujawnionej oraz ich źródeł, przy zaznaczeniu roli efektywności postępowania karnego i znaczenia informacji o przestępstwie w kontekście rozważań prowadzonych na podstawie wyników badań wiktymizacyjnych.

Rozdział II dotyczy obrazu przestępczości i oddziałujących na niego czynników. W tej części znajdujemy teoretyczne rozwinięcie idei badania rozmiarów omawianego zjawiska. Autorka zdecydowanie twierdzi, że wartość poznawcza statystyk (policyjnych) sprowadza się do informowania o poziomie aktywności organów ścigania

[1] Warszawa 2011, C.H. Beck, 358 ss.

oraz o polityce rejestracji przestępstw, nie zaś o faktycznych rozmiarach przestępczości. Wątpliwości w zakresie ujęcia przestępczości w kształcie przekazywanym opinii publicznej są wzmocnione opisem zjawisk skutkujących zwiększeniem lub obniżeniem statystycznego obrazu tego zjawiska. Autorka, odnosząc do rzeczywistości polskiej, opisuje powody manipulowania danymi statystycznymi przed przełomem ustrojowym w 1989 r., kiedy to programowo skuteczne działanie organów ścigania miało dostarczać powodów do utrzymywania pożądanej wizji społeczeństwa. Uwypukla tu szczególnie krytyczne zachowania organów ścigania, w których „moda na skuteczność", wyrażana przez spektakularne sukcesy, jest wynikiem oczekiwanej efektywności. Problem dążenia do uzyskania odpowiednich nakładów na instytucję proporcjonalnie do jej osiągnięć, zjawiska związane ze świadomym fałszowaniem danych statystycznych, selekcjonowaniem danych przekazywanych opinii publicznej, a w konsekwencji prezentowanie wyników świadczących o wysokiej wykrywalności, to negatywne elementy przedstawionej w książce rzeczywistości. Autorka postuluje przeprowadzenie na gruncie europejskim niezbędnych zmian w grupowaniu i przedstawianiu danych statystycznych, obejmujących np. moment rejestracji przestępstwa (w siedmiu krajach europejskich rejestracja następuje po zakończeniu postępowania przygotowawczego).

Rozdział III zatytułowany *Obraz przestępczości w środkach masowego przekazu w europejskich systemach niedemokratycznych* zawiera opis funkcjonowania mediów w modelach: totalitarnym i właściwym dla powojennej Polski modelu nietotalitarnym społeczeństwa niedemokratycznego. Mass media w tych systemach, odnosząc się do współczesnych, demokratycznych, realiów, osiągały dysfunkcję, wyrażającą się w utracie roli, jaką powinny odgrywać, tj. roli stricte informacyjnej, na rzecz propagandowej. Chociaż temat propagandy w czasach PRL jest przedmiotem wielu publikacji, to autorka również odnosi się do tej kwestii. Nawiązuje do rozpoczętej (w związku z dekretem PKWN w 1944 r.) *bitwy o mobilizację*, której towarzyszyło wiele haseł propagandowych budzących dzisiaj uśmiech, choć wówczas stanowiły część rodzącej się agitacji partyjnej. Prowadzono ją w systemie, w którym na mocy innego dekretu (z 13 czerwca 1946 r. o *przestępstwach szczególnie niebezpiecznych w okresie odbudowy państwa*) skazywano na kary więzienia za wykonywanie utworów muzycznych (autorka powołuje się na wyrok z 21 marca 1952 r., w którym skazano sześć osób na karę pozbawienia wolności za rozpowszechnianie piosenki o treści uznanej w uzasadnieniu wyroku za ironiczny komentarz na temat braków żywnościowych w Polsce). K. Witkowska-Rozpara wskazuje, jakie doniesienia dotyczące przestępstw były najbardziej pożądane, posługując się szczegółowymi danymi statystycznymi i odnoszącymi się do preferencji w Polsce, zmieniających się aż do 1989 r. Analizuje także doniesienia prasowe dotyczące przestępczości w niemieckiej prasie.

Rozdział IV rozpoczyna się od rozważań nad znaczeniem pojęć „polityka karna" i „polityka kryminalna". Wyjaśnienie tych terminów jest niezbędne ze względu na przedmiot analizy zawartej w tym rozdziale, związany z wpływem środków masowego przekazu na kształtowanie polityki karnej w systemach niedemokratycznych. W odniesieniu do Polski przed 1989 r. uwagę zwraca szeroki zakres penalizacji; ustawodawstwo karne traktowano wówczas jako normatywną gwarancję bytu ustroju politycznego Polski Ludowej. W omawianym okresie poprzez niewątpliwe wyolbrzymianie poziomu zagrożenia przestępczością podkreślano konieczność dokonywania zmian w prawie karnym, w kierunku zwiększania jego punitywności jako reakcji oczekiwanej przez obywateli, mającej gwarantować ich bezpieczeństwo. Rozważania zawarte w tym rozdziale są poparte zestawieniami tabelarycznymi, w tym prezentującymi rodzaje i wymiar środków

karnych, które odnoszą się się do braku skuteczności kary pozbawienia wolności jako środka odstraszającego przed popełnianiem przestępstw po jej zakończeniu. Rozdział kończy ocena wpływu środków masowego przekazu na kształtowanie polityki karnej w systemach niedemokratycznych. Jak wyraża K. Witkowska-Rozpara, media, dbając o „estetyczną" stronę decyzji podejmowanych przez władzę, stanowiły również narzędzie umożliwiające dyskurs, który ostatecznie przyczynił się do podniesienia świadomości prawnej społeczeństwa i otwarcia debaty nad racjonalizacją polityki karnej.

W kolejnym rozdziale, piątym, autorka przedstawia obraz przestępczości i rolę środków masowego przekazu w systemach demokratycznych. Pojawiają się tu rozważania dotyczące roli mediów w życiu społecznym i stosowanych w tym zakresie typologii, a także dotyczące wolności słowa i jej ograniczeń, w tym ograniczenia swobody dziennikarskiej. K. Witkowska-Rozpara wymienia przypadki takich ograniczeń, wskazując zarówno ich regulację prawną w *Konstytucji RP* i niektórych innych ustawach (w tej części wskazuje np. na rezygnację w ustawie z 5 sierpnia 2010 r. o ochronie informacji niejawnych z traktowania informacji dotyczących prawnie chronionych interesów obywateli i jednostek organizacyjnych jako informacji niejawnych), jak i przywołując zasadę ochrony czci i dobrego imienia, przewidzianą w *Międzynarodowym Pakcie Praw Obywatelskich i Politycznych* oraz *Europejskiej Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności*. Autorka w swoich rozważaniach nawiązuje do debaty dotyczącej naruszania sfery prywatnej osób publicznych, przyjmując za Z. Hołdą, że każdy polityk uczestniczący w życiu publicznym powinien liczyć się z ograniczeniem przysługującego mu prawa do ochrony swojej prywatności. Przejście do działalności publicznej, jak wywodzi dalej, wymaga od polityków chociażby odporności na nadużywanie wobec nich słów brutalnych. Autorka zaznacza, że wszelkiego rodzaju propaganda wywrotowa w postaci nawoływania do obalenia legalnych władz czy podżegania do buntu jest na gruncie większości ustawodawstw europejskich zakazana, a odpowiedzialności za takie postępowanie nie można uniknąć, powołując się na wolność słowa.

Przyczyny zamieszczania w środkach masowego przekazu informacji dotyczących przestępczości i problem wynikający z podejmowania takich właśnie tematów przez media są szczególnie interesującym obszarem rozważań K. Witkowskiej-Rozpary. Autorka analizuje zniekształcenia obrazu przestępczości w zależności od charakteru mediów. Ważnym podsumowaniem tych rozważań jest stwierdzenie odnoszące się do wykluczania możliwości prezentowania w telewizji przestępczości stanowiącej rzeczywiste zagrożenie dla społeczeństwa na rzecz konstruowania takich form jej ujęcia, aby przyciągały uwagę odbiorców. A osiąga się to dzięki „właściwemu" doborowi tematów, nasilaniu w relacjach sugestywności obrazu i zachowania sprawców przestępstw, których nazwiska w istocie rzeczy rzadko przewijają się w policyjnych statystykach.

W rozdziale VI zatytułowanym *Rola środków masowego przekazu w kształtowaniu podstawowych założeń polityki karnej realizowanej w systemach demokratycznych* autorka zadaje pytanie, czy w Polsce w ostatnich latach polityka karna bardziej uwzględnia aktualne potrzeby polityczne niż badania kryminologiczne i opinie przedstawicieli nauk prawnych. Pytanie to otwiera obszar rozważań dotyczących kształtowania prawa w związku z koniecznością dokonania w nim zmian i poprawieniem skuteczności nowych regulacji (jak przywrócenie po 2006 r. instytucji występku chuligańskiego), ale również dotyczących braku wydolności polityki penitencjarnej. Wreszcie autorka opisuje najważniejsze w książce pojęcie „populizmu penalnego". Ukazuje reakcję polityków podsycaną przez media w okresie kampanii wyborczych, związaną z propagowaniem

zaostrzania polityki karnej przy wykorzystaniu zakorzenionego w społeczeństwie poczucia zagrożenia. Jako regulację motywowaną populistycznie autorka wskazuje tę związaną z przestępczością o charakterze chuligańskim. Jej nowe unormowanie doprowadziło do traktowania sprawców występków chuligańskich jak wielokrotnych recydywistów, pomimo że nie obserwowano nasilenia tego rodzaju przestępczości. Na podkreślenie nietrafności poglądu o potrzebie zaostrzenia polityki wobec sprawców występków o takim charakterze przywołano dane dotyczące wzrastającego od 2002 r. poczucia bezpieczeństwa obywateli. K. Witkowska-Rozpara pisze wprost o fetyszyzmie prawnym polityków, bazujących na przekonaniu, iż przyjęcie ustawy karnej gwarantuje automatyczne rozwiązanie problemu społecznego. Tym bardziej podlega to krytyce, gdy problemu nie ma, albo gdy nie ma on charakteru powszechnego, a dotyczy jedynie wyobrażenia określonej grupy bądź jest elementem konkurencji politycznej. Rozdział VI zawiera także opis definicyjny takich pojęć, jak „dziennikarstwo śledcze" czy „prowokacja dziennikarska".

We wnioskach ujętych w ostatnim, tj. VII, rozdziale autorka podkreśla, że lęk przed przestępczością stanowi jeden z najważniejszych „lęków ludzkości". Urynkowienie informacji o przestępczości w społeczeństwach faktycznie spowodowało, że informacje te stały się towarem na sprzedaż. Zjawisko to, powodując polaryzację zachowania odbiorców takich informacji, jest kluczem do dalszego zrozumienia wykorzystania odwołań do przestępczości przez polityków i rozwoju populizmu penalnego.

Przed przystąpieniem do lektury recenzowanej monografii (jedynie na podstawie jej wstępnego przeglądu) można odnieść wrażenie, że będzie ona dotyczyć roli mediów w ujawnianiu i przedstawianiu przestępstw. Po lekturze pierwszych stron, na których zawarta jest analiza pojęcia „przestępczość", takie wrażenie zanika. Autorka przyjęła za cel opisanie problemu w sposób, który ma prowadzić wprost do przyjęcia słuszności końcowego postulatu, tj. stworzenia i realizacji prawa w odniesieniu do efektywnej, a nie efektownej polityki karnej. Wywody przedstawione w książce należy uznać za słuszne.

Szczegółowość omawianej publikacji może jedynie częściowo sprawiać wrażenie „gubienia" przez czytelnika powiązania ze sobą opisywanych problemów. Odnosi się to zwłaszcza do szczegółowości zestawień tabelarycznych (część danych może być nieaktualna). W świetle konkluzji opierającej się na ukazaniu braku związku pomiędzy realizmem zagrożenia przestępczością a kreowanymi instrumentami wyrażającymi jego nasilenie (cechy „populizmu penalnego"), takie wrażenie ulega zatarciu.

Autorka w ciekawy sposób prezentuje część historyczną swojej publikacji, przypominając o takich zdarzeniach z najnowszej historii Polski, jak afera Rywina czy afera w zakładach mięsnych Constar SA. Wymienia je jako przykłady podkreślające rolę mediów w ujawnianiu przestępczości, ale przypomina także, zwracając uwagę na tworzenie i egzekwowanie prawa podbudowanego ideologicznie, o niechlubnej historii związanej z procesami politycznymi przeprowadzanymi w Polsce Ludowej, jak choćby o drakońskich karach, jakie zapadły w tzw. aferze mięsnej. Takie elementy na pewno ożywiają publikację.

Co do roli mediów w kształtowaniu opinii publicznej, to sposób opisania ich wpływu na politykę karną w recenzowanej publikacji najpełniej chyba potwierdza ich znaczenie jako tzw. czwartej władzy. Czytając książkę, można odnieść wrażenie, że nawet jeśli jej fragmenty wprost nie odnoszą się do mediów, to jednak omawiane tu zjawiska zachodzą przy ich udziale. Podsumowując należy stwierdzić, że monografia Katarzyny Witkowskiej-Rozpary jest godna uwagi i polecenia.

Kamil Frąckowiak

„Piracy and Maritime Crime. Historical and Modern Case Studies”, B.A. Elleman, A. Forbes, D. Rosenberg (red.)[1]

Kto jest właścicielem akwenów morskich? Kto ma prawo do swobodnej nawigacji przez morza i oceany? Kto jest odpowiedzialny za ochronę statków na morzu przed atakami piratów? Te istotne zagadnienia do dnia dzisiejszego są przedmiotem licznych dyskusji naukowych.

Przez większą część historii ludzkości morze otwarte było postrzegane jako niebezpieczny bezmiar wód. Na mapach żeglarskich było pokryte licznymi białymi plamami przyozdabionymi wizerunkami morskich potworów. W związku z tym zakładano, że morza i oceany nie mogą mieć właściciela i że nie mogą być okupowane ani zarządzane. Równocześnie zwalczanie aktów piractwa, mimo że niezmiernie pożądane, było poza jurysdykcją i możliwościami państw i feudalnych, i narodowych.

Piractwo morskie było i jest głównym obiektem zainteresowania wszystkich marynarek wojennych świata. Od początków istnienia państwowych wojsk morskich eliminowanie piractwa było jednym z ich głównych obowiązków. Jako anegdotę można przywołać autentyczną historię związaną z Juliuszem Cezarem, który, wykupiony z niewoli piratów morskich w 76 roku p.n.e., niezwłocznie utworzył eskadrę statków, by wzięły pomstę na jego porywaczach.

Mimo wagi problemu, jakim jest piractwo morskie, zarówno w Polsce, jak i za granicą pojawia się stosunkowo niewiele prawniczych opracowań naukowych poświęconych analizie aktów przemocy na morzu i przeciwdziałaniu zjawisku piractwa morskiego. Tym bardziej należy pozytywnie ocenić tę stosunkowo nową pozycję wydawniczą, która stara się zapełnić zasygnalizowaną lukę.

Z uwagi na dynamiczny rozwój piractwa morskiego oraz różne definicje aktów przemocy na morzu wykrywanie, przeciwdziałanie, a nawet określenie rozmiarów skali tego zjawiska staje się niezwykle trudne. Dane dotyczące piractwa morskiego w najlepszym przypadku mogą zostać uznane jedynie za orientacyjne. W związku z tym nie można opracować ściśle określonych standardów postępowania w celu eliminowania ataków pirackich. Dlatego też ocenę przestępczości morskiej poprzez historyczną i prawnoporównawczą analizę studiów przypadków należy uznać za szczególnie użyteczną.

Rezcenzowana publikacja składa się z 13 rozdziałów, z czego 12 zostało ujętych w trzech częściach. W rozdziale pierwszym, zatytułowanym *Współczesna historia definicji piractwa morskiego w prawie międzynarodowym*, zawarto trzy eseje poświęcone prawnej analizie wielu definicji piractwa w aktach prawa międzynarodowego. Komandor Australijskiej Królewskiej Marynarki Wojennej Penny Campbell wskazuje m.in., że definicja piractwa morskiego w aktach prawa międzynarodowego nie ulegała znacznej zmianie mimo upływu czasu. Jednocześnie zauważa, że różne organizacje międzynarodowe modyfikowały swoje definicje, by skuteczniej przeciwdziałać piractwu. Tym samym z biegiem lat wykształciło się kilka, niekiedy sprzecznych ze sobą, definicji piractwa, które funkcjonują w tej samej przestrzeni prawnej. Dokonanie

[1] Newport, Rhode Island 2010 r., Naval War College Press.

wyboru jednej z nich ma istotne znaczenie w przypadku kwestii związanych z wypłatą ubezpieczenia z tytułu odszkodowania, skutecznego ścigania karnego czy współpracy międzynarodowej w czasie antypirackich patroli przez Cieśninę Malakka.

W części pierwszej, zawierającej cztery kolejne rozdziały, autorzy skupili się na piractwie morskim w Azji Wschodniej oraz na Morzu Południowochińskim. Robert J. Antony dokonał analizy przypadków piractwa na wybrzeżu południowochińskim aż do czasów współczesnych. Jak pisze, w historii Chin za akty piractwa karano śmiercią. Do schyłkowych lat XVIII wieku urzędnicy państwowi zachowywali uprawnienia do dokonywania egzekucji natychmiast po zakończeniu procesu sądowego. W dzisiejszych Chinach syndykaty pirackie przeniosły się na południe, na wody Indonezji i Cieśniny Malakka.

Bruce A. Elleman w artykule *Rebelia Taiping, piractwo i „wojna strzał"* opisuje, w jaki sposób piractwo morskie zagrażało handlowi Imperium Brytyjskiego, szczególnie podczas Rebelii Taiping (1851–64). Z kolei za przyczynę „wojny strzał" (1856–60) autor uznaje próby zdławienia właśnie piractwa morskiego. Zauważa również, że po tej wojnie zawarto liczne chińsko-brytyjskie porozumienia, które zezwalały brytyjskiej marynarce na swobodne operowanie na wodach chińskich w celu przeciwdziałania piractwu.

W kolejnym artykule Charles W. Koburger jr. omawia zjawisko piractwa na Morzu Południowochińskim w powojennych Chinach. Podczas II wojny światowej, kiedy tradycyjne szlaki dostaw z Europy z powodu sześciu lat ciągłych walk praktycznie zamarły, akty przemocy na morzu gwałtownie wzrosły w całym regionie. Nowe państwa, powstałe w wyniku dekolonizacji, nie były szczególnie zainteresowane dławieniem piractwa, upatrując w nim *patriotyczą reakcję na morski handel międzynarodowy.*

David Rosenberg dokonuje z kolei oceny politycznej ekonomii piractwa na Morzu Południowochińskim. Pisze, że wydatnie się ono nasiliło w ciągu ostatnich dwóch dekad. Od 1990 r. ponad połowę światowych przypadków piractwa morskiego odnotowano właśnie we wspomnianym regionie. Do chwili obecnej nie wypracowano jednak, jak się zdaje, żadnego porozumienia, równomiernie rozkładającego podział ról i obowiązków pomiędzy państwa zainteresowane zwalczaniem tego zjawiska.

Część drugą publikacji poświęcono studiom przypadków aktów przemocy morskiej w południowej i południowo-wschodniej Azji. Bruce Elleman opisuje tu na przykład proceder rozbójnictwa w Wietnamie, popełnianego na tzw. ludziach łodzi. Po zakończeniu wojny wietnamskiej około trzech milionów ludności uciekło z Wietnamu, Laosu i Kambodży. Ci, którzy uciekali przez morze, stawali się ofiarami napaści lokalnych piratów żerujących na ich skromnym dobytku.

Catherine Zara Raymond analizuje piractwo i rozbójnictwo w Cieśninie Malakka. Zauważa, że w roku 2000 w tej cieśninie doszło do 75 proc. wszystkich ataków pirackich przeprowadzonych na świecie, ale np. w roku 2007 przeprowadzono ich już jedynie trzy. Ta zaskakująca zmiana jest związana, zdaniem autorki, z podejmowaniem środków zaradczych przez kapitanów statków.

Samuel Pyeatt Meneffe omawia zjawisko piractwa w Bangladeszu, którego miasto Chittagong zostało obwołane przez Międzynarodowe Biuro Morskie najniebezpieczniejszym portem na świecie. Z uwagi jednak na fakt, że port ten nie leży w pobliżu najważniejszych szlaków handlowych, rosnące zjawisko piractwa spotyka się z nikłą reakcją społeczności międzynarodowej, co w przyszłości może zagrażać bezpieczeństwu żeglugi morskiej.

Sam Bateman dokonuje analizy przestępczości morskiej na wodach południowochińskich. Autor postuluje rozszerzenie definicji piractwa morskiego o kwestię przemytu kontrabandy, nielegalnego połowu ryb i zanieczyszczania środowiska morskiego.

Część trzecia opracowania przedstawia skalę i uwarunkowania piractwa afrykańskiego. Robert F. Turner opisuje na przykład amerykański kazus *Prezydent Thomas Jefferson i Piraci*, który skutecznie ograniczył akty piractwa w rejonie północnej Afryki. Szef państwa amerykańskiego przeznaczył bowiem dwie trzecie jednostek marynarki wojennej Stanów Zjednoczonych do walki z piratami w celu ukrócenia procederu żądania okupu od rządu.

Andrew Lambert w artykule *Ograniczenia Morskiej Siły Zbrojnej: Bryg Kupiecki „Trzy Siostry"*, *Piraci Pogranicza oraz Brytyjskie Statki Wojenne* przedstawia, w jaki sposób po okresie 50-letniego spokoju po działaniach marynarki wojennej USA, Wielka Brytania stanęła przed podobnym problemem piratów atakujących statki transportowe na szlaku przez Morze Śródziemne. Rozwiązaniem problemu nie był bezpośredni atak na statki pirackie, lecz udzielenie pomocy finansowej dla Maroka, które w wysokim stopniu udoskonaliło funkcjonowanie swego wymiaru sprawiedliwości. Jeden z wniosków autora wydaje się szczególnie godny przywołania: (…) *piraci muszą żyć na lądzie, więc to na lądzie muszą zostać powstrzymani; żadne siły morskie nigdy nie będą wystarczające do przeciwdziałania piractwu*.

Arild Nodland natomiast dokonuje przeglądu skali przestępczości morskiej w Nigerii, najliczebniejszym państwie Afryki. Konkluduje, że jednym ze sposobów powstrzymania piractwa jest pomoc finansowa dla władz nigeryjskich na wzmocnienie krajowego wymiaru sprawiedliwości oraz zaangażowanie Stanów Zjednoczonych i Chin w stabilizację polityczną w regionie.

Gary Wier opisuje zjawisko piractwa w Rogu Afryki i międzynarodową reakcję na gwałtowny wzrost aktywności piratów. Omawia postanowienia *Rezolucji ONZ z 22 kwietnia 2008 r.* umożliwiające dokonywanie morskich patroli międzynarodowych na wodach terytorialnych Somalii w celu przeciwdziałania piractwu. Autor jednak słusznie zauważa, że powstrzymanie piratów na morzu nie oznacza jeszcze zwycięstwa na lądzie, szczególnie, gdy rząd Somalii kontroluje jedynie dwie trzecie terytorium państwa.

Całe opracowanie kończą wnioski autorów, którzy trafnie przedstawiają i selekcjonują czynniki wpływające na rozwój piractwa morskiego oraz morskiego tranzytu międzynarodowego. Dokonują również krytycznej charakterystyki multilateralnych relacji marynarek wojennych państw przeciwdziałających aktom przemocy na morzu. Wreszcie dokonują interesującej i potrzebnej oceny wdrażania i ograniczeń antypirackich operacji morskich przy użyciu nowoczesnych technologii. Zarysowują również cele polityki międzynarodowej dotyczącej omawianego zjawiska.

Monografia *Piracy and Maritime Crime. Historical and Modern Case Studies,* ze względu na walory merytoryczne jest godna polecenia przede wszystkim osobom zajmującym się zjawiskiem piractwa morskiego naukowo. Książka jest cennym źródłem wiedzy, które syntetycznie przedstawia kwestie związane z historycznymi, strategicznymi oraz prawnymi aspektami tej problematyki. Opracowanie może również zaciekawić szerokie grono odbiorców profesjonalnie związanych z żeglugą oraz osoby zajmujace się tym zagadnieniem hobbistycznie. Kolejną grupą, którą niniejsza publikacja może zainteresować, mogą być specjaliści z dziedziny stosunków międzynarodowych, konfliktów zbrojnych i bezpieczeństwa wewnętrznego, a także publicyści i dziennikarze. Praca ta jest także inspiracją do podejmowania dalszych poszukiwań naukowych dotyczących przedmiotowego tematu.

Recenzowana publikacja w znaczący sposób wypełnia lukę powstałą na krajowym rynku wydawniczym i bez wątpienia przyczynia się do lepszego zrozumienia zjawiska piractwa morskiego oraz związanego z nim zagrożenia dla bezpieczeństwa i ładu międzynarodowego.

Fabiana Fetke (I)
Krzysztof Izak (II)

Michael Bar-Zohar, Nissim Mishal, *Mossad. Najważniejsze misje izraelskich tajnych służb*[1]

I.

W czerwcu 2010 r. na lotnisku Okęcie w Warszawie Straż Graniczna zatrzymała niepozornie wyglądającego mężczyznę legitymującego się paszportem wystawionym na nazwisko Uri Brodsky. Polskie służby zatrzymały go na podstawie Europejskiego Nakazu Aresztowania wydanego przez Niemcy. Strona niemiecka zarzucała Brodsky'emu prowadzenie działalności wywiadowczej przeciwko Niemcom, poświadczenie nieprawdy oraz pomoc w sfałszowaniu dokumentów dla osoby, która miała brać udział w zabójstwie lidera Hamasu, Mahmuda al-Mabhuha[2]. 19 stycznia 2010 r. al-Mabhuh, jeden z założycieli brygady im. Izza ad-Dina al-Kassama, zbrojnego skrzydła Hamasu, został zamordowany w jednym z hoteli w Dubaju. Nieznani sprawcy weszli do pokoju al-Mabhuha i wstrzyknęli mu silny środek znieczulający na bazie hydrochlorydu, wykorzystywanego przed operacjami, a następnie udusili go, aby śmierć wyglądała na naturalną. O zabójstwo od początku były podejrzewane izraelskie służby specjalne. O kulisach tego zabójstwa można przeczytać w jednym z rozdziałów książki autorstwa Michaela Bara-Zohara i Nissima Mishala *MOSSAD – najważniejsze misje izraelskich tajnych służb*, która ukazała się na polskim rynku na początku listopada 2012 r. nakładem wydawnictwa REBIS. Warto wspomnieć, że wcześniejsza wersja tej pozycji, wydana w Izraelu w roku 2010, przez ponad 70 tygodni utrzymywała się na liście izraelskich bestsellerów, a najnowsze wydanie ukazało się prawie równocześnie w ponad 20 krajach.

Mossad[3] w świecie służb specjalnych ma opinię instytucji tajemniczej, niezwykle skutecznej, ale przede wszystkim bezwzględnej, której funkcjonariusze nie wahają się stosować najbardziej radykalnych metod, aby zapewnić bezpieczeństwo swojemu krajowi. Działalność tej służby obrosła legendą głównie za sprawą operacji z lat 60. i 70. XX wieku, ale i dziś Mossad czynnie uczestniczy w wojnie z terroryzmem. Mossad to nie tylko genialni szefowie, których wyjątkowa wyobraźnia, umiejętność przewidywania posunięć przeciwnika i perfekcyjna logistyka doprowadziła tę służbę niemal do doskonałości. Siłą napędową Mossadu są przede wszystkim bezimienni bojownicy, mężczyźni i kobiety, którzy ryzykują życie, żyją z dala od swych rodzin pod przybranymi nazwiskami, przeprowadzają śmiałe operacje we wrogich krajach, gdzie

[1] Poznań 2012, REBIS, 384 ss.

[2] Ostatecznie 12 sierpnia 2010 r. Uri Brodsky został wydany stronie niemieckiej. Warunkiem dopuszczalności ekstradycji był brak możliwości sądzenia go w Niemczech za szpiegostwo, a tylko za poświadczenie nieprawdy i pomoc w sfałszowaniu dokumentów. Po wpłaceniu kaucji w wysokości 100 tys. euro Brodsky został zwolniony z niemieckiego aresztu i wyjechał do Izraela.

[3] Oficjalna nazwa Mossadu to Instytut do spraw Wywiadu i Zadań Specjalnych (*Ha-Mossad le-Modiin u-le Tafkidim Mejuchadim*). Mossad został formalnie utworzony 1 kwietnia 1951 r. jako Instytut Koordynacji (*Ha Mossad Leteum*). Obecna nazwa została nadana w 1963 r.

najmniejszy błąd może doprowadzić do ich aresztowania, torturowania lub śmierci[4]. I właśnie tym wszystkim ludziom jest poświęcona niniejsza publikacja.

Autorzy książki to osoby mające szeroką wiedzę na temat służb. Michael Bar-Zohar jest uważany w Izraelu za jednego z najlepszych specjalistów od spraw wywiadu. Informacje często uzyskiwał z pierwszej ręki, jest bowiem nie tylko pisarzem i wykładowcą akademickim, ale w przeszłości zasiadał w parlamencie. Stąd jego osobista znajomość z wieloma najważniejszymi osobami w Izraelu, również z tymi odpowiadającymi za służby specjalne i ich działanie. Warto wspomnieć, że M. Bar-Zohar jest autorem wielu publikacji z dziedziny faktu oraz oficjalnych biografii pierwszego premiera Izraela Dawida Ben Guriona oraz obecnego prezydenta Szymona Peresa. Nissim Mishal zaś to jedna z najbardziej znanych postaci izraelskiej telewizji: reporter polityczny, były korespondent w Waszyngtonie, a także były dyrektor generalny izraelskiej telewizji państwowej.

Autorzy podzielili książkę na 21 rozdziałów opowiadających o najważniejszych i najciekawszych operacjach przeprowadzonych przez Mossad w ciągu 60 lat jego działalności. Operacji, które wpłynęły nie tylko na los Izraela, ale pod pewnymi względami miały również niebagatelne znaczenie dla reszty świata. Wśród przedstawionych w książce działań są dobrze znane misje, wielokrotnie opisywane, a nawet filmowane, jak choćby uprowadzenie hitlerowskiego zbrodniarza wojennego Rudolfa Eichmanna[5] czy odwet na terrorystach z organizacji Czarny Wrzesień, odpowiedzialnych za masakrę na olimpiadzie w Monachium[6]. Co istotne, autorzy przedstawiają również kulisy tych mniej znanych operacji, ujawnionych dopiero w ostatnim czasie, a nawet tych, o których nikt jeszcze nie słyszał. Nie skupiają się przy tym wyłącznie na działaniach międzynarodowych, takich jak eliminacja dowódców Ludowego Frontu Wyzwolenia Palestyny, zniszczenie syryjskich instalacji nuklearnych i zamachy na czołowych irańskich fizyków jądrowych, lecz także na operacjach prowadzonych wewnątrz Izraela, niejako przeciwko obywatelom własnego kraju, jak choćby kulisy penetrowania przez służbę środowisk żydowskich w poszukiwaniu małego chłopca Josele Schuchmachera, porwanego przez ortodoksyjną sektę.

Warto zauważyć, że autorzy nie zawahali się wspomnieć również o porażkach Mossadu wynikających z rutyny, błędów i zaniedbań poszczególnych agentów czy też ich przełożonych, które często kosztowały życie wielu osób. Autorzy bezlitośnie odkrywają kulisy nieudanej operacji ukierunkowanej na zabicie przywódcy Biura Politycznego Hamasu Chalida Meszala. Operacja ta zakończyła się kompletnym fiaskiem militarnym i politycznym, a przy okazji doprowadziła do absurdalnej sytuacji, kiedy to Izraelczycy najpierw próbowali otruć Maszala, a gdy zostali zdemaskowani, to wspólnie z Jordańczykami uczestniczyli w wyścigu z czasem o uratowanie życia ich największego wroga.

Wspomniane na wstępie zatrzymanie Uriego Brodsky'ego na warszawskim lotnisku Okęcie to nie jedyny wątek polski opisany przez autorów. Gdyby bowiem na przykład, o czym piszą autorzy, Witold Grajewski nie zaniósł do izraelskiej ambasady dokumentów udostępnionych mu przez swoją kochankę – współpracownicę Edwarda

[4] M. Bar-Zohar, N. Mishal, *MOSSAD – najważniejsze misje izraelskich tajnych służb,* Poznań 2012, REBIS, s. 13.

[5] *Człowiek, który pojmał Eichmanna (The Man Who Captured Eichmann*), reż. W. A. Graham; *Eichmann (Eichmann*), reż. R. Yung.

[6] *Miecz Gideona (Sword of Gideon)*, reż. M. Anderson; *Monachium (Monachium*), reż. S. Spielberg.

Ochaba, pierwszego sekretarza PZPR – do amerykańskich gazet nie trafiłaby treść tajnego referatu Nikity Chruszowa wygłoszonego na XX Zjeździe Komunistycznej Partii Związku Radzieckiego w lutym 1956 r., który wywołał wstrząs w świecie komunistycznym i spowodował zacieśnienie relacji amerykańskich i izraelskich służb specjalnych.

Mossad – najważniejsze misje izraelskich tajnych służb to przede wszystkim książka historyczna, napisana jasnym i niezwykle wciągającym stylem utrzymanym w tonie popularnonaukowym, który miejscami został jednak zbeletryzowany. Dlatego też po jej przeczytaniu powinny być usatysfakcjonowane nie tylko osoby zainteresowane historią i polityką Izraela, konfliktem na Bliskim Wschodzie czy tematyką służb wywiadowczych, lecz także miłośnicy dobrej literatury sensacyjnej.

Warto też wspomnieć o bogatej, liczącej 30 stron bibliografii. Autorzy podkreślili, że z uwagi na fakt, że tematyka książki dotyczy często kwestii niejawnych, ważne było dotarcie do wiarygodnych, solidnych źródeł. Podczas prac nad poszczególnymi rozdziałami opierali się na obszernych materiałach: książkach, dokumentach, artykułach prasowych, ale przede wszystkim na relacjach osób, które były świadkami opisywanych operacji, bezpośrednio brały w nich udział, a często również decydowały o ich przebiegu. Całości dopełniają kolorowe fotografie przedstawiające głównych bohaterów opisywanych w poszczególnych rozdziałach, pochodzące w większości z archiwum autorów, oraz pomocny *Indeks* zamieszczony na końcu książki.

Spośród wielu publikacji dotyczących historii i działalności izraelskich służb specjalnych tę wyróżniają dwie istotne cechy. Po pierwsze aktualność – autorzy nie skupili się bowiem wyłącznie na historii Mossadu, ale dotarli do informacji o wydarzeniach z niedalekiej przeszłości, których głównymi bohaterami były osoby jeszcze nie tak dawno stojące na czele tej organizacji, goszczące nawet w siedzibie Agencji Bezpieczeństwa Wewnętrznego (jak choćby Meir Dagan – Dyrektor Mossadu w latach 2002–2010). Po drugie zaś przedstawili poszczególne wydarzenia nie tylko odtwórczo, lecz także spróbowali włączyć się we współczesną debatę polityczną, wskazując we wstępie na fiasko „arabskiej wiosny" i związane z nią niebezpieczeństwa dla świata zachodniego oraz zadając w epilogu pytania o zasadność ewentualnej interwencji zbrojnej przeciwko fanatykom rządzącym Iranem, którzy stanowią poważne, ale przede wszystkim realne, zagrożenie nie tylko dla Izraela. Zagrożenie, które – jak wskazują– Izraelczykom przywołuje na myśl starą talmudyczną maksymę: *Jeśli ktoś przychodzi, by cię zabić, wstań i zabij go pierwszy*.

Na zakończenie należy zwrócić uwagę na jeszcze jedną rzecz. Cytując powyższą maksymę, nie sposób nie zauważyć, iż z uwagi na przedstawione w książce metody stosowane przez służby izraelskie, niejednokrotnie polegające na fizycznej eliminacji przeciwników, u niektórych czytelników, zwłaszcza tych słabiej zorientowanych w realiach panujących na Bliskim Wschodzie, recenzowana publikacja może wywołać sprzeciw, że w majestacie prawa zabijani są ludzie – terroryści, zabójcy – ale jednak ludzie, którym bezpowrotnie odbiera się prawo do sprawiedliwego procesu i wyroku.

II.

Do serii publikacji dotyczących historii i działalności największych i najbardziej znanych służb specjalnych na świecie dołączyła w końcu 2012 r. książka dwóch izraelskich autorów na temat cywilnego wywiadu Izraela – Mossadu. Jej wcześniejsza wersja ukazała się w Izraelu w 2010 r. i przez prawie półtora roku utrzymywała się na listach bestsellerów, bijąc rekordy sprzedaży. Obecne wydanie ukazało się równocześnie

w ponad dwudziestu krajach na świecie i odniosło wielki sukces wydawniczy. W Polsce prawdopodobnie nie będzie inaczej i publikacja ta stanie się równie popularna jak *Szpiedzy Gideona. Tajna historia Mossadu*, książka autorstwa Gordona Thomasa, wydana w 2000 r. przez wydawnictwo Magnum, a potem kilkakrotnie wznawiana[7].

Michael Bar-Zohar jest jednym z najlepszych izraelskich specjalistów od spraw wywiadu, autorem licznych książek naukowych i popularnonaukowych, w tym oficjalnych biografii premierów Izraela Dawida Ben Guriona i Szimona Peresa. Wykładał na Uniwersytecie w Hajfie i Emory University w Atlancie. Nissim Mishal natomiast jest jedną z najbardziej znanych postaci izraelskiej telewizji. Był reporterem politycznym, korespondentem w Waszyngtonie i dyrektorem generalnym izraelskiej telewizji państwowej. Książka *Mossad*... rozsławiła obu autorów w wielu krajach na świecie i nie ma w tym nic dziwnego, ponieważ jest to porywająca lektura, którą czyta się jak doskonałą powieść sensacyjną.

Autorzy zgromadzili olbrzymi materiał badawczy i dziennikarski, przeprowadzając dziesiątki rozmów i wywiadów z kolejnymi szefami izraelskiego wywiadu cywilnego i jego agentami uczestniczącymi w najważniejszych operacjach wywiadowczych na całym świecie. Barwnie przedstawili ich sylwetki i ryzykowną działalność ocierającą się często o granicę życia i śmierci. Były to nie tylko operacje wynikające z głębokiego patriotyzmu i strategicznych celów Izraela, ale także przedsięwzięcia kontrowersyjne, budzące wątpliwości, których źródłem był konflikt interesów. Wywoływały one nieraz oburzenie światowej opinii publicznej i powodowały zaostrzenie stosunków Izraela z zagranicznymi partnerami.

Mossad bowiem przeprowadzał nie tylko zagraniczne operacje na rzecz bezpieczeństwa państwowego i obronności, lecz także działania mające na celu kradzież najnowszych technologii, wykonywał wyroki śmierci na hitlerowskich zbrodniarzach i arabskich terrorystach oraz prowadził poszukiwania własnych obywateli. Nie obeszło się przy tym bez pomyłek i błędów wynikających z rutyny, lekkomyślności lub złamania procedur.

Książka składa się z 21 rozdziałów zapoznających czytelnika z poszczególnymi operacjami Mossadu. Zostały one ułożone chronologicznie, z wyjątkiem dwóch pierwszych i ostatniego. Rozdział pierwszy, zatytułowany *Król Cieni*, jest niejako hołdem złożonym ostatniemu szefowi, czyli *ramsadowi* (skrót od rosz Ha-Mossad – szef Mossadu) Meirowi Daganowi, który kierował izraelskim wywiadem przez osiem i pół roku (sierpień 2002–styczeń 2010 r.), a więc dłużej niż większość dyrektorów Mossadu. Stanowisko objął po Efraimie Halevym. Funkcję szefa wywiadu przejmował w momencie, gdy służba ta znajdowała się w kryzysie spowodowanym porażkami (m.in. nieudany zamach na działacza Hamasu Chalida Meszala w Ammanie czy aresztowania izraelskich agentów w Szwajcarii, na Cyprze i Nowej Zelandii). Dagan nie został dobrze przyjęty przez Mossad. W proteście przeciwko jego nominacji kilku wysokich oficerów

[7] Niemal 10 lat wcześniej, bo w 1991 r., nakładem wydawnictwa Polus, ukazała się książka Claire Hoy i Victora Ostrovsky'ego zatytułowana: *Z tajemnic izraelskiego wywiadu*. Ostrovsky opuścił Mossad w atmosferze skandalu, a jego byli pracodawcy usiłowali zapobiec wydaniu książki. Gordon Thomas jest natomiast autorem ponad 30 książek, w tym kilku poświęconych służbom wywiadowczym (m.in. MI6 i CIA). Jego bestseller, *Szpiedzy Gideona. Tajna historia Mossadu*, był pierwszą książką na temat Mossadu, napisaną na podstawie rozmów przeprowadzonych z jego szefami i agentami oraz na podstawie tajnych dokumentów. Autor w sposób sensacyjny omawia operacje izraelskiej tajnej służby: zabójstwa, porwania i zamachy, wprowadzając narrację bohaterów. W celu uzupełnienia tej krótkiej notki bibliograficznej należy jeszcze wymienić wymienić książkę *AMAN. Wywiad wojskowy Izraela*, pióra Samuela M. Katza, wydaną w 1999 r. przez Bellonę.

złożyło dymisję. Nieprzychylna była mu również prasa, która krytykowała go za surowe traktowanie podwładnych (Dagan, były wojskowy w randze generała, w 2002 r. przeszedł na emeryturę, z której ściągnięto go na stanowisko *ramsada*). Jednak stanął na wysokości zadania. Pod jego kierownictwem Mossad przeprowadził skuteczne operacje, eliminując przywódcę wojskowego skrzydła Hezbollahu – Imada Fajiza Mughniję oraz innych liderów terrorystycznych ugrupowań w Libanie i Syrii, a także przyczynił się do zniszczenia syryjskiego reaktora atomowego w 2007 r. i prowadził udane operacje przeciwko tajnemu irańskiemu programowi atomowemu.

Te ostatnie działania są tematem drugiego rozdziału. Autorzy nie opisują ich jednak z pozycji uczestników operacji, które wciąż są prowadzone, lecz widzą je oczami komentatorów międzynarodowych mediów i zachodnich służb specjalnych. I tak, według źródeł francuskich, Mossad współpracował z CIA i MI6, przy czym odpowiadał za likwidację w Iranie osób cywilnych i wojskowych związanych z programem atomowym. Zabójstwa irańskich uczonych stanowiły tylko jeden z elementów w tej walce. Według brytyjskiego „The Daily Telegraph" Mossad pod kierownictwem Dagana zorganizował oddział szturmowy, grupy uderzeniowe oraz firmy sabotażowe i fasadowe, które sprzedawały Iranowi uszkodzony sprzęt, infekując wirusami oprogramowanie komputerowe wykorzystywane przy wzbogacaniu uranu. Kiedy na początku stycznia 2011 r. Dagan odchodził ze stanowiska, to poinformował, że Iranowi nie uda się do 2015 r. wyprodukować broni jądrowej i dlatego zaproponował kontynuowanie tych samych działań swojemu następcy, Tamirowi Pardzie[8]. Odniesienia do irańskiej antynuklearnej działalności Mossadu znalazły również miejsce w epilogu.

Historyczne ujęcie działań izraelskiego wywiadu otwiera rozdział *Szubienice w Bagdadzie*. Opisane są tu początki działań izraelskiego wywiadu, kiedy to po powstaniu państwa Izrael zaszła konieczność walki o jego przetrwanie z arabskimi sąsiadami. W tym czasie działania wywiadowcze prowadziły niezależne grupy złożone z bojowników Hagany[9], Irgunu[10] i Grupy

[8] Meir Dagan jest przeciwnikiem izraelskiego ataku na irańskie instalacje jądrowe. Stwierdził wprost, że taki atak *byłby najgłupszą rzeczą, jaką można sobie wyobrazić*, gdyż doprowadziłby do zdestabilizowania sytuacji w regionie. M. Kęskrawiec, *Teheran przyparty do muru* [online], www.tygodnik.onet.pl [dostęp: 26 IV 2012].

[9] Hagana, czyli Obrona, była paramilitarną żydowską organizacją działającą na terenie Palestyny. Powstała w 1920 r. w celu obrony żydowskich osadników przed Arabami, którzy nie zgadzając się z napływem żydowskich imigrantów z Europy wzniecali zamieszki i powstania. Z czasem Hagana przeobraziła się z organizacji paramilitarnej w strukturę wojskową. Podczas drugiej wojny światowej nawiązała współpracę z Brytyjczykami, a jej bojownicy zaciągali się również do armii brytyjskiej na Bliskim Wschodzie. Po utworzeniu Izraela Hagana stanowiła trzon armii nowego państwa, zwanej Siłami Obronnymi Izraela (*Cewa Hagana le-Israel – Cahal*). Zob. *Hagana* [online], http://wikipedia.org/wiki/Hagana [dostęp: 8 I 2013].

[10] Pełna nazwa to Irgun Cwai Leumi – Narodowa Organizacja Wojskowa (w skrócie ECEL). Została założona w 1937 r. przez Dawida Raziela, z inspiracji Włodzimierza Żabotyńskiego, który namówił grupę zwolenników do odłączenia się od Hagany i założenia nowego ruchu zbrojnego, którego celem byłoby doprowadzenie do powstania państwa żydowskiego w Palestynie. Sposobem do osiągnięcia tego celu była walka zbrojna. W swojej działalności Irgun stosował terroryzm wymierzony w brytyjskich żołnierzy i administrację na terenie Palestyny. W latach 1943–1948 przywódcą Irgunu był Menachem Begin, późniejszy premier Izraela. A. Krawczyk, *Terroryzm ugrupowań fundamentalistycznych na obszarze Izraela w drugiej połowie XX wieku*, Toruń 2007, Adam Marszałek, s. 44–45.

Sterna[11], które angażowały się w antybrytyjskie i antyarabskie akcje o charakterze terrorystycznym w Palestynie w latach 30. i 40. XX w. W grudniu 1949 r. Ben Gurion, zwany „twórcą Izraela" lub „ojcem narodu" rozkazał założenie Mossadu, czyli Instytutu, który kontrolowałby agencje wywiadowcze[12]. Jednak dopiero po dwóch latach powstała scentralizowana instytucja wywiadowcza, nazwana *Ha-Mossad le-Modi'in ule Tafkidim Meyuhadim* – Instytut do spraw Wywiadu i Zadań Specjalnych, na którego czele stanął Reuwen Sziloach. Jednym z głównych jego zadań w pierwszych latach istnienia było sprowadzenie do Izraela dziesiątków tysięcy zagrożonych Żydów z krajów arabskich, w tym z Iraku. Operację przeprowadzała tam izraelska siatka wywiadowcza pod dowództwem Mordechaja Ben Porata, działającego pod pseudonimem Zaki Awiw.

W kolejnych rozdziałach znajdujemy informacje dotyczące podstawowych zasad działania Mossadu. Niewątpliwie najważniejsza z nich to poświęcanie wszystkich sił i środków dla ratowania agenta i sprowadzenia go do kraju, niezależnie od sytuacji, choć często są to operacje, które nie zawsze kończą się sukcesem, oraz zasada niewykorzystywania diaspory żydowskiej w operacjach wywiadowczych i specjalnych na terenie kraju jej zamieszkiwania ze względu na jej bezpieczeństwo. Poznajemy strukturę organizacyjną Mossadu z jego podstawowymi wydziałami i ich szefami, tj. Wydział Operacji Specjalnych „Cezarea" z elitarną jednostką Kidon, Wydział Wywiadu ds. Informacji (Tzomet), Wydział Wywiadu ds. Monitoringu Celów Wroga (Newiot), Wydział Współpracy z Zagranicznymi Służbami Wywiadu (Tewel), Wydział Badań i Wydział Techniki Specjalnej oraz jednostkę ochrony Żydów we wrogich krajach, ułatwiającą im jednocześnie imigrowanie do Izraela (Bitzur, a następnie Tzafririm).

Autorzy kreślą sylwetki kolejnych szefów Mossadu i niektórych jego agentów, wiele miejsca poświęcając Isserowi Harelowi, legendarnemu dyrektorowi wywiadu w latach 1952–1963 i przyjacielowi premiera Ben Guriona. Przyjaźń ta zakończyła się kłótnią i dymisją Harela po ujawnieniu akcji izraelskiego wywiadu w Egipcie, gdzie w najlepsze rozwijała się współpraca z niemieckimi inżynierami na rzecz skonstruowania egipskiej broni rakietowej. Kierujący się obsesyjną niechęcią do Niemców Harel nakazał agentom Mossadu spenetrowanie służb wywiadowczych RFN i Egiptu. Posługując się przy tym zastraszaniem i działaniami terrorystycznymi, doprowadził do przerwania współpracy zachodnioniemieckich inżynierów z egipskim przemysłem zbrojeniowym. Ujawnienie tych działań, a towarzyszyły im wyolbrzymiona przez media skala zagrożenia dla Izraela ze strony Egiptu i oskarżenia pod adresem RFN, musiały doprowadzić do kryzysu dyplomatycznego, tym bardziej, że po wcześniejszym

[11] Właściwa nazwa organizacji brzmiała: Lohamei Herut Izrael – Lehi (Bojownicy o Wolność Izraela). Organizacja ta w roku 1940 oddzieliła się od Irgunu. Powodem rozłamu było odrzucenie przez jej członków zawieszenia broni z Brytyjczykami po wybuchu drugiej wojny światowej i uznanie ich za głównego wroga. Organizacja nazywana była Grupą Sterna, od nazwiska jej przywódcy – Abrahama Sterna, który dążył do nawiązania współpracy z Niemcami wymierzonej przeciwko Wielkiej Brytanii. Napisał nawet list do Hitlera, który jednak pozostał bez odpowiedzi. Organizacja dokonała licznych aktów terroru wymierzonych przeciwko brytyjskiej obecności w Palestynie i arabskim działaczom. C. Shindler, *Historia współczesnego Izraela*, Warszawa 2011, Książka i Wiedza, s. 218–219.

[12] W maju 1948 r. różne grupy żydowskich bojowników, w tym Hagany, Irgunu i Grupy Sterna połączyły się z rozkazu Ben Guriona w Siły Obronne Izraela, tworząc regularną armię, skutecznie walczącą z wojskami Libanu, Syrii, Jordanii i Egiptu. J. Jarząbek, *Palestyńczycy na drodze do niepodległości. Rozwój, przemiany i kryzys ruchu narodowego*, Warszawa 2012, Trio, s. 28–30.

spotkaniu Ben Guriona z kanclerzem Niemiec, Konradem Adenauerem, stosunki między obu krajami wydawały się normalizować.

Brak obiektywizmu podczas egipskiej operacji zarzucił Mossadowi gen. Meir Amit – szef Amanu (Wywiadu Sił Obronnych Izraela). W szczegółowym raporcie przedstawionym premierowi poinformował, że pracujący w Egipcie niemieccy uczeni byli w stanie skonstruować jedynie przestarzałe technologicznie pociski rakietowe. Ich działalność rzeczywiście stwarzała niebezpieczeństwo, panika jednak, która zapanowała wówczas w mediach i kręgach rządowych Izraela, była niewspółmierna. Po dymisji Issera Harela to właśnie Amit został kolejnym ramsadem.

Trudno oprzeć się wrażeniu, że raport Amita mógł stanowić odwet za nieudaną operację Amanu przeprowadzoną w 1954 r. również w Egipcie. Tym razem minister obrony, Pinhas Lawon, i poprzedni szef wywiadu wojskowego – płk Benjamin Gibli, chcąc powstrzymać Brytyjczyków przed opuszczeniem Egiptu, opracowali niebezpieczny plan przeprowadzenia zamachów terrorystycznych na terytorium zachodniego sąsiada[13].

Mając na uwadze klauzulę brytyjsko-egipskiego porozumienia, która zezwalała na powrót wojsk Wielkiej Brytanii do głównych baz w przypadku wybuchu kryzysu, szefowie izraelskich sił zbrojnych założyli, że zamachy terrorystyczne wywołają w Egipcie chaos, który spowoduje pozostanie jednostek brytyjskich w tym kraju. Zaplanowano zatem zamachy wymierzone w amerykańskie i brytyjskie ośrodki oświatowe i kulturalne oraz w kina, poczty i budynki użyteczności publicznej. Do przeprowadzenia ataków terrorystycznych zmobilizowano miejscowych młodych Żydów (kobiety i mężczyzn, żarliwych syjonistów) wyposażając ich w prymitywne ładunki wybuchowe z opóźnionym zapłonem, które umożliwiały sprawcom ucieczkę przed wybuchem. Po kilku mniejszych akcjach jeden z żydowskich terrorystów został zatrzymany przez policję przed wejściem do kina w Aleksandrii[14]. Wkrótce aresztowano wszystkich członków syjonistycznej siatki. Stanęli oni przed egipskim sądem. Dwóch z nich skazano na karę śmierci, a pozostałych na kary więzienia, z karą dożywocia włącznie. Jeden z oskarżonych popełnił w więzieniu samobójstwo.

Aman złamał wówczas uświęconą zasadę izraelskiego wywiadu, która głosi zakaz angażowania miejscowych Żydów we wrogie operacje na terenie kraju ich zamieszkiwania. Ponadto członkowie siatki nie zostali odpowiednio przeszkoleni do tego typu akcji, co skończyło się dla nich tragicznie, a cała sprawa, zwana „aferą Lawona" (do której nikt nie chciał się przyznać) zakończyła się głębokim kryzysem politycznym w Izraelu. W jego wyniku minister obrony Pinhas Lawon został zmuszony do rezygnacji ze stanowiska, a szef Amanu, Benjamin Gibli, wystąpił z wojska. Wizerunkowo natomiast zyskał Mossad.

---

[13] Do dnia 19 czerwca 1954 r. Brytyjczycy zgodzili się wycofać z Egiptu. Wojskowa obecność Wielkiej Brytanii w bazach wzdłuż Kanału Sueskiego była gwarantem bezpieczeństwa dla Izraela. W chwili ewakuacji Brytyjczyków w rękach armii egipskiej znalazłyby się bazy i lotniska wraz z wyposażeniem, które znacznie podniosłyby jej zdolności bojowe. B. Stępniewska-Holzer, J. Holzer, *Egipt. Stulecie przemian*, Warszawa 2006, Collegium Civitas, Dialog, s. 114–115.

[14] Zamach w aleksandryjskim kinie „Rio" miał być dokonany w drugą rocznicę przewrotu Ruchu Młodych Oficerów, na czele z płk. Gamalem Abdelem Naserem, który doprowadził do obalenia króla Faruka I i detronizacji jego syna, Fuada II. M. Bar-Zohar, N. Mishal, *Mossad*…, s. 146.

Polski wątek działalności Mossadu przewija się w spontanicznej operacji zdobycia tajnego referatu Nikity Chruszczowa, wygłoszonego podczas zamkniętej części XX Zjazdu Komunistycznej Partii Związku Radzieckiego w 1956 r. (rozdział 5). CIA oferowała milion dolarów nagrody za ten dokument, przewidując, że jego opublikowanie może wywołać kryzys polityczny w krajach bloku komunistycznego. W zdobycie tego referatu przypadkowo zaangażował się Wiktor Grajewski, redaktor Polskiej Agencji Prasowej, zajmujący się problematyką wschodnioeuropejską. Był polskim Żydem; w rzeczywistości nazywał się Wiktor Szpilman. Jego kochanką była Łucja Baranowska, sekretarka Edwarda Ochaba, ówczesnego I sekretarza PZPR. Grajewski, widząc na biurku w sekretariacie KC PZPR polskie tłumaczenie przemówienia Chruszczowa opatrzone klauzulą „ściśle tajne", poprosił Baranowską o wypożyczenie tego dokumentu na kilka godzin w celu jego przeczytania. Kobieta ku jego zaskoczeniu dokument przekazała. Po zapoznaniu się z jego treścią Grajewski postanowił zrobić z niego użytek i pokazał go w Ambasadzie Izraela w Warszawie. Tam zrobiono jego fotokopię, która pocztą dyplomatyczną trafiła do Tel Awiwu, a następnie do Waszyngtonu, a w dniu 5 czerwca 1956 r. została opublikowana w „New York Times". Publikacja referatu Chruszczowa wywołała na świecie wstrząs. Światowa opinia publiczna oficjalnie dowiedziała się o niewyobrażalnych zbrodniach stalinowskich. Niektórzy historycy uważają wręcz, że opublikowanie tego dokumentu przyczyniło się do wystąpień antykomunistycznych w Polsce w 1956 r. i powstania na Węgrzech jesienią tego samego roku. Poza tym doprowadziło do przełomu w relacjach Mossadu z CIA.

Interesujące były dalsze losy agenta Szpilmana, które również zostały w omawianej publikacji opisane. Równie niezwykłe było umiejscowienie jednego z współpracowników Mossadu w najwyższych kręgach władzy Egiptu. Był nim Aszraf Marwan, od 1966 r. mąż córki prezydenta Egiptu Gamala Abdela Nasera. O szczegółach nawiązania przez niego współpracy z izraelskim wywiadem można przeczytać w rozdziale 14. Po śmierci teścia w 1970 r. kontynuował on współpracę z Mossadem, przekazując informacje, za które każdorazowo otrzymywał honorarium w wysokości 100 tys. USD. Niewątpliwie były to informacje pierwszorzędnej wagi. Przekazywał je potem jako sekretarz prezydenta Anwara as-Sadata do spraw informacji i specjalny doradca. „Anioł", bo taki był jego pseudonim, dostarczył Mossadowi wyprzedzającą wiadomość o przygotowywaniu ataku Egiptu i Syrii na Izrael w dniu 6 października 1973 r., podczas żydowskiego święta Jom Kipur[15]. Izrael odniósł wówczas zwycięstwo, ale wojna kosztowała go ponad 2600 zabitych i ponad 7200 rannych. Zbyt duże straty wywołały protesty w izraelskim społeczeństwie. Powołana wówczas przez rząd komisja śledcza mająca zbadać proces decyzyjny podczas wojny nakazała natychmiastowe zdymisjonowanie szefa Amanu gen. Eliego Zeiry, szefa sztabu Dawida Elazara i kilku innych wysokich oficerów izraelskiej armii. Po wojnie w Jom Kipur „Anioł" kontynuował współpracę z Mossadem i CIA. Po latach jednak izraelska prasa i Eli

[15] Wojna zakończyła się 23 października 1973 r. Armia syryjska została pokonana na Wzgórzach Golan, a wojska izraelskie znalazły się ok. 30 km od Damaszku. Egipcjanie zajęli pas ziemi o szerokości 8 km po izraelskiej stronie Kanału Sueskiego (Półwysep Synaj znajdował się pod panowaniem Izraela od wojny sześciodniowej w 1967 r.), lecz egipska 3. Armia została otoczona przez siły izraelskie, które zdobyły również przyczółek na terytorium Egiptu i zbliżyły się na odległość 100 km od Kairu. Sytuacja zmusiła Egipt do negocjacji, w których wyniku podpisano dwa porozumienia: jedno o zakończeniu walk, a drugie ustanawiające trwały pokój między stronami. Syria odmówiła udziału w procesie pokojowym. M. Bar-Zohar, N. Mishal, *Mossad*…, s. 239.

Zeira ujawnili jego tożsamość. W imię dowiedzenia własnej prawdy Zeira oraz historyk Ahron Bregman ujawnili tożsamość izraelskiego szpiega, co nigdy wcześniej się nie zdarzyło. Aszraf Marwan został w czerwcu 2007 r. zamordowany.

Mossad przeprowadził serię operacji wymierzonych w iracki kompleks przemysłowo-wojskowy. Zyskał w tym niezwykle cennego sojusznika – Kurdów, którzy zawsze występowali w opozycji do władz, niezależnie od tego, czy byli to Brytyjczycy, monarchia, czy w końcu republika. Domagali się najpierw własnej państwowości, a potem szerokiej autonomii. Władze w Bagdadzie od zawsze im to obiecywały, a potem, gdy zaczynały czuć się wystarczająco silne wysyłały przeciwko nim wojsko[16]. W celu nawiązania współpracy w 1965 r. oficjalna izraelska delegacja pojawiła się w obozie kurdyjskiego przywódcy Mustafy Barzaniego. Przyjazd oficerów Mossadu do Kurdystanu uznano za ogromny sukces izraelskiego wywiadu. Pierwsze spotkanie zapoczątkowało bliską współpracę, która trwała wiele lat. Barzani i kurdyjscy wodzowie przybyli też z wizytą do Izraela. Szef Mossadu, Meir Amit, i jego najbliżsi współpracownicy udali się do Kurdystanu z rewizytą. Izrael dostarczył Kurdom broń i występował w ich interesach na forach międzynarodowych. Tel Awiw uważał bowiem, że gdyby udało się stworzyć z Kurdów siłę militarną, to władze irackie musiałyby całkowicie skupić swoją uwagę na sprawach wewnętrznych, co zminimalizowałoby skalę zagrożenia Izraela ze strony Iraku.

Wykorzystując sojusz z Kurdami, Mossad przeprowadził operację pod kryptonimem „Diament", tj. porwał radziecki samolot Mig-21, najnowocześniejszy w tamtym czasie, który pod względem szybkości i zwrotności prześcigał konstrukcje zachodnie. Izraelczykom udało się zwerbować irackiego pilota, Munira Redfę (o tym, w jaki sposób autorzy piszą w rozdziale 10 i zsynchronizować jego ucieczkę Migiem z wyjazdem z Iraku całej jego rodziny. Samolot uznawany dotąd za główne zagrożenie dla zachodnich sił powietrznych w sierpniu 1967 r. znalazł się rękach Izraela. Mossad ujawnił Amerykanom tajemnice dotyczące jego konstrukcji w zamian za przekazanie informacji na temat nowego radzieckiego pocisku przeciwlotniczego S-75. Zbadanie rozwiązań technologicznych Miga-21 okazało się bardzo pomocne dla izraelskich sił powietrznych i odegrało ważną rolę podczas przygotowań do konfrontacji z arabskimi Migami, do której doszło w czerwcu 1967 r. podczas wojny sześciodniowej. Mossad pomógł Munirowi Redfie i jego rodzinie urządzić się w Izraelu, jednak Irakijczycy nie potrafili się tam zaaklimatyzować. Wobec tego zorganizowano im wyjazd z nową tożsamością do Europy Zachodniej. Jednak i tu, z dala od ojczyzny i krewnych, w otoczeniu izraelskich agentów, czuli się osamotnieni. Wyższy oficer Mossadu sformułował wówczas istotną tezę, że zbudowanie nowego życia dla agenta kulturowo obcego, poza jego własnym krajem, jest prawie niemożliwe. Wniosek ten jest dość aktualny i powinien być brany pod uwagę również przez polskie służby organizujące wyjazd i pobyt w naszym kraju afgańskim współpracownikom Polskiego Kontyngentu Wojskowego przed jego wycofaniem się z Afganistanu w 2014 r.

Mossad pokrzyżował plany irackiego dyktatora Saddama Husajna, dążącego do wyprodukowania broni jądrowej. Najpierw zabił trzech irackich fizyków jądrowych, a następnie siły powietrzne Izraela zbombardowały (7 czerwca 1981 r.) reaktor atomowy w Osirak k. Bagdadu (operacja „Opera"). Potem były prowadzone wielowątkowe działania mające na celu uniemożliwienie skonstruowania w Iraku superdziała,

[16] Krótki, ale interesujący opis relacji iracko-kurdyjskich: M. Zawadzki, *Nowy wspaniały Irak*, Warszawa 2012, W.A.B., s. 174–180.

które mogłoby być wykorzystane do ostrzału Izraela. Jeśli już mowa o niszczeniu arsenałów potencjalnych wrogów Izraela, to należy wspomnieć o skomplikowanej i precyzyjnie przeprowadzonej operacji „Sad", w której ramach nocą 5 września 2007 r. zbombardowano syryjskie instalacje jądrowe w Dayr Az-Zur, budowane przez północnokoreańskich fizyków za pieniądze irańskie (rozdział 18). Epilogiem syryjskiego programu atomowego było zabicie 2 sierpnia 2008 r. gen. Muhammada Sulejmana, doradcy prezydenta Baszara al-Asada w sprawach wojskowych, który kierował dostawami materiałów i części do reaktora atomowego oraz nadzorował prace koreańskich techników i inżynierów. Zaczął nawet planować budowę drugiego reaktora. Jego śmierć przekreśliła wszelkie spekulacje na ten temat.

Tak jak Izrael niweczył plany i projekty atomowe swoich wrogów, tak w konsekwentny sposób realizował własny program jądrowy w Dimonie na pustyni Negew i wciąż strzeże jego tajemnicy. W październiku 1986 r. została ona jednak ujawniona brytyjskiej gazecie „London Sunday Times" przez byłego pracownika Dimony Mordechaja Wanunu, który rok wcześniej został zwolniony z pracy i wyjechał z Izraela. Mossad podjął się jego porwania z Europy i sprowadzenia go do kraju (operacja pod krypt. „Kaniuk") w celu postawienia przed sądem (rozdział 15). W związku z tym podstawiono mu piękna agentkę, która go uwiodła. Izrael nie chciał jednak uprowadzać go z terytorium brytyjskiego, obawiając się konfrontacji z Margaret Thatcher i zaostrzenia stosunków dyplomatycznych. Uznano, że najlepszym miejscem do przeprowadzenia operacji będzie Rzym. Mimo ostrzeżeń ze strony brytyjskiego dziennikarza, Wanunu dał się namówić kobiecie na wspólną wycieczkę do Rzymu, skąd 30 września został porwany do Izraela. W czasie, gdy był w drodze do kraju, „Sunday Times" zaczął publikować serię artykułów z jego rewelacjami. Artykuły poparte zdjęciami i szkicami przedrukowały gazety na całym świecie.

Uwagę w omawianej publikacji zwracają rozdziały poświęcone działaniom antyterrorystycznym, począwszy od znanej z literatury, mediów i kina operacji „Gniew Boga"[17]. Jej celem była fizyczna eliminacja działaczy organizacji Czarny Wrzesień, która podczas igrzysk olimpijskich w Monachium w 1972 r. dokonała ataku terrorystycznego na izraelskich sportowców (rozdział 12). Operacja „Gniew Boga" była realizowana w państwach Europy Zachodniej i w Libanie. Zakończyła się wraz z wyeliminowaniem przywódcy Czarnego Września, Alego Hasana Salameha, w styczniu 1979 r. Zginął on w wyniku eksplozji samochodu pułapki. W międzyczasie, w marcu 1978 r., został otruty Wadi Haddad, szef Ludowego Frontu Wyzwolenia Palestyny, którego członkowie w 1976 r. uprowadzili do Ugandy samolot Air France, lecący z Tel Awiwu do Paryża. Chociaż sama operacja odbicia zakładników, przeprowadzona przez izraelską jednostkę specjalną Sajeret Matkal, jest dobrze znana (tzw. operacja „Piorun"), to niewiele wiadomo o poprzedzających ją działaniach wywiadowczych, mających na celu zdobycie informacji na temat lotniska w Entebbe k. Kampali i strzegących go sił wojskowych Ugandy.

Spektakularną porażką Mossadu zakończyła się próba zabicia we wrześniu 1997 r. Chalida Meszala, ważnego wówczas aktywisty Hamasu (rozdział 17). Finał akcji był taki, że Meszal przeżył atak izraelskiego wywiadu w Ammanie, a dla ratowania swych dwóch agentów, którzy zostali aresztowani przez jordańską policję, Izrael został

[17] Operacja „Gniew Boga" stała się tematem filmu *Monachium* (2005) w reżyserii Stevena Spielberga, z Erikiem Baną i Danielem Craigiem w rolach głównych, a wcześniej *Miecza Gideona* z 1986 r., opartego na fabule książki George'a Jonasa pt. *Monachium. Zemsta*.

zmuszony do zwolnienia z więzienia przywódcy Hamasu, Ahmeda Jasina i dwudziestu innych Palestyńczyków. Meszal zyskał ogromną popularność i stał się jednym z głównych przywódców Hamasu.

Sukcesem, choć połowicznym, okazał się finał operacji zabicia w styczniu 2010 r. w Dubaju Mahmuda Abdela Raufa al-Mabhuha, jednego z liderów Hamasu, odpowiedzialnego za dostarczanie broni tej palestyńskiej organizacji. Co prawda został on zabity w hotelowym pokoju po zaaplikowaniu mu trucizny, ale kamery rozmieszczone w hotelu i na lotnisku sfilmowały agentów, co pozwoliło odtworzyć cały przebieg operacji i ustalić wszystkich jej uczestników. Ujawnienie ich tożsamości, oczywiście fałszywej, wywołało międzynarodowy skandal, gdyż posługiwali się oni paszportami brytyjskimi, francuskimi, australijskimi, irlandzkimi i niemieckimi, wystawionymi na nazwiska żyjących obywateli tych krajów[18]. Hipokryzją nazwali autorzy książki reakcję na to państw zachodnich (m.in. wydaliły przedstawicieli Mossadu ze swoich terytoriów), ponieważ – jak piszą – używanie fałszywych lub spreparowanych dokumentów jest powszechnie stosowaną praktyką przez wszystkie tajne służby.

Michael Bar-Zohar i Nissim Mishal w sposób mało obiektywny podeszli w recenzowanej publikacji do niektórych zagadnień, zwłaszcza odnoszących się do łamania prawa międzynarodowego przez Mossad w imię narodowych interesów i bezpieczeństwa Izraela. Poza tym, mając na uwadze wrażliwość wielu innych kwestii podejmowanych w książce, starali się zachować bezstronność w opisywanej faktografii. Czy im się to udało, niech czytelnicy ocenią sami.

Książka *Mossad. Najważniejsze misje izraelskich tajnych służb* została wydana starannie. Uwagę zwraca dobra kompozycja oraz doskonały styl i narracja. Publikację wzbogacają czarno-białe i kolorowe fotografie, przypisy i wyjaśnienia umieszczone na jej końcu oraz bibliografia, indeksy nazwisk, nazw organizacji i nazw geograficznych. Jej lekturę należy polecić szczególnie funkcjonariuszom służb odpowiedzialnych za bezpieczeństwo państwa.

[18] Sprawa miała również swój polski wątek. W dniu 4 czerwca 2010 r. na lotnisku Okęcie aresztowano mężczyznę o nazwisku Uri Brodsky, ściganego w Niemczech za pomoc agentowi Mossadu Michaelowi Bodenheimerowi (uczestniczącemu w przygotowaniu operacji w Dubaju), w uzyskaniu niemieckiego paszportu. Niemcy domagały się od polskich władz jego ekstradycji, a Izrael prosił o odesłanie go jako własnego obywatela do kraju. W lipcu 2010 r. warszawski Sąd Okręgowy orzekł, że Brodsky może być przekazany do Niemiec, ale nie może być tam sądzony za szpiegostwo, tylko za poświadczenie nieprawdy i pomoc w sfałszowaniu dokumentów dla osoby, która miała brać udział w zabójstwie Mabhuha. Ostatecznie w dniu 5 sierpnia 2010 r. Sąd Apelacyjny podjął decyzję o przekazaniu Brodsky'ego Niemcom. Jeszcze w sierpniu 2010 r. prokuratura w Kolonii poinformowała o jego zwolnieniu za kaucją z prawem swobodnego podróżowania. W styczniu 2011 r. sąd niemiecki skazał Brodsky'ego na karę grzywny w wysokości 100 tys. euro za sfałszowanie niemieckiego paszportu. *Polacy złapali, a Niemcy zwolnili domniemanego agenta* [online], http://wiadomości.wp.pl [dostęp: 13 VIII 2010]; *Uri Brodsky, domniemany agent Mosadu, skazany na karę grzywny* [online], http//wiadomości.gazeta.pl [dostęp: 16 I 2011].

IV
PRZEGLĄD PRAC KONKURSOWYCH

Ogólnopolski konkurs szefa Agencji Bezpieczeństwa Wewnętrznego na najlepszą pracę licencjacką/magisterską z dziedziny bezpieczeństwa wewnętrznego państwa

Edycja 2011/2012 – wyniki konkursu

W wyniku ogłoszonego przez szefa Agencji Bezpieczeństwa Wewnętrznego konkursu dla absolwentów studiów licencjackich i magisterskich wpłynęło 36 prac obronionych w roku akademickim 2011/2012.

Komitet Konkursowy, po dokonaniu oceny nadesłanych dysertacji, zdecydował:

- nie przyznać I i II nagrody,
- III nagrodę przyznać Panu Arkadiuszowi Królowi (Wyższa Szkoła Oficerska Wojsk Lądowych, Wydział Nauk o Bezpieczeństwie) za pracę magisterską pt. *Działalność operacyjna służb specjalnych w systemie bezpieczeństwa państwa*,
- a także przyznać 2 wyróżnienia:
- Panu Maciejowi Smolakowi (Uniwersytet Marii Curie-Skłodowskiej w Lublinie, Wydział Prawa i Administracji) za pracę magisterską pt. *Formy zwalczania procederu prania brudnych pieniędzy*,
- Panu Maciejowi Musiejko (Uniwersytet Gdański, Wydział Prawa i Administracji) za pracę magisterską pt. *Zjawisko cyberterroryzmu w polskim prawie karnym*.

Edycja 2012/2013 – ogłoszenie konkursu

W listopadzie 2012 r. szef Agencji Bezpieczeństwa Wewnętrznego ogłosił konkurs na najlepszą pracę licencjacką/magisterską z dziedziny bezpieczeństwa wewnętrznego państwa obronioną w roku akademickim 2012/2013.

Celem konkursu jest promocja i upowszechnianie problematyki bezpieczeństwa wewnętrznego państwa wśród młodzieży i kadry akademickiej, zwiększenie świadomości społecznej w tym zakresie oraz profilaktyka i edukacja na rzecz bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Obszary tematyczne konkursu:

1. Służby specjalne II a III RP – studium porównawcze,
2. Rola służb specjalnych w demokratycznym państwie prawa,
3. Konstytucyjne prawa obywateli a uprawnienia polskich służb specjalnych,
4. Bezpieczeństwo Polski w XXI wieku – zagrożenia i wyzwania,
5. Czy Polsce potrzebne są służby specjalne?
6. Obraz służb specjalnych w mediach – stereotypy i uprzedzenia,
7. Służby specjalne w literaturze i sztuce.

Do konkursu uczestnicy mogą zgłosić własną pracę licencjacką lub magisterską napisaną w języku polskim i bronioną w roku akademickim 2012/2013.

Prace powinny zostać przesłane w wersji papierowej i elektronicznej (mailowej) wraz z wypełnionym formularzem zgłoszenia (plik do pobrania na oficjalnej stronie internetowej ABW).

Do pracy powinny być dołączone opinie promotora/recenzentów i ich pisemna zgoda na wykorzystanie opinii/recenzji dla celów konkursu.

Prace powinny być przesłane na adres:

Gabinet Szefa
ABW
00-993 Warszawa
ul. Rakowiecka 2a
z dopiskiem „KONKURS”

e-mail: redakcja.pbw@abw.gov.pl

Prace należy przesłać do 31 lipca 2013 r. (decyduje data stempla pocztowego).

Prace ocenia, Komitet Konkursowy powołany przez szefa ABW, który wyłoni laureatów konkursu w terminie do 30 września 2013 r. przyznając I, II oraz III miejsce, a także wyróżnienia.

Wyniki konkursu zostaną opublikowane na stronie internetowej www.abw.gov.pl. Laureaci i ich macierzyste uczelnie otrzymają pisemne powiadomienia.

Nagrody:

I miejsce – nagroda finansowa w wysokośći 3000 zł oraz publikacja pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”,

II miejsce – nagroda finansowa w wysokośći 2500 zł oraz publikacja pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”,

III miejsce nagroda – finansowa w wysokośći 2000 zł oraz publikacja pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”,

Wyróżnienia – nagroda rzeczowa, publikacja pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego”.

Wybrany fragment pracy laureata drugiej edycji konkursu szefa ABW
na najlepszą pracę licencjacką/magisterską
z dziedziny bezpieczeństwa wewnętrznego
2011/2012

Maciej Musiejko

Zjawisko cyberterroryzmu w polskim prawie karnym

Od najdawniejszych czasów rozwój techniczny wpływał na sposób życia człowieka. Obecnie, gdy nabrał on niespotykanego dotąd tempa, zmiany dokonują się niemal na naszych oczach. Postęp jest szczególnie dobrze widoczny w krajach, które wychodzą z technologicznego zapóźnienia. Jeszcze dwadzieścia lat temu komputer osobisty był urządzeniem nieosiągalnym dla większości polskiego społeczeństwa, a dostęp do internetu miały jedynie niektóre ośrodki naukowe. Obecnie komputer jest powszechnie stosowanym narzędziem pracy i rozrywki, a dostęp do szerokopasmowego internetu jest prawie tak naturalny, jak dostęp do bieżącej wody. Co więcej, z ogólnoświatowej sieci można korzystać już nie tylko siedząc przy biurku, ale też za pomocą komputerów przenośnych, a nawet telefonów komórkowych.

W ślad za postępem technicznym podąża nieustannie rozszerzające się spektrum możliwości wykorzystania istniejącej infrastruktury sieciowej. W swoich „młodzieńczych" latach internet był jedynie zbiorem statycznych stron www, w niektórych przypadkach zawierających niskiej jakości grafikę. Jego zawartość była skierowana bardziej do wąskiego grona odbiorców, niż do użytkowników masowych. Stopniowe upowszechnienie dostępu do sieci dało jednak impuls do zmian i przeistoczenia militarno-naukowego tworu (bo taki charakter miał z założenia ARPANET – protoplasta internetu) w globalną sieć wykorzystywaną do celów komercyjnych i rozrywkowych. Zaczęły powstawać sklepy internetowe (np. Amazon.com) umożliwiające dokonywanie zakupów bez zrobienia choćby kroku w stronę drzwi mieszkania. Pojawiła się możliwość nawiązywania kontaktów z ludźmi z całego świata za pośrednictwem czatów i forów dyskusyjnych. Zwykli użytkownicy dzięki temu mogą opowiedzieć o sobie lub o tym, co ich interesuje. W tym celu mogą również zaprojektować własne strony www. Papierowe wydania prasy codziennej, tygodników i innych gazet zaczęły być częściowo dostępne także w wersji elektronicznej. Banki zaoferowały swoim klientom dostęp do kont przy wykorzystaniu internetu, administracja publiczna zaś przedstawiła w tenże sposób informacje na temat swojej działalności.

Obecnie wykorzystanie internetu do celów komercyjnych poszło o krok dalej. Sklepy internetowe i serwisy aukcyjne pozwalają kupić wszystko, czego można zapragnąć – nawet produkty spożywcze. Istnieje możliwość zapłacenia rachunków (otrzymywanych e-mailem) przy korzystaniu z usług banku internetowego. Sam bank nie musi posiadać oddziałów, w których można wypłacić pieniądze, a konto można założyć on-line, wypełniając stosowny formularz. Wpływy na ów wirtualny rachunek zapewnia na przykład telepraca, w pełni dopuszczalna w świetle zapisów kodeksu pracy[1]. Zeznanie podatkowe można złożyć w postaci elektronicznej, do czego zresztą

[1] Rozdział IIb *Ustawy z dnia 26 czerwca 1974 r. Kodeks pracy* (Dz.U. z 1998 r Nr 21, poz. 94 z późn. zm.).

zachęca samo Ministerstwo Finansów. Wdrażane są również inne programy oferujące załatwianie spraw urzędowych przez internet. Także wymiar sprawiedliwości korzysta z sieci, umożliwiając złożenie pozwu w tzw. e-Sądzie[2] działającym przy Sądzie Rejonowym Lublin-Zachód w Lublinie. Niektóre uczelnie uruchamiają tzw. studia e-learningowe, proponując kształcenie się przy użyciu komputera. Rozrywkę natomiast zapewniają między innymi możliwość oglądania telewizji przez internet czy dostępna w sieci ogromna liczba gier, w tym z opcją gry wieloosobowej. Nawiązywaniu i podtrzymywaniu kontaktów towarzyskich służą portale społecznościowe, takie jak np. Facebook, na którym konto posiada ponad pół miliarda osób. Komunikatory, m.in. Skype, pozwalają w czasie rzeczywistym widzieć i rozmawiać z osobą na innym kontynencie. Rozwój sieci internet sprawił, że człowiek XXI wieku nie musi już praktycznie wychodzić z domu.

Oczywiście globalna sieć komputerowa nie jest tworem idealnym, pozbawionym zagrożeń. W równie wysokim stopniu jak działalności legalnej, internet służy czynom zakazanym przez prawo – m.in. dystrybucji pornografii dziecięcej, sprzedaży niedostępnych w kraju środków farmakologicznych, szpiegostwu, hackingowi, oszustwom internetowym. Przestępczość w sieci nie ogranicza się tylko do dokonywania „tradycyjnych" czynów zabronionych przez prawo przy pomocy nowego narzędzia (np. oszustw na aukcjach internetowych), ale zdołała wykształcić nowe, mające wyłącznie wirtualny charakter, przestępstwa, jak choćby hackerstwo. Co więcej, przestrzeń wirtualna stała się polem rywalizacji międzynarodowej – światowe mocarstwa starają się rozszerzyć swoją strefę wpływów na cyberprzestrzeń i wykorzystywać ją do uzyskania przewagi nad swoimi rywalami. Coraz częstsze są akcje grup hackerów kierowane przeciwko stronom i serwerom państwowym. Oficjalnie sprawcy tych czynów są potępiani i piętnowani, nieoficjalnie zaś uzyskują wsparcie rodzimych agend rządowych. Niektórzy badacze i wojskowi wskazują nawet, że cyberprzestrzeń jest nowym rodzajem pola walki zbrojnej.

W takiej sytuacji nie powinna dziwić wzmożona aktywność państw i organizacji międzynarodowych w sferze szeroko rozumianego cyberbezpieczeństwa. W dziedzinie wojskowości na przykład normą staje się powoływanie do życia oddziałów wojskowych specjalizujących się w zabezpieczaniu działań armii oraz prowadzeniu walki w cyberprzestrzeni. Prym w tej kwestii wiodą Stany Zjednoczone, dysponujące takimi oddziałami w niemal każdym rodzaju sił zbrojnych oraz wspólnym dla nich dowództwem (USCYBERCOM[3]). Podobne inicjatywy podjęły już między innymi armia brytyjska, niemiecka, chińska, a także polska – ta ostatnia pod postacią Centrum Bezpieczeństwa Cybernetycznego w Białobrzegach. W strukturach polskich sił zbrojnych planowane jest utworzenie „batalionów cyfrowych", których zadaniem będzie zapewnienie bezpieczeństwa armii[4]. Oprócz tego typu inicjatyw podejmowane są również działania w ramach międzynarodowej współpracy militarnej. Pamiętając o wydarzeniach z przełomu kwietnia i maja 2007 r. w Estonii, powołano do życia Centrum Doskonalenia Obrony Cybernetycznej[5], które w październiku 2008 r. uzyskało akredytację NATO i stało się międzynarodową organizacją wojskową. Wagę problemu zauważył nie tylko

[2] www.e-sad.gov.pl [dostęp: 17 III 2012].

[3] Z ang. *United States Cyber Command*.

[4] „Tygodnik BBN" 14–20 stycznia 2011 r., nr 16, s. 6, www.bbn.gov.pl/portal/pl/561/2446/ tygodnik_ BBN.html [dostęp: 4 II 2011].

[5] Z ang. *Cooperative Cyber Defence Centre of Excellence* (CCD COE).

sektor wojskowy – coraz częściej jest ona dostrzegana przez najważniejsze organizacje międzynarodowe[6]. Zarówno ONZ, jak i Unia Europejska stworzyły ośrodki, które mają zajmować się bezpieczeństwem cyberprzestrzeni – odpowiednio Światową Agencję ds. Cyberbezpieczeństwa (GCA)[7] oraz Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA). Swoje strategie cyberbezpieczeństwa przygotowały już między innymi Stany Zjednoczone, Kanada, Francja, Niemcy, a nawet Estonia. W Polsce natomiast tworzony jest Rządowy Program Ochrony Cyberprzestrzeni (RPOC), którego realizacja ma zwiększyć zdolność zapobiegania niebezpieczeństwom płynącym ze strony cyberprzestrzeni oraz ich zwalczania. Wyraźnie więc widać, że zagrożenia, jakie mogą się wiązać z cyberprzestrzenią, zostały dostrzeżone i poważnie potraktowane przez społeczność międzynarodową.

Do największych zagrożeń XXI wieku można zaliczyć także terroryzm. Zamachy w Nowym Yorku, Madrycie i Londynie pokazały, że nikt nie może czuć się w pełni bezpiecznym. Nawet obywatele najbardziej rozwiniętych i najpotężniejszych światowych mocarstw muszą być przygotowani na akty przemocy skierowane przeciwko nim. Choć do tej pory przemoc ta przybierała formę zamachów bombowych, porwań i egzekucji niewinnych osób, to naiwnością byłoby wierzyć, że terroryści nie będą korzystać z nowych technologii. Rozwój i wzrost znaczenia cyberprzestrzeni otwiera przed nimi nowe możliwości – zarówno organizowania zamachów, jak i ich przeprowadzania. Cyberterroryzm jest więc połączeniem obu wymienionych powyżej zagrożeń.

Z uwagi na poruszone kwestie potrzebne wydaje się przeanalizowanie polskich regulacji prawnych odnoszących się do cyberterroryzmu. Przemawia za tym również fakt, iż w skład Rządowego Programu Ochrony Cyberprzestrzeni będzie wchodzić wiele działań legislacyjnych, które mają stanowić pierwszy etap w procesie zapewnienia bezpieczeństwa cyberprzestrzeni. Niniejsza praca stanowi próbę przeanalizowania tych regulacji w zakresie dotyczącym prawa karnego materialnego. Autor będzie starał się znaleźć odpowiedź na pytanie, czy polskie prawo karne odnosi się do zjawiska cyberterroryzmu, a jeśli tak, to w jaki sposób. Niezbędne będzie wyjaśnienie, czym jest cyberterroryzm. Ponadto celem publikacji jest wskazanie ewentualnych luk w prawie i wysunięcie postulatów *de lege ferenda*. Posłuży do tego analiza dogmatyczna treści aktów prawnych oraz krytyka i analiza literatury.

Istnieje stosunkowo niewiele opracowań na temat cyberterroryzmu w kontekście prawnym, toteż konieczne jest odwołanie się do literatury spoza dziedziny prawa, głównie dotyczącej bezpieczeństwa państwa, ale również do źródeł o charakterze technicznym czy odnoszących się do kwestii lingwistycznych. Z tego powodu część pracy traktuje o kwestiach pozaprawnych, co jest zabiegiem niezbędnym, by w sposób możliwie jak najbardziej kompleksowy oddać problematykę dotyczącą cyberterroryzmu. Mała liczba źródeł implikowała również badawczy charakter pracy, stąd znaczna część twierdzeń w niej zawartych stanowi pogląd autora.

---

[6] Szerzej: K. Liedel, *Cyberbezpieczeństwo – wyzwanie przyszłości. Działania społeczności międzynarodowej,* w: *Bezpieczeństwo w XXI wieku. Asymetryczny świat*, K. Liedel, P. Piasecka, T.R. Aleksandrowicz (red.), Warszawa 2011, Difin.

[7] *Global Cybersecurity Agenda* – wchodzi ona w skład Międzynarodowego Związku Telekomunikacyjnego.

Przepisy penalizujące ataki w cyberprzestrzeni

Poszukiwanie przepisów odnoszących się do cyberterroryzmu należy rozpocząć w rozdziale XXXIII kodeksu karnego, w którym wymienione są przestępstwa przeciwko ochronie informacji. W jego skład wchodzą zarówno przepisy chroniące informację w szerokim tego słowa rozumieniu, jak i bezpieczeństwo danych, systemów oraz sieci.

Artykuły 265 i 266 kk penalizują ujawnienie oraz wykorzystanie informacji niejawnych w sposób naruszający zapisy ustawy o ochronie informacji niejawnych[8]. Choć ze względu na górną granicę zagrożenia karnego przestępstwo z art. 265 kk można by w niektórych przypadkach uznać za przestępstwo o charakterze terrorystycznym[9], to jednak wziąwszy pod uwagę czynność sprawczą (ujawnienie lub wykorzystanie wbrew przepisom ustawy informacji niejawnych o klauzuli „tajne" lub „ściśle tajne") trudno jest uznać je za akt cyberterroryzmu. Artykuł 266 kk natomiast nie spełnia nawet wymogu zagrożenia karą pięciu lat pozbawienia wolności. W związku z tym dalsza analiza tych artykułów jest bezcelowa.

Kolejnym przepisem dotyczącym przedmiotowej tematyki jest artykuł 267 kk, który stanowi:

> „Art. 267 § 1. Kto bez uprawnienia uzyskuje dostęp do informacji dla niego nieprzeznaczonej, otwierając zamknięte pismo, podłączając się do sieci telekomunikacyjnej lub przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.
> § 2. Tej samej karze podlega, kto bez uprawnienia uzyskuje dostęp do całości lub części systemu informatycznego.
> § 3. Tej samej karze podlega, kto w celu uzyskania informacji, do której nie jest uprawniony, zakłada lub posługuje się urządzeniem podsłuchowym, wizualnym albo innym urządzeniem lub oprogramowaniem.
> § 4. Tej samej karze podlega, kto informację uzyskaną w sposób określony w § 1–3 ujawnia innej osobie.
> § 5. Ściganie przestępstwa określonego w § 1–4 następuje na wniosek pokrzywdzonego".

Przepis ten chroni poufność informacji w szerokim zakresie – dotyczy informacji zapisanej zarówno w tradycyjny sposób (*otwierając zamknięte pismo*), przekazywanej na odległość (*podłączając się do sieci telekomunikacyjnej*) czy też zawartej na nośnikach nowoczesnego typu (*przełamując albo omijając elektroniczne, magnetyczne, informatyczne lub inne szczególne jej zabezpieczenie*). W literaturze zwraca się uwagę na to, że przepis ten jest także środkiem mogącym służyć do walki z hackingiem[10].

---

[8] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r. Nr 182, poz. 1228).

[9] „Art. 115 § 20 Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu:
1) poważnego zastraszenia wielu osób,
2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności,
3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej
– a także groźba popełnienia takiego czynu".

[10] A. Suchorzewska, *Ochrona prawna systemów informatycznych wobec zagrożenia cyberterroryzmem,* Warszawa 2010, Wolters Kluwer Business, s. 211.

W kontekście cyberterroryzmu szczególnie interesujący wydaje się § 2 tego przepisu. Został on wprowadzony ustawą[11], która miała za zadanie m.in. implementację *Decyzji ramowej Rady 2005/222/WSiSW* w sprawie ataków na systemy informatyczne i dostosowanie polskich przepisów do *Konwencji o cyberprzestępczości*. Prócz zmiany dość archaicznych zapisów art. 267 § 1 kk (we wcześniejszej wersji była mowa o podłączaniu się *do przewodu służącego do przekazywania informacji*), za przestępstwo zostało uznane samo uzyskanie dostępu do całości lub części systemu informatycznego. Jak wskazano w projekcie ustawy, *czyn taki może polegać np. na wprowadzeniu do systemu informatycznego oprogramowania, które umożliwia sprawcy przejęcie zdalnej kontroli nad komputerem, w celu wykonania z jego wykorzystaniem zmasowanych ataków na określone strony internetowe. Sprawca w takim przypadku nie działa w celu uzyskania informacji znajdującej się w zasobach przejętego systemu lub dostępu do niej, lecz w celu przejęcia kontroli nad systemem jako narzędziem do bezprawnego wykorzystywania*[12]. Mowa zatem o tworzeniu Botnetu[13], który mógłby służyć przeprowadzeniu ataku typu DDoS, a stąd już tylko krok do cyberataków. Niemniej jednak uzyskanie dostępu do informacji lub systemu nie spełnia kryteriów z art. 115 § 20, toteż nie może ono stanowić przestępstwa o charakterze terrorystycznym.

Konieczne wydaje się wyjaśnienie pojęcia „system informatyczny", które pojawiło się w art. 267 kk i występuje także w innych przepisach. Pomimo ujednolicenia terminologii informatycznej i wprowadzenia do ustaw terminu „system teleinformatyczny" ustawodawca posłużył się innym określeniem, nie zdefiniowanym ustawowo. Definicję „system informatyczny" można natomiast znaleźć w art. 1 *Konwencji o cyberprzestępczości*. Zgodnie z nią jest to *każde urządzenie lub grupa wzajemnie połączonych lub związanych ze sobą urządzeń, z których jedno lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych*. Ta definicja zasadniczo zgadza się z definicją „systemu teleinformatycznego"[14], z tą różnicą, że nie obejmuje funkcji wysyłania i odbierania danych. Podobnego zdania jest A. Baworowski, który twierdzi, że pojęcie „system teleinformatyczny" jest szersze od pojęcia „system informatyczny", gdyż system teleinformatyczny oprócz przetwarzania i przechowywania danych będzie służył także do ich przesyłania i odbierania. Jak zauważa, *każdy system teleinformatyczny jest systemem informatycznym, lecz nie każdy system informatyczny jest systemem teleinformatycznym*[15].

---

[11] *Ustawa z dnia 24 października 2008 r. o zmianie ustawy Kodeks karny oraz niektórych innych ustaw* (Dz.U. z 2008 r. Nr 214, poz. 1344).

[12] *Uzasadnienie projektu ustawy z dnia 24 października 2008 r. o zmianie ustawy Kodeks karny oraz niektórych innych ustaw.*

[13] *Botnet – sieć zawirusowanych i przejętych komputerów, które raportują swojemu właścicielowi i są zarządzane w czasie rzeczywistym przez serwer kontrolujący. Botnety najczęściej są wykorzystywane do przeprowadzania zmasowanych ataków typu DDoS, rozsyłania spamu itp.* Źródło: http://www.orange.pl/kid,4002354750,id,4002365117,title,slownikB,article.html [dostęp: 12 V 2012].

[14] W rozumieniu przepisów *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* system teleinformatyczny jest to zespół współpracujących ze sobą urządzeń informatycznych i oprogramowania zapewniający przetwarzanie, przechowywanie, a także wysyłanie i odbieranie danych przez sieci telekomunikacyjne za pomocą telekomunikacyjnego urządzenia końcowego właściwego dla danego rodzaju sieci.

[15] A. Baworowski, *Problemy wykładni przepisów art. 268 § 2, 269 § 2, 267 i 269a kk po nowelizacjach z 2008 r.,* „Diariusz Prawniczy" 2009, nr 10/11.

Następnym przepisem służącym ochronie informacji jest art. 268 kk:

„Art. 268 § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa lub zmienia zapis istotnej informacji albo w inny sposób udaremnia lub znacznie utrudnia osobie uprawnionej zapoznanie się z nią, podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do lat 2.

§ 2. Jeżeli czyn określony w § 1 dotyczy zapisu na informatycznym nośniku danych, sprawca podlega karze pozbawienia wolności do lat 3.

§ 3. Kto, dopuszczając się czynu określonego w § 1 lub 2, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 4. Ściganie przestępstwa określonego w § 1–3 następuje na wniosek pokrzywdzonego".

Nie chodzi tu jednak o każdą informację, lecz o taką, która jest w pewien sposób istotna. Jak zauważa M. Kalitkowski, kwestia wagi informacji zależy od jej znaczenia dla jej dysponenta oraz celu, któremu służyła lub miała służyć[16]. Karalne jest zatem działanie, które udaremnia lub utrudnia zapoznanie się z zapisem istotnej informacji, w szczególności poprzez zniszczenie, uszkodzenie, usunięcie lub zmianę tego zapisu. Poprzez udaremnienie zapoznania się z informacją należy rozumieć *całkowite uniemożliwienie* (...) *zrozumienia sensu zapisu tej informacji*. O znacznym utrudnieniu można mówić natomiast wtedy, gdy do odczytania informacji jest niezbędny znaczny nakład czasu lub wysiłku, a także, gdy informacja jest niekompletna lub znacznie zniekształcona[17]. Typ kwalifikowany tego przestępstwa został zawarty w paragrafie drugim art. 268, który odnosi się do zapisu istotnej informacji na informatycznym nośniku danych. Zgodnie z ustawą o informatyzacji „informatyczny nośnik danych" to *materiał lub urządzenie służące do zapisywania, przechowywania i odczytywania danych w postaci cyfrowej lub analogowej*. Jako przykładowe informatyczne nośniki danych można wskazać dyskietki, płyty CD, DVD, Blu-ray, dyski twarde, pamięci flash, taśmy oraz dyski magnetyczne. Udaremnienie lub utrudnienie zapoznania się z informacjami przechowywanymi na nośniku informatycznym może zostać dokonane w taki sam sposób, jak w przypadku informacji zawartych na nośniku nieinformatycznym (np. poprzez ich uszkodzenie lub choćby schowanie), ale również w sposób charakterystyczny tylko dla nich. W. Wróbel jako przykład podaje wprowadzenie do komputera programu blokującego możliwość zapoznania się z treścią poczty elektronicznej czy korzystania z bazy danych[18]. Także M. Kalitkowski zauważa możliwość wprowadzenia do systemu wirusa komputerowego w celu uniemożliwienia dostępu do informacji. W przypadku, gdy taki czyn wywoła znaczną szkodę majątkową[19], zagrożenie karne wzrasta do pięciu lat pozbawienia wolności, co wiąże się z możliwością uznania go za przestępstwo o charakterze terrorystycznym. Tym samym art. 268 kk może w odpowiednich okolicznościach (np. w przypadku utrudnienia lub uniemożliwienia zapoznania się z istotną informacją, gdy została ona zapisana na informatycznym nośniku danych lub w przypadku spowodowania znacznej szkody majątkowej) służyć karaniu aktów cyberterroryzmu.

---

[16] *Kodeks karny. Komentarz*, M. Filar (red.), Warszawa 2010, LexisNexis, s. 1146.

[17] *Kodeks karny. Część szczególna,* t. 2, A. Zoll (red.), Warszawa 2008, Wolters Kluwer Polska, s. 1300.

[18] Tamże, s. 1301.

[19] Zgodnie z art. 115 § 5 i § 7 o znacznej szkodzie majątkowej można mówić wtedy, gdy jej wartość przekroczy 200 000 złotych.

Jednym z przepisów dodanych w celu dostosowania regulacji kodeksu karnego do postanowień *Konwencji o cyberprzestępczości* jest art. 268a kk. Jak wskazuje B. Kunicka-Michalska, stanowi on o jednej z postaci sabotażu komputerowego. Przestępstwo to jest w jej opinii ujęte w kilku odrębnych przepisach kodeksu karnego, jego postaci zaś są opisane także w artykułach 269 kk oraz 269a kk[20].

W obecnym brzmieniu przepis ten stanowi, że:

„Art. 268a § 1. Kto, nie będąc do tego uprawnionym, niszczy, uszkadza, usuwa, zmienia lub utrudnia dostęp do danych informatycznych albo w istotnym stopniu zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności do lat 3.

§ 2. Kto, dopuszczając się czynu określonego w § 1, wyrządza znaczną szkodę majątkową, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.

§ 3. Ściganie przestępstwa określonego w § 1 lub 2 następuje na wniosek pokrzywdzonego".

Dobrem chronionym przez ten przepis są dane informatyczne, ale można tu zauważyć pewne podobieństwo do art. 268 kk. Podobnie jak zapis informacji, tak i dane są tu chronione przed zniszczeniem, uszkodzeniem, usunięciem lub zmianą, a także utrudnieniem dostępu do nich. W istocie informacje zapisane na informatycznym nośniku danych można utożsamiać z danymi informatycznymi, co zdaje się potwierdzać takie samo zagrożenie karne w art. 268 § 2 i 268a § 1 kk. Wobec braku definicji legalnej „danych informatycznych" wyjaśnienia tego terminu należy szukać u źródła jego powstania. Konwencja o cyberprzestępczości rozumie pod tym pojęciem *dowolne przedstawienie faktów, informacji lub pojęć w formie właściwej do przetwarzania w systemie komputerowym, łącznie z odpowiednim programem powodującym wykonanie funkcji przez system informatyczny*. Oprócz działań przeciwko danym informatycznym wspomnianych w pierwszej części przepisu, art. 268a kk przewiduje również karalność zakłóceń w istotnym stopniu lub uniemożliwienia automatycznego przetwarzania, gromadzenia lub przekazywania danych. Przetwarzaniem danych informatycznych według M. Dąbrowskiej-Kardas i P. Kardasa jest *opracowywanie za pomocą maszyn cyfrowych dużych ilości danych*[21]. Jak zauważa P. Kozłowska-Kalisz, o automatycznym charakterze przetwarzania można mówić wtedy, gdy odbywa się ono za pomocą urządzeń sterujących, bez niczyjej ingerencji, bądź z ograniczonym udziałem czynnika ludzkiego[22]. „Gromadzenie" to sposób koncentracji danych informatycznych, ich archiwizacja, umieszczanie w jednym pliku, „przekazywanie" zaś jest właściwie tożsame z „przesyłaniem", którym to terminem posługiwano się w poprzedniej wersji przepisu[23]. Opis działania sprawcy, w kontekście cech systemów informatycznych i teleinformatycznych, zdaje się sugerować, że karze podlegają także działania skierowane przeciwko systemom i sieciom. Artykuł 268a kk nie zawiera wskazania, w jaki sposób miałoby dojść do zakłócenia lub uniemożliwienia automatycznego przetwarzania danych. Stąd wniosek, że chodzi o jakiekolwiek działanie, np. uszkodzenie urządzeń, odcięcie

[20] *Kodeks karny. Część szczególna. Komentarz do artykułów 222–316,* A. Wąsek, R. Zawłocki (red.), Warszawa 2010, C.H. Beck, s. 720.

[21] *Kodeks karny. Część szczególna*, t. 3, A. Zoll (red.), Warszawa 2008, Wolters Kluwer Polska, s. 327.

[22] *Kodeks Karny. Praktyczny Komentarz,* M. Mozgawa (red.), Warszawa 2007, Wolters Kluwer Polska, s. 523.

[23] *Kodeks karny*, t. 3, A. Zoll (red.), s. 328.

dopływu prądu czy wprowadzenie wirusa komputerowego[24]. Ważne jest natomiast, aby skutkiem oddziaływania było uniemożliwienie automatycznego przetwarzania danych albo co najmniej zakłócenie go w istotnym stopniu. Zgodnie z definicją słownikową „istotny" oznacza tyle co „duży, znaczny"[25], zatem chodzi o zakłócenie poważne, na dużą skalę, niemal uniemożliwiające prawidłowe działanie. Tym samym karze nie podlega takie działanie sprawcy, które nie wywołuje zbyt dotkliwych skutków. Analogicznie do art. 268 kk, jeśli skutkiem czynu opisanego w paragrafie pierwszym będzie znaczna szkoda majątkowa, to sprawca podlega karze do pięciu lat pozbawienia wolności. Rozwiązanie takie czyni art. 268a kk kolejnym narzędziem z cyberterroryzmem.

Istotnym zagadnieniem jest problem relacji między przepisami zawartymi w artykułach 268 i 268a kk. W kwestii tej doktryna nie jest zgodna i proponuje różne rozwiązania. Z jednej strony art. 268 kk jest uznawany za *lex specialis* wobec art. 268a kk (tego zdania jest m.in. W. Wróbel) w sytuacji, gdy dane będą nośnikiem istotnej informacji. Inne stanowisko prezentuje B. Kunicka-Michalska sugerując, iż art. 268a kk jako *lex consumens* wyłączy stosowanie art. 268 kk. A. Suchorzewska natomiast wskazuje na pojawiające się w literaturze postulaty, aby usunąć art. 268 § 2 kk, gdyż zakres jego penalizacji został pochłonięty przez 268a kk[26].

W kontekście ochrony infrastruktury krytycznej, która jest najprawdopodobniejszym celem ataku cyberterrorystów, wyróżnia się kolejny przepis:

> „Art. 269 § 1. Kto niszczy, uszkadza, usuwa lub zmienia dane informatyczne o szczególnym znaczeniu dla obronności kraju, bezpieczeństwa w komunikacji, funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego albo zakłóca lub uniemożliwia automatyczne przetwarzanie, gromadzenie lub przekazywanie takich danych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
>
> § 2. Tej samej karze podlega, kto dopuszcza się czynu określonego w § 1, niszcząc albo wymieniając informatyczny nośnik danych lub niszcząc albo uszkadzając urządzenie służące do automatycznego przetwarzania, gromadzenia lub przekazywania danych informatycznych".

Łatwo można dostrzec podobieństwa między tym przepisem a przepisem dotyczącym przestępstwa z artykułu 268a kk. W obu przypadkach przedmiotem ochrony są dane informatyczne, a znamiona określające czynność sprawczą są identycznie niemalże ujęte. Podobieństwo to może uzasadniać koncepcję B. Kunickiej-Michalskiej o „rozbiciu" przepisu odnoszącego się do przestępstwa sabotażu komputerowego na kilka przepisów. Niemniej jednak istnieją cechy w znaczący sposób odróżniające art. 269 kk od art. 268a kk. Przede wszystkim art. 269 kk chroni jedynie te dane, które cechują się szczególnym znaczeniem dla:

a) obronności kraju,
b) bezpieczeństwa w komunikacji,

---

[24] Przykłady za: *Kodeks karny...*, A. Wąsek, R. Zawłocki (red.), s. 1177.

[25] Zob. http://sjp.pwn.pl/szukaj/istotny [dostęp: 7 III 2012].

[26] D. Harbat, *Ochrona informacji w kodeksie karnym na tle postanowień „Konwencji o cyberprzestępczości"*, w: *Zmiany w polskim prawie karnym po wejściu w życie kodeksu karnego z 1997 roku,* T. Bojarski, K. Nazar, A. Nowosad (red.), Lublin 2006, Wydawnictwo Uniwersytetu Marii Curie-Skłodowskiej, s. 302.

c) funkcjonowania administracji rządowej, innego organu państwowego lub instytucji państwowej albo samorządu terytorialnego.

W pewnym stopniu wyliczenie to pokrywa się z definicją infrastruktury krytycznej z art. 3 pkt. 2 *Ustawy o zarządzaniu kryzysowym*, art. 269 kk nie chroni jednak wszystkich systemów w niej wymienionych. Choć może się wydawać, że takie dane znajdują się wyłącznie w posiadaniu państwa, to jednak należy zauważyć, że przestępstwo to może dotyczyć danych informatycznych znajdujących się w rękach prywatnych – np. danych zawartych w komputerze pokładowym samolotu pasażerskiego. Ustawodawca przewidział różne formy popełnienia przestępstwa:

a) niszczenie, uszkadzanie, usuwanie, zmienianie danych,
b) zakłócanie lub uniemożliwianie automatycznego przetwarzania, gromadzenia lub przekazywania danych,
c) niszczenie lub wymiana informatycznego nośnika danych,
d) niszczenie lub uszkadzanie urządzeń służących do automatycznego przetwarzania, gromadzenia lub przekazywania danych.

Działania wymienione w punkcie „a" są analogiczne do tych wymienionych w art. 268a § 1 kk, z tą jednak różnicą, że brak wśród nich utrudniania dostępu do danych. Węższy zakres kryminalizacji w tym przypadku wydaje się być przeoczeniem ustawodawcy.

Kolejną różnicą jest objęcie karalnością zakłócania automatycznego przetwarzania, gromadzenia lub przekazywania danych, bez względu na to, jak istotne skutki ono wywoła. Stanowi to znaczne rozszerzenie kręgu działań podlegających karze. Paragraf drugi zakłada, że karze podlega sprawca, który popełnił czyn opisany w paragrafie pierwszym, poprzez wskazane działania skierowane przeciwko nośnikowi danych informatycznych lub urządzeniu służącemu do ich automatycznego przetwarzania, gromadzenia lub przekazywania. Nie budzi wątpliwości to, że fizyczne niszczenie i uszkadzanie nośników danych lub urządzeń wchodzi w zakres regulacji art. 269 § 2 kk. Niemniej jednak A. Baworowski zauważa, że również ingerencja w procesy inicjowane przez oprogramowanie może doprowadzić do uszkodzenia czy nawet zniszczenia urządzenia[27]. Właśnie taka niefizyczna destrukcja może być aktem cyberterroryzmu. Zważywszy na to, że górna granica zagrożenia karnego przekracza wymagane pięć lat pozbawienia wolności, artykuł 269 kk należy zaliczyć do grona przepisów penalizujących cyberterroryzm.

Przyjmuje się, że art. 269 kk stanowi *lex specialis* wobec art. 268a kk. Wydaje się, że taka sama relacja zachodzi również między nim a art. 268 kk. Z uwagi na specyficzny charakter danych możliwy jest kumulatywny zbieg przepisów z artykułami 173, 174 oraz 165 kk. W opinii autora także art. 140 kk może pozostawać w zbiegu kumulatywnym z art. 269 kk.

Przepisem, który może budzić problemy interpretacyjne jest art. 269a kk. Celem jego wprowadzenia była pełna realizacja założeń art. 5 *Konwencji o cyberprzestępczości* poprzez wypełnienie pewnej luki w zakresie penalizacji dokonywanej przez art. 269 i 287 kk – ten pierwszy odnosi się wyłącznie do określonych danych, drugi zaś nie dotyczy czynów popełnionych w innym celu, niż tylko z chęci osiągnięcia korzy-

[27] Szerzej zob. A. Baworowski, *Problemy wykładni przepisów..*, s. 75.

ści majątkowej[28]. Wobec takiego stanu rzeczy do kodeksu karnego dodano art. 269a o następującym brzmieniu:

> „Art. 269a. Kto, nie będąc do tego uprawnionym, przez transmisję, zniszczenie, usunięcie, uszkodzenie, utrudnienie dostępu lub zmianę danych informatycznych, w istotnym stopniu zakłóca pracę systemu komputerowego lub sieci teleinformatycznej, podlega karze pozbawienia wolności od 3 miesięcy do lat 5".

Karze podlega sprawca, który w istotny sposób zakłóci pracę systemu komputerowego lub sieci teleinformatycznej. Obok działań wymienionych w poprzednich przepisach pojawia się novum – zakłócanie działania (systemu lub sieci) poprzez transmisję danych. „Transmisja danych" to ich przesyłanie poprzez sieć do oraz z systemu (a także wewnątrz niego). Nadmierna transmisja danych może zakłócić działanie sieci („zapychając" ją) oraz systemu (wykorzystując całe dostępne zasoby pamięci i mocy obliczeniowej), co odpowiada *mail bombingowi* i atakom DDoS. Warto zauważyć, że działanie sprawcy musi dotyczyć danych informatycznych, a nie procesów ich dotyczących. Skutki oddziaływania na te dane muszą natomiast doprowadzić do istotnego zakłócenia pracy systemu lub sieci. Wydaje się zatem, że w art. 269a kk chodzi (za wyjątkiem transmisji) o dane mające szczególne znacznie dla działania systemów i sieci, tj. o pliki systemowe, ustawienia konfiguracyjne sprzętu itd.

Przedmiotem ochrony jest prawidłowe funkcjonowanie sieci teleinformatycznych i systemów komputerowych. Użycie sformułowania „system komputerowy" znacznie komplikuje prawidłowe zrozumienie art. 269a kk. O ile „system teleinformatyczny" posiada definicję legalną w ustawie, a „system informatyczny" w *Konwencji o cyberprzestępczości*, o tyle pojęcie „system komputerowy" nie występuje w polskim prawie karnym. W. Wróbel nie dostrzega dostatecznych racji, aby odróżniać pojęcie „system komputerowy" od terminu „system informatyczny". Podobnego zdania jest B. Kunicka-Michalska wskazująca na jego interpretację w myśl *Konwencji*, której rozwiązania art. 269a kk ma przecież wprowadzać do polskiego systemu prawnego. Trudno w tym przypadku posądzać ustawodawcę o pomyłkę, skoro ustawa ujednolicająca zmieniła treść sąsiednich przepisów, pozostawiła natomiast określenia „system komputerowy" oraz „sieć teleinformatyczna", co oznacza, że wolą ustawodawcy było odróżnienie go od innych systemów. Konieczne jest zatem ustalenie, czym jest system komputerowy i jaka jest różnica między nim a systemem informatycznym i teleinformatycznym. Wyjątkowo trafna jest uwaga B. Kunickiej-Michalskiej, że system komputerowy jest systemem informatycznym, w którym rolę „urządzenia" pełni komputer. Za taką interpretacją przemawia zarówno geneza przepisu, jak i działania, które mogą spowodować zakłócenie funkcjonowania systemu informatycznego. Systemem komputerowym w takim rozumieniu byłby zatem *każdy komputer lub grupa wzajemnie połączonych lub związanych ze sobą komputerów, z których jeden lub więcej, zgodnie z programem, wykonuje automatyczne przetwarzanie danych*. Być może zamysłem ustawodawcy było posłużenie się przymiotnikiem „komputerowy" w powszechnym tego słowa rozumieniu. Odróżniałoby to działania przeciwko komputerom osobistym (które prócz przetwarzania danych służą także uzyskiwaniu dostępu do informacji) od tych, podejmowanych przeciw tak złożonym urządzeniom, jak superkomputery, czy rozbudowanym systemom, których zadaniem jest przetwarzanie ogromnych ilości danych.

[28] Uzasadnienie projektu ustawy z dnia 18 marca 2004 r. o zmianie ustawy *Kodeks karny*, ustawy *Kodeks postępowania karnego* oraz ustawy *Kodeks wykroczeń*.

Odchodząc od zagadnień interpretacyjnych, należy zwrócić uwagę na przewidziane zagrożenie karne – podobnie jak w przypadku art. 268 § 3 oraz 268a § 2 kk wynosi ono od trzech miesięcy do pięciu lat pozbawienia wolności. Jednocześnie warto zauważyć, że art. 269a kk jako *lex consumens* wyłącza stosowanie wspomnianych przepisów, ale jednocześnie sam może być wyłączony przez art. 269 kk stanowiący wobec niego *lex specialis*. Skutkiem tego art. 269a kk jawi się jako podstawowy przepis zwalczający akty terrorystyczne w cyberprzestrzeni.

Wspomniany wcześniej artykuł 287 kk jest przepisem umiejscowionym w rozdziale XXXV dotyczącym przestępstw przeciwko mieniu. W doktrynie zyskał on nazwę oszustwa komputerowego, w skutek połączenia określenia, jakim opisuje się to przestępstwo w paragrafie i metod działania sprawcy.

> „Art. 287 § 1. Kto, w celu osiągnięcia korzyści majątkowej lub wyrządzenia innej osobie szkody, bez upoważnienia, wpływa na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub zmienia, usuwa albo wprowadza nowy zapis danych informatycznych, podlega karze pozbawienia wolności od 3 miesięcy do lat 5.
> § 2. W wypadku mniejszej wagi, sprawca podlega grzywnie, karze ograniczenia wolności albo pozbawienia wolności do roku.
> § 3. Jeżeli oszustwo popełniono na szkodę osoby najbliższej, ściganie następuje na wniosek pokrzywdzonego."

Dobrem chronionym przez ten przepis jest mienie, ale, jak zauważa A. Suchorzewska, wnioskując ze znamion przestępstwa i kontekstu ustawowego, chodzi o *zbiorczą nazwę dla wszelkich praw majątkowych, których potwierdzeniem (dowodem istnienia) jest odpowiedni zapis w systemie gromadzącym, przetwarzającym lub przesyłającym automatycznie dane informatyczne albo mienie, z którym związany jest taki zapis*[29]. Z racji takiego ujęcia przedmiotu przestępstwa art. 287 kk obejmuje swą ochroną przede wszystkim własność oraz inne prawa rzeczowe (również obligacyjne) do mienia, które zostały wyrażone na nośniku informacji[30]. Jako przykład mienia można więc podać zapis stanu konta na rachunku bankowym, skład portfela inwestycyjnego prowadzonego przez dom maklerski, ale również kolekcję plików muzycznych przechowywaną na dysku twardym czy też aktualnie pisaną publikację, tworzoną grafikę albo komponowany utwór. Działanie sprawcy opisane w dyspozycji analizowanego przepisu polega na wpływaniu na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych lub ingerowaniu (zmienianiu, usuwaniu albo wprowadzaniu nowego zapisu) w dane informatyczne. Wpływanie takie, według M. Dąbrowskiej-Kardas i P. Kardasa, może się przejawiać we wszystkich formach zakłócania procesu, utrudnianiu jego przebiegu, uniemożliwianiu rozpoczęcia, przebiegu i zakończenia go, a także zniekształceniu tego procesu lub jego wyników[31]. Ze względu na znamię celu przestępstwo z art. 287 kk można by podzielić, co często czyni doktryna, na dwie odmiany – oszustwo komputerowe (mające na celu osiągnięcie korzyści majątkowej) oraz na szkodnictwo komputerowe (za cel stawiające sobie wyrządzenie innej osobie szkody). Choć osiągnięcie korzyści majątkowej może nosić cechy czynności przygotowawczej do aktu cyberterroryzmu, to jednak w kontekście popełnienia takiego aktu ważniejsze wydaje się działanie, które ma wyrządzić szkodę innej osobie – zwłaszcza,

[29] A. Suchorzewska, *Ochrona prawa systemów...*, s. 242.

[30] Tamże.

[31] Więcej na ten temat zob. *Kodeks karny...* t. 3, A. Zoll (red.), s. 324 i nast.

że górna granica zagrożenia karnego pozwala kwalifikować czyn stypizowany w art. 287 kk jako przestępstwo o charakterze terrorystycznym. Biorąc pod uwagę fakt, że penalizowane zachowanie bardzo przypomina zachowanie opisane w dyspozycjach wcześniej omawianych przepisów, ważną kwestią staje się określenie ich wzajemnej relacji. Ze względu na majątkowy charakter dóbr, w które godzi zachowanie sprawcy, art. 287 kk stanowi *lex specialis* wobec art. 268, 268a oraz 269a kk. W literaturze wskazano natomiast, że kumulatywny zbieg z art. 269 § 2 kk może mieć miejsce wtedy, gdy modyfikacja danych (usunięcie, zmiana wprowadzenie nowych zapisów) będzie dotyczyła danych odnośnie do mienia i jednocześnie mających szczególne znaczenie[32].

Wszystkie analizowane powyżej przepisy zakładają karalność umyślnego działania sprawcy, co wydaje się być zabiegiem właściwym. Należy pamiętać, że standardowym działaniem administratorów jest zabezpieczanie i ograniczanie dostępu do danych oraz systemów przed ingerencją osób niepowołanych. Trudno więc sobie wyobrazić, by osoba o przeciętnych umiejętnościach obsługi komputera mogła w sposób przypadkowy dopuścić się czynów stypizowanych w powyższych przepisach. Odpowiada to również naturze przestępstwa o charakterze terrorystycznym, które jest popełniane „w celu", a zatem zawsze w zamiarze umyślnym. Niemal wszystkie artykuły (za wyjątkiem art. 269 i 287 kk) przewidują karalność działań osoby, która nie jest uprawniona do ich wykonania. Okolicznością wyłączającą kryminalną bezprawność czynu jest zatem fakt działania osoby upoważnionej, np. administratora systemu czy funkcjonariuszy organów powołanych do ochrony bezpieczeństwa publicznego.

Przepisy penalizujące skutki cyberataków

Skutki popełniania powyższych przestępstw sprowadzają się do powodowania strat w cyberprzestrzeni – głównie niszczenia danych, utrudnienia ich przetwarzania, zakłócenia działania systemów i sieci, a niekiedy także uszkodzenia lub zniszczenia sprzętu. Oczywiście już takie straty mogą spowodować, że cel działania terrorystów zostanie osiągnięty. Przykładowo, uniemożliwienie działania systemów giełdy może spowodować poważne zakłócenia w gospodarce, a zablokowanie dostępu do kont bankowych zastraszyć wiele osób. Niemniej jednak, jak wcześniej wskazano, działania w cyberprzestrzeni mogą być tylko środkiem mającym wywołać straty w świecie rzeczywistym. Wobec tego warto przeanalizować także przestępstwa, które mogą być skutkiem działań dokonywanych w cyberprzestrzeni.

Przepisem najczęściej wymienianym w literaturze, który został wskazany także w założeniach do RPOC[33], jest artykuł 165 kk. Penalizuje on spowodowanie niebezpieczeństwa dla dóbr, jakimi są życie i zdrowie wielu osób oraz mienia w wielkich rozmiarach, przy czym może być ono rozumiane w sposób tożsamy z mieniem wielkiej wartości w rozumieniu art. 115 kk. W rzeczywistości chodzi o fizyczne rozmiary mienia, a nie jego wartość[34]. Zagrożenie to nie musi mieć charakteru bezpośredniego, konieczne jest jednak by było realne, a nie abstrakcyjne[35]. Formy działania prowadzące do wywołania tego zagrożenia zostały opisane w paragrafie pierwszym tego przepisu:

---

[32] Tamże, s. 335.

[33] http://bip.msw.gov.pl/download/4/4297/program_20ochrony_20cyberprzestrzeni.pdf [dostęp: 25 VI 2011].

[34] R.A. Stefański, *Pojęcie „mienia o wielkich rozmiarach"*, „Prokuratura i Prawo" 1999, nr 1.

[35] *Kodeks karny*..., M. Filar (red.), s. 735.

„Art. 165 § 1. Kto sprowadza niebezpieczeństwo dla życia lub zdrowia wielu osób albo dla mienia w wielkich rozmiarach:
1) powodując zagrożenie epidemiologiczne lub szerzenie się choroby zakaźnej albo zarazy zwierzęcej lub roślinnej,
2) wyrabiając lub wprowadzając do obrotu szkodliwe dla zdrowia substancje, środki spożywcze lub inne artykuły powszechnego użytku lub też środki farmaceutyczne nie odpowiadające obowiązującym warunkom jakości,
3) powodując uszkodzenie lub unieruchomienie urządzenia użyteczności publicznej, w szczególności urządzenia dostarczającego wodę, światło, ciepło, gaz, energię albo urządzenia zabezpieczającego przed nastąpieniem niebezpieczeństwa powszechnego lub służącego do jego uchylenia,
4) zakłócając, uniemożliwiając lub w inny sposób wpływając na automatyczne przetwarzanie, gromadzenie lub przekazywanie danych informatycznych,
5) działając w inny sposób w okolicznościach szczególnie niebezpiecznych, podlega karze pozbawienia wolności od 6 miesięcy do lat 8".

Szczególnie interesujące w kontekście cyberataków są punkty 3 i 4. Punkt trzeci przewiduje karalność uszkodzenia lub unieruchomienia urządzeń użyteczności publicznej i jednocześnie podaje ich przykłady. Wydaje się, że działanie opisane w art. 165 § 1 pkt. 3 kk może dotyczyć większości (a być może nawet wszystkich) systemów składających się na infrastrukturę krytyczną. Ustawodawca wskazuje jedynie na urządzenia użyteczności publicznej, których naruszenie może powodować powstanie niebezpieczeństwa dla ludzi lub mienia, nie określając jednocześnie, w jaki sposób miałyby one zostać uszkodzone lub unieruchomione. Tym samym zakresem penalizacji przepisu jest objęte każde działanie, które może wywołać wspomniany skutek, np. odcięcie źródła zasilania, wymontowanie ważnych elementów, fizyczne zniszczenie, ale też oddziaływanie na układ sterujący czy wprowadzenie fałszywych danych. Tymczasem wymieniany w punkcie czwartym sposób działania sprowadza się do wpływania na automatyczne przetwarzanie, gromadzenie i przekazywanie danych, bez konkretnego wskazania treści czy charakteru tych danych. Zatem przy dokonywaniu kwalifikacji prawnej cyberataku o charakterze terrorystycznym czyn ten będzie, co do zasady, jednocześnie wypełniał znamiona opisane w obu wspomnianych punktach. Karą, jaką ustawodawca przewidział za popełnienie tego przestępstwa w typie podstawowym, jest pozbawienie wolności od sześciu miesięcy do ośmiu lat. Jeśli następstwem czynu będzie śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób, to granice wymiaru kary będą wynosiły od dwóch do dwunastu lat pozbawienia wolności. Wydaje się, że możliwy jest kumulatywny zbieg przestępstw wymienionych w artykułach 268a i 269 kk. Ze względu na wartość mienia chronionego przez art. 165 kk będzie on stanowił *lex consumens* wobec art. 287 kk. Nie da się też wykluczyć możliwości zbiegu art. 165 § 1 pkt. 3 z art. 269a kk.

Artykuł 163 kk przewiduje karę za spowodowanie zdarzenia, które zagraża życiu lub zdrowiu wielu osób albo mieniu w wielkich rozmiarach. Aby można było je za takie uznać, powinno ono przyjąć jedną z form wymienionych w § 1, czyli formę:
- pożaru,
- zawalenia się budowli, jej zalania albo obsunięcia się na nią ziemi, skał lub śniegu,
- eksplozji materiałów wybuchowych lub łatwopalnych albo innego gwałtownego wyzwolenia energii, rozprzestrzenienia się substancji trujących, duszących lub parzących,
- gwałtownego wyzwolenia energii jądrowej lub wyzwolenia promieniowania jonizującego.

Można sobie wyobrazić, że w niektórych przypadkach działania w cyberprzestrzeni mogą wywołać zdarzenie, które będzie miało jedną z wyżej wymienionych form, np. będzie to pożar w fabryce wywołany przez awarię spowodowaną wyłączeniem systemu chłodzenia albo zalanie dużych obszarów poprzez jednoczesne, całkowite otwarcie wszystkich śluz w tamie. W takim przypadku przewidywana kara wynosi od roku do dziesięciu lat pozbawienia wolności, w typie kwalifikowanym zaś (gdy następstwem jest śmierć człowieka lub ciężki uszczerbek na zdrowiu wielu osób) od dwóch do dwunastu lat pozbawienia wolności. Samo sprowadzenie bezpośredniego niebezpieczeństwa takiego zdarzenia podlega natomiast, w myśl art. 164 kk, karze pozbawienia wolności od sześciu miesięcy do ośmiu lat.

Sektorem szczególnie narażonym na ataki terrorystyczne jest transport i komunikacja. To właśnie środki transportu zbiorowego były celem zamachów w Madrycie (2004 r.) i Londynie (2005 r.). Także działania terrorystów w cyberprzestrzeni, polegające na przejęciu kontroli nad systemami zarządzającymi transportem i komunikacją, mogą wywołać tragiczne skutki. Stąd też wobec sprawców takich ataków może mieć zastosowanie art. 173 kk:

> „Art. 173 § 1. Kto sprowadza katastrofę w ruchu lądowym, wodnym lub powietrznym zagrażającą życiu lub zdrowiu wielu osób albo mieniu w wielkich rozmiarach, podlega karze pozbawienia wolności od roku do lat 10".

Karalnością jest objęte każde działanie, które doprowadza do katastrofy wszelkiego rodzaju środków transportu, zagrażające ludzkiemu życiu, zdrowiu lub mieniu w wielkich rozmiarach. Wydaje się, że, podobnie jak niebezpieczeństwa wymienione w art. 165 kk, zagrożenie to może być realne. Przykładem działania cyberterrorystycznego wypełniajacego znamiona art. 173 kk byłoby spowodowanie karambolu samochodowego poprzez ingerencję w działanie sygnalizacji świetlnej albo wprowadzenie statku na mieliznę poprzez modyfikację danych systemu GPS na temat jego położenia. Zagrożenie karne za popełnienie tego czynu jest analogiczne jak w przypadku art. 163 kk – od roku do dziesięciu lat pozbawienia wolności w typie podstawowym, od dwóch do dwunastu lat, jeśli doprowadzi do śmierci człowieka lub ciężkiego uszczerbku na zdrowiu wielu osób (art. 173 § 3 kk), i od sześciu miesięcy do ośmiu lat pozbawienia wolności za sprowadzenie bezpośredniego niebezpieczeństwa katastrofy (art. 174 § 1 kk).

Powyższe wyliczenie nie stanowi zamkniętego katalogu czynów karalnych, które mogą być skutkiem cyberataków. W istocie ma ono jedynie charakter przykładowy, wskazujący na najbardziej prawdopodobne przestępstwa. Trudno przewidzieć sposób działania cyberterrorystów i dobra prawne, które będą naruszać, wskutek czego niemożliwe jest wskazanie dokładnej kwalifikacji prawnej czynu. Wydaje się jednak, że nie będą oni poprzestawać na powodowaniu strat w cyberprzestrzeni i że będą dążyć do wywołania szkód w świecie rzeczywistym, przedkładając efektowność działań nad ich efektywność.

V
DOKUMENTY I SPRAWOZDANIA

Arkadiusz Iwaniuch
Ryszard Oleszkowicz

Konferencja Agencji Bezpieczeństwa Wewnętrznego pt. „Kontrwywiad II RP (1914) 1918–1945 (1948)” (7–8 listopada 2012 r., Emów)

W dniach 7–8 listopada 2012 r. w Centralnym Ośrodku Szkolenia Agencji Bezpieczeństwa Wewnętrznego im. gen. dyw. Stefana Roweckiego „Grota” w Emowie odbyła się konferencja naukowa pt. „Kontrwywiad II RP (1914) 1918–1945 (1948)”. Jej celem było przedstawienie działalności kontrwywiadowczej polskich służb specjalnych II Rzeczpospolitej na tle kształtującego się Państwa Polskiego oraz umiejscowienie służb odpowiedzialnych za bezpieczeństwo kraju w jego strukturach. Należy podkreślić, że była to jedna z pierwszych po 1989 r. konferencji naukowych poświęcona służbom specjalnym.

Konferencja ta była kolejną konferencją zorganizowaną przez Agencję Bezpieczeństwa Wewnętrznego, która zgromadziła polskich historyków zajmujących się badaniami historii polskich służb specjalnych. Wzięli w niej udział naukowcy prowadzący badania na podstawie krajowych i zagranicznych zasobów archiwalnych. Niektórzy z nich podjęli te prace już latach 90. XX wieku, niezwłocznie po zaistnieniu warunków do nieskrępowanego dostępu do materiałów źródłowych. Jako prelegenci wystąpili także przedstawiciele młodego pokolenia historyków, którzy dopiero w ostatnich latach podjęli ten temat.

Konferencja była jedną z inicjatyw dotyczacych ożywienia w ABW tradycji służb specjalnych II RP i Polskiego Państwa Podziemnego, podjętych w 2012 r. Inną inicjatywą była zorganizowana po raz pierwszy według ceremoniału wojskowego, odwołującego się do tradycji II RP, uroczysta promocja na pierwszy stopień oficerski oraz odsłonięcie na terenie Centralnego Ośrodka Szkolenia ABW popiersia patrona ośrodka – gen. dyw. Stefana Roweckiego „Grota”.

W wystąpieniu inaugurującym konferencję szef Agencji Bezpieczeństwa Wewnętrznego gen. bryg. Krzysztof Bondaryk podkreślił rolę kontrwywiadu w okresie II RP. Dziękując prelegentom za przybycie, zaznaczył, że udział w konferencji z pewnością przyczyni się do wymiany doświadczeń oraz zainicjuje opracowanie syntezy historii polskiego kontrwywiadu w okresie 1914–1918.

Dyrektor Centralnego Ośrodka Szkolenia ABW w Emowie mjr dr Zbigniew Nawrocki w swym wystąpieniu podkreślił, że wybór ośrodka jako miejsca konferencji uwzględniał także aspekty dydaktyczne przedsięwzięcia. Ponieważ do ustawowych zadań Agencji należy m.in. prowadzenie kontrwywiadowczej ochrony państwa, to treści prezentowane podczas konferencji z pewnością przyczynią się do poszerzenia historycznej wiedzy funkcjonariuszy dotyczącej metod i form działania polskich służb specjalnych w przeszłości, a także z pożytkiem zostaną wykorzystane w praktyce.

W imieniu organizatorów konferencji dyrektor COS ABW wyraził nadzieję, że nie będzie to ostatnia konferencja poświęcona temu tematowi. Na następnych, dorocznych spotkaniach uczestnicy mogliby zaprezentować najnowsze wyniki badań dotyczących polskich służb specjalnych. Oprócz historyków polskich planowane jest zaproszenie do udziału w konferencjach gości z państw sąsiednich. Celem spotkań byłoby opracowanie

i wydanie monografii poświęconej historii polskiego kontrwywiadu jako agendy niepodległego państwa polskiego.

Konferencji towarzyszyła okolicznościowa wystawa przedmiotów i sprzętów wykorzystywanych przez polskie służby specjalne – można było zobaczyć m.in. słynną maszynę szyfrującą Enigmę oraz obejrzeć odsłonięty we wrześniu 2012 r. pomnik patrona Ośrodka – gen. dyw. Stefana Roweckiego „Grota", Komendanta Głównego Armii Krajowej.

Zdj. 1. Wystąpienie szefa ABW gen. bryg. Krzysztofa Bondaryka.

Zdj. 2. Wystąpienie dyrektora COS ABW w Emowie mjr. dr. Zbigniewa Nawrockiego.

Zdj. 3. Uczestnik konferencji prof. Henryk Ćwięk przy oryginalnym egzemplarzu Enigmy ze zbiorów COS ABW w Emowie.

Jarosław Szatkowski

Dwudziestolecie jednostki antyterrorystycznej UOP-ABW (1993–2013)

Urząd Ochrony Państwa RP został utworzony w 1990 r. w miejsce zlikwidowanej Służby Bezpieczeństwa. Jako cywilna służba specjalna, w ramach nałożonych na nią ustawowo kompetencji, realizował zadania związane m.in. z rozpoznawaniem i przeciwdziałaniem zagrożeniom godzącym w bezpieczeństwo państwa, do jego zadań należało zapobieganie szpiegostwu, terroryzmowi i wykrywanie tych przestępstw.

Następujące w tamtym czasie zmiany polityczne zbiegły się z okresem, w którym obserwowano gwałtowny wzrost aktywności i brutalizacji zorganizowanych grup przestępczych (w tym o charakterze międzynarodowym). Otwarcie granic spowodowało zwiększenie przemytu dóbr konsumpcyjnych, ale też narkotyków, broni palnej oraz materiałów wybuchowych. Rezydenci zagranicznych zorganizowanych grup przestępczych działający na terenie naszego kraju, zwłaszcza ci zza wschodniej granicy, rozpoczęli walkę z rodzimymi grupami przestępczymi o strefę wpływów w tej części Europy. Zrodziło się nowe zjawisko nazwane terrorem kryminalnym. Oprócz tego również zmiany zachodzące w polityce zagranicznej Polski, m.in. nawiązanie stosunków dyplomatycznych z Izraelem czy opowiedzenie się po stronie koalicji w konflikcie o Kuwejt, sprowadziły na nasz kraj realną groźbę przeprowadzenia tu zamachów terrorystycznych.

Nowe zagrożenia dla bezpieczeństwa wewnętrznego państwa i ich skala doprowadziły do ewolucji służb odpowiedzialnych za rozpoznananie tych zagrożeń i przeciwdziałanie im. Konieczne okazało się utworzenie od nowa struktur przygotowanych do fizycznego reagowania na nowe formy przestępstw godzących w bezpieczeństwo wewnętrzne państwa.

W pierwszych latach istnienia UOP podczas wykonywania szczególnie niebezpiecznych zadań, zwłaszcza przy zatrzymaniach wysokiego ryzyka, funkcjonariusze tej instytucji korzystali ze wsparcia policyjnych pododdziałów antyterrorystycznych oraz funkcjonariuszy JW 2305 GROM, podległej wówczas MSW. Chociaż współpraca w tym zakresie układała się pomyślnie, to wobec rosnącej liczby realizacji oraz w celu usprawnienia i usamodzielnienia działań Urzędu postanowiono powołać do życia własną grupę taktyczną.

Na przełomie kwietnia i maja 1993 r. na wniosek ówczesnego szefa UOP Jerzego Koniecznego utworzono w ramach Zarządu Śledczego jednostkę specjalną – Wydział V Zabezpieczenia Realizacji (WZR). Misję budowy nowej struktury oraz dowodzenie nią powierzono Romualdowi Maniszewskiemu, a na jego zastępcę powołano Jana Gawrońskiego. Obaj oficerowie byli doświadczonymi funkcjonariuszami Wydziału Antyterrorystycznego Komendy Stołecznej Policji (AT KSP).

Zadania postawione WZR sprowadzały się do zapewnienia ochrony i siłowego wsparcia struktur dochodzeniowo-śledczych podczas przeprowadzania najtrudniejszych operacji specjalnych przeciwko przestępczości zorganizowanej oraz do przeciwdziałania zagrożeniom terrorystycznym w zakresie ustawowych działań Urzędu. Z czasem, przy znacznej liczbie realizacji bojowych, zwiększeniu stanu osobowego oraz

nałożeniu dodatkowych zadań na jednostkę, Wydział V Zabezpieczenia Realizacji przemianowano na Wydział V – Działań Antyterrorystycznych i Zabezpieczenia Realizacji Zarządu Śledczego UOP (nieformalnie nazywany „Piątką"). Z uwagi na wytyczone kierownictwu jednostki zadanie osiągnięcia gotowości do działań realizacyjnych już po sześciu miesiącach jej funkcjonowania, a także oczekiwaną „antyterrorystyczną jakość" wyszkolenia, trzon nowego Wydziłu V oraz pierwszą kadrę instruktorską stanowili funkcjonariusze Wydziału AT KSP i wojskowych jednostek specjalnych.

Pierwsze programy szkolenia zostały opracowane przez kadrę instruktorów „Piątki" z wykorzystaniem doświadczeń jednostek specjalnych Policji. Zakres tych szkoleń, oprócz sprawności ogólnej, strzeleckiej, taktyki specjalnej i jazdy samochodami obejmował wiedzę o strukturze i zadaniach UOP, podstawach pracy operacyjnej i śledczej, obserwacji, ochronie osób oraz obiektów strategicznych. Główny nacisk kładziono na bezpieczeństwo funkcjonariuszy w trakcie przeprowadzania realizacji bojowych. Z czasem programy szkolenia zostały wzbogacone o nowe zagadnienia, a funkcjonariusze poszerzali swoją wiedzę o umiejętności z zakresu technik wysokościowych, spadochronowych, płetwonurkowych i jaskiniowych. Znaczna liczba trudnych realizacji, tj. z koniecznością użycia specjalistycznych technik, środków i taktyki AT, przeprowadzonych profesjonalnie przez funkcjonariuszy Wydziału V, przekonała kierownictwo UOP do potrzeby inwestowania w tę jednostkę, tak w zakresie wyposażenia w sprzęt, jak i wyszkolenia funkcjonariuszy. Już w październiku 1993 r. czterech funkcjonariuszy wydziału uczestniczyło w intensywnym, pięciotygodniowym szkoleniu dla operatorów jednostek antyterrorystycznych w Stanach Zjednoczonych, zorganizowanym przez Departament Stanu USA. Ponadto dzięki coraz lepiej rozwijającej się współpracy ze służbami specjalnymi tego kraju cały stan osobowy Wydziału odbył dwukrotnie (tj. w 1996 i 1997 r.) szkolenia o charakterze antyterrorystycznym na terenie Stanów Zjednoczonych. Na szkolenia tematyczne do USA funkcjonariusze Wydziału V wyjeżdżali także w trybie indywidualnym. Kadrę instruktorską na tych kursach stanowili zarówno pozostający w służbie czynnej funkcjonariusze i żołnierze takich formacji specjalnych, jak Navy Seals, Delta Force, Special Air Service (SAS), FBI SWAT, jak i weterani tych jednostek. Możliwość odbycia treningów przez cały stan osobowy Wydziału V, zakres oraz intensywność tych kursów, a także fakt, że były one specjalnie przygotowane dla „Piątki", pozwoliły na osiągnięcie wysokiego, równego poziomu wyszkolenia funkcjonariuszy, dającego możliwość stworzenia zupełnie nowych, jak na polskie warunki, własnych procedur działań bojowych oraz standardów szkolenia.

Wzrost profesjonalizacji wyszkolenia funkcjonariuszy Wydziału V został potwierdzony m.in. zajęciem pierwszego miejsca w międzynarodowych zawodach pododdziałów antyterrorystycznych w 1996 r. (jedynych tego typu zawodach organizowanych na terytorium RP). Wielokrotnie, z reguły na terenie poligonu w Wędrzynie, kadra instruktorska Wydziału V prowadziła szkolenia z zakresu działań specjalnych dla policyjnych jednostek antyterrorystycznych, BOR oraz wojskowych jednostek specjalnych (m.in. FORMOZY). Jednocześnie instruktorzy „Piątki" systematycznie przekazywali swoje umiejętności (prowadząc szkolenia w zakresie taktyki zatrzymań, strzelania i sportów walki) funkcjonariuszom Zarządu Śledczego (z centrali i delegatur) oraz innych pionów UOP (w tym Zarządu Wywiadu).

W 2002 r., po przekształceniu UOP w Agencję Bezpieczeństwa Wewnętrznego, Wydział V, zachowując dotychczasową nazwę, został podporządkowany Departamentowi Postępowań Karnych (DPK). Większość zadań, które funkcjonariusze „Piątki" od

tamtej pory realizują (samodzielnie lub we współpracy z antyterrorystami policyjnymi), dotyczy szeroko pojętego terroru kryminalnego, w tym zwalczania najgroźniejszych zorganizowanych grup przestępczych.

Jednym z ważniejszych zadań Wydziału jest prowadzenie działań ochronnych – funkcjonariusze w wymagających tego sytuacjach strzegli bezpieczeństwa kierownictwa oraz wskazanych funkcjonariuszy ABW, członków parlamentarnych komisji śledczych, wspierali działania ochronne prowadzone przez BOR w trakcie wizyt w Polsce papieży Jana Pawła II i Benedykta XVI oraz prezydenta USA Baracka Obamy. Działania ochronne realizowane są również w przypadku spotkań szefa ABW z szefami zagranicznych służb specjalnych lub innymi ważnymi osobistościami (np. zabezpieczenie wizyt szefów służb specjalnych państw UE w Krakowie w trakcie Prezydencji RP w Radzie Unii Europejskiej w 2011 r. podczas posiedzenia Club de Berne – CdB i Counterterrosim Group – (CTG).

Jednostka czynnie uczestniczyła w pracach mających na celu przygotowanie i zabezpieczenie antyterrorystyczne przedsięwzięć związanych z Mistrzostwami Europy w Piłce Nożnej EURO 2012 rozgrywanymi na terenie RP i Ukrainy. W ramach przygotowań funkcjonariusze „Piątki" dwukrotnie brali udział we wspólnych ćwiczeniach z ukraińską jednostką antyterrorystyczną „Alfa" SBU, przeprowadzonych w Polsce i na Ukrainie. Ponadto wraz z funkcjonariuszami Biura Operacji Antyterrorystycznych KGP i żołnierzami JW 2305 GROM uczestniczyli w ćwiczeniach antyterrorystycznych POLONIA 2010 na pierwszoligowym warszawskim stadionie piłkarskim oraz w zorganizowanych przez ABW międzynarodowych ćwiczeniach „OFFSIDE".

W ramach doskonalenia zawodowego Wydział V w dalszym ciągu prowadzi wymianę doświadczeń z czołowymi jednostkami specjalnymi zarówno w kraju, jak i za granicą. Współpracuje m.in. z JW 2305 GROM, Wydziałem Realizacji Komendy Stołecznej Policji, Morskim Oddziałem Straży Granicznej, Oddziałem Specjalnym Żandarmerii Wojskowej z Warszawy oraz Wydziałem Zabezpieczenia Działań Karpackiego Oddziału Straży Granicznej. W latach 2002–2005 i 2007–2008 realizowana była współpraca z zagranicznymi jednostkami specjalnymi, m.in. z francuską jednostką antyterrorystyczną RAID czy amerykańskimi jednostkami SWAT i HRT. Kontakty te są uzależnione od oficerów łącznikowych danego kraju i bieżących relacji między służbami. Współpraca z tak wieloma różnorodnymi służbami i formacjami pozwala na korzystanie z wiedzy i doświadczeń ekspertów realizujących zadania w obszarach i warunkach innych niż te, z którymi ma do czynienia Wydział V DPK ABW.

To, co odróżnia „Piątkę" od pozostałych jednostek antyterrorystycznych (np. Policji, której zadaniem jest przede wszystkim interweniowanie w wypadku już dokonanego aktu terrorystycznego), to fakt, że jej działania zawsze mają charakter wyprzedzający.

Zaostrzony proces rekrutacji, doskonalony przez lata proces szkolenia, doświadczenie zdobyte podczas kilkuset realizacji bojowych (przeprowadzonych nie tylko na potrzeby UOP czy ABW) oraz niezwykłe zaangażowanie funkcjonariuszy zapewniły jednostce wyjątkową jakość, która umożliwia bezpieczną realizację praktycznie każdego antyterrorystycznego zadania.

Obecnie Wydział V Antyterrorystyczny czeka na przeprowadzkę do nowej siedziby w Centralnym Ośrodku Szkolenia ABW. Infrastruktura Ośrodka stworzy możliwość poszerzenia współpracy z innymi jednostkami taktycznymi służb systemu bezpieczeństwa państwa, a także bardziej profesjonalnego przygotowania funkcjonariuszy do realizacji ustawowych zadań ABW.

Na zakończenie pragnę w imieniu swoim oraz moich poprzedników podziękować wszystkim byłym i obecnym funkcjonariuszom jednostki antyterrorystycznej za dwadzieścia lat *odwagi, honoru i żarliwej dla Narodu służby.*

Zdj. 1. Kurs spadochronowy dla funkcjonariuszy Wydziału V Działań Antyterrorystycznych i Zabezpieczenia Realizacji Zarządu Śledczego Urzędu Ochrony Państwa – Inowrocław 2001 r.

Zdj. 2. Funkcjonariusze Wydziału V Departamentu Postępowań Karnych ABW podczas wizytacji Prezesa Rady Ministrów oraz szefa ABW w 2002 r.

Zdj. 3. Ćwiczenia taktyczne Wydziału V Departamentu Postępowań Karnych ABW w obiektach treningowych COS ABW w Emowie w 2008 r.

O autorach

About the Authors

1. Magdalena Adamczuk – doktorantka Akademii Obrony Narodowej, starszy specjalista w Departamencie Prawa i Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego.
2. Mariusz Cichomski – naczelnik Wydziału Przeciwdziałania Zagrożeniom Terrorystycznym i Przestępczości Zorganizowanej Departamentu Nadzoru w MSW, z wykształcenia prawnik, socjolog, absolwent studiów doktoranckich na Uniwersytecie Warszawskim.
3. Krzysztof Danielewicz – dr, żołnierz Wojska Polskiego w służbie czynnej.
4. Arkadiusz Dymowski – dr, kpt., Agencja Bezpieczeństwa Wewnętrznego.
5. Fabiana Fetke – mjr, Agencja Bezpieczeństwa Wewnętrznego.
6. Kamil Frąckowiak – dr, Katedra Prawa Karnego Materialnego Wydział Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.
7. Marcin Gołaszewski – doktorant Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, st. plut. Agencja Bezpieczeństwa Wewnętrznego.
8. Arkadiusz Iwaniuch – por., Agencja Bezpieczeństwa Wewnętrznego.
9. Krzysztof Izak – mjr, Agencja Bezpieczeństwa Wewnętrznego.
10. Anna Kańciak – doktorantka Uniwersytetu Warszawskiego, st. plut. Agencja Bezpieczeństwa Wewnętrznego.
11. Maciej Aleksander Kędzierski – mł. insp., Centralne Biuro Śledcze Komendy Głównej Policji.
12. Krzysztof Krełowski – por., Agencja Bezpieczeństwa Wewnętrznego.
13. Mirosław Kumanek – pracownik Wydziału Przeciwdziałania Zagrożeniom Terrorystycznym i Przestępczości Zorganizowanej Departamentu Nadzoru w MSW.
14. Maciej Musiejko – mgr, wyróżniony w konkursie szefa ABW dla absolwentów studiów licencjackich i magisterskich w roku akademickim 2011/2012
15. Ryszard Oleszkowicz – ppłk, Agencja Bezpieczeństwa Wewnętrznego.
16. Dariusz Pożaroszczyk – st. kpr., Agencja Bezpieczeństwa Wewnętrznego, doktorant Uniwersytetu Warszawskiego.
17. Kacper Rękawek – dr, analityk w grupie ds. bezpieczeństwa międzynarodowego w Polskim Instytucie Spraw Międzynarodowych.
18. Mirosław Sadowski – dr hab., adiunkt w Katedrze Doktryn Politycznych i Prawnych Wydział Prawa, Administracji i Ekonomii Uniwersytetu Wrocławskiego.
19. Tomasz Safjański – dr, mł. insp., Pełnomocnik Komendanta Głównego Policji.
20. Sławomir Suchecki – mjr, Agencja Bezpieczeństwa Wewnętrznego.
21. Jarosław Szatkowski – mjr, Agencja Bezpieczeństwa Wewnętrznego.
22. Przemysław Szustakiewicz – dr, sędzia Wojewódzkiego Sądu Administracyjnego w Warszawie, adiunkt w Katedrze Prawa Administracyjnego na Uczelni Łazarskiego w Warszawie, członek Rady Programowej Zrzeszenia Prawników Polskich.
23. Luiza Wojnicz – dr, adiunkt w Zakładzie Strategii i Bezpieczeństwa Europejskiego Uniwersytetu Szczecińskiego.
24. Piotr Wojtunik – por., Agencja Bezpieczeństwa Wewnętrznego.

Informacja dla autorów „Przeglądu Bezpieczeństwa Wewnętrznego”

Redakcja zwraca się do wszystkich autorów nadsyłających teksty do druku o stosowanie następujących zasad:

1. Wszystkie teksty należy przesyłać w postaci zapisu elektronicznego (Word, Open Office) pod adresem Redakcji: redakcja.pbw@abw.gov.pl
2. Do artykułu należy dołączyć: streszczenie o objętości tekstu do pół strony wydruku komputerowego oraz notkę o autorze (zawód lub tytuł naukowy, miejsce pracy). W miarę możliwości prosimy również o nadsyłanie streszczenia w języku angielskim.
3. Autorzy powinni wypełnić dostępny na stronie Agencji Bezpieczeństwa Wewnętrznego *Formularz zgody autora na publikację artykułu w czasopiśmie „PBW”* i przesłać go pod adresem Redakcji podanym w punkcie pierwszym.
4. Wszelkie ilustracje, zdjecia 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 otrzymane po wydruku oraz możliwie jak najlepszej jakości (min. 600 dpi). W przypadku dostarczenia ilustracji złej jakości, Redakcja zastrzega sobie prawo do ich nieumieszczania.
5. Należy podać źródła wszystkich materiałów ilustracyjnych (zdjęć, rysunków, wykresów, schematów, tabel itd.).
6. Na końcu podpisu pod materiałem ilustracyjnym należy stawiać kropkę.
7. Odsyłacze do przypisów powinny być umieszczone w tekście przed znakami interpunkcyjnymi – kropką kończącą zdanie (wyjątek: skrót r. – rok lub podobny), przecinkiem itd.
8. Cytaty ze źródeł i literatury przedmiotu, nazwy ustaw i innych aktów prawnych, tytuły prac naukowych, utworów literackich, muzycznych, dramatycznych, obrazów, wystaw, konferencji, sesji naukowych, konkursów należy wyróżnić kursywą.
9. W bibliografii i przypisach powinien być zachowany następujący schemat opisu:
   a) przypis zaczynamy wielką literą (wyjątek stanowi przypis internetowy) i kończymy kropką,
   b) przypis archiwalny: nazwa archiwum, po przecinku nazwa zespołu, sygnatura, ewentualnie tom, tytuł dokumentu (kursywą), data, karta,

   PRZYKŁAD:
   AIPN, OBUiAD w Krakowie, IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57.

   c) druki zwarte: inicjał imienia, nazwisko autora, po przecinku tytuł (kursywą), po przecinku ewentualnie tom, po przecinku miejsce i rok wydania, po przecinku strony; po tytule publikacji zamieszczonej w pracy zbiorowej stawiamy przecinek i piszemy: w: i tytuł pracy (kursywą),

   PRZYKŁAD:
   W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, K. Kowalski (red.), t. 3, Warszawa 1999, PWN, s. 36.

d) artykuły w czasopismach: inicjał imienia, nazwisko autora, po przecinku tytuł (kursywą), po przecinku tytuł czasopisma w cudzysłowie, dalej (bez przecinka) rok wydania, po przecinku tom, zeszyt, numer, część (w opisie należy stosować cyfry arabskie), po przecinku strony,

PRZYKŁAD:
W. Nowak, *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 13.

e) wydawnictwa internetowe: adres internetowy (bez podkreśleń i hiperłączy), po przecinku w nawiasie kwadratowym informacja o dostępie (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:
http://www.pbw.gov/abw/cat.htm, [dostęp: 1 XII 2011].

f) podając strony należy stosować skrót: s. i dywiz ze światłami, np.: s. 30, s. 24–27,
g) należy stosować oznaczenia: tamże, ten sam, ta sama, passim, (Jeżeli zwroty tego typu rozpoczynają przypis, należy stosować wielką literę), inicjał imienia, nazwisko autora, po przecinku skrót tytułu (kursywą), po przecinku strony; nie stosujemy: *op. cit.*, *loc. cit.,*

PRZYKŁAD:
W. Nowak, *Służba*..., s. 12.
Tamże, s. 14.

h) po skrócie : zob. i por. nie stawiamy dwukropka,
i) po skrócie: cyt. za: stawiamy dwukropek.

10. W tekstach zasadniczych należy stosować ogólnie przyjęte skróty (np., itp., m.in., rkps, mps, t., z., itd.), a także z reguły: r. (rok) i w. (wiek).
11. W tekście głównym należy stosować zapis daty: 3 lipca 1969 r.; w przypisach nazwę miesięcy należy podać cyfrą rzymską, gdy występują wraz z dniem i rokiem (bez oddzielających je kropek), w innych przypadkach słownie.
12. Należy podawać pełne imię i nazwisko osoby, która wymieniana jest w tekście po raz pierwszy.
13. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp., jeśli są wymienione w tekście po raz pierwszy.
14. Obce nazwy organizacji oraz skróty od nich utworzone powinny być pisane antykwą (tekstem prostym).
15. Nie należy stosować tzw. twardych spacji.
16. Przy edycji dokumentów źródłowych należy stosować następujące zasady:
    a) nagłówek dokumentu powinien składać się z daty powstania dokumentu, miejsca powstania dokumentu oraz – po myślniku – regestu dokumentu (data powstania dokumentu ma następujący zapis: rok, miesiąc, dzieło, a brakujące elementy daty należy uzupełnić w nawiasie kwadratowym),
    b) ortografię i interpunkcję tekstu należy uwspółcześniać,
    c) stosowane w dokumentach różne sposoby zapisu daty powinny być ujednolicone do następującej formy, np. 12 VIII 1946, nie należy zamieniać na liczbę rzymską nazw miesięcy pisanych słownie,

d) wszelkie wyróżnienia w oryginalnym tekście dokumentu, dokonane przez jego twórcę, powinny być oddane za pomocą czcionki wytłuszczonej,
e) nawiasy ukośne /…/ powinny być zamieniane na nawiasy półokrągłe (…),
f) skróty słownikowe należy pozostawić bez rozwinięcia,
g) skróty niekonwencjonalne należy rozwijać w nawiasach kwadratowych antykwą,
h) opuszczenia pochodzące od wydawcy powinny być zaznaczone trzema kropkami w nawiasie okrągłym,
i) opuszczenia w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie kwadratowym.

10. Redakcja zastrzega sobie prawo do zwracania autorom tekstów opracowanych bez uwzględnienia powyższych zasad.
11. Redakcja zastrzega sobie prawo do dokonywania zmian i skrótów w porozumieniu z autorem.
12. Redakcja zwraca uwagę, że *ghostwriting*[1] i *guest authorship*[2] są przejawem nierzetelności naukowej, a wszelkie wykryte przypadki praktyk niezgodnych z zasadami etyki obowiązującej w nauce będą ujawniane, włącznie z powiadomieniem odpowiednich podmiotów (instytucji zatrudniających autorów, towarzystw naukowych, stowarzyszeń edytorów naukowych itp.).
13. Redakcja zwraca uwagę, iż autorzy tekstów powinni w sposób przejrzysty, rzetelny i uczciwy prezentować rezultaty swojej pracy, a wszelkie przejawy nierzetelności naukowej, zwłaszcza łamanie i naruszanie zasad etyki obowiązujących w nauce, będą dokumentowane przez Redakcję.

[1] 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.

[2] Sytuacja określana też jako *honorary authorship* – osoba podana jako autor czy współautor tekstu miała znikomy udział lub wcale nie uczestniczyła w tworzeniu publikacji.