Nr 16 (9) 2017

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

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

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 16 (9) 2017

INTERNAL SECURITY REVIEW

WARSAW 16 (9) 2017

ISSN 2080-1335

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

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

„Przegląd Bezpieczeństwa Wewnętrznego" (PBW) znajduje się na liście czasopism naukowych Ministra Nauki i Szkolnictwa Wyższego z liczbą 5 punktów za umieszczone w nim publikacje. PBW można odnaleźć także w *Index Copernicus Journal Master List* z liczbą 53,77 punktów. Czasopismo jest również dostępne w bazach: *Central European Journal of Social Science and Humanities* i Polska Bibliografia Naukowa (PBN).

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

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

Numer zamknięto i oddano do druku w marcu 2017 r.

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

SPIS TREŚCI

I. ARTYKUŁY I ROZPRAWY

II. STUDIA I ANALIZY

CONTENTS

I. ARTICLES AND DISSERTATIONS

II. STUDIES AND ANALYSES

I
ARTYKUŁY I ROZPRAWY

Michał Wojnowski

Koncepcja wojny sieciowej Aleksandra Dugina jako narzędzie realizacji celów geopolitycznych Federacji Rosyjskiej

Wstęp

Od początku lat 90. XX w. w rosyjskich doktrynach geopolitycznych wojna sieciowa i walka informacyjna stały się głównymi środkami do osiągania celów państwa w polityce międzynarodowej, regionalnej i wewnętrznej. Według rosyjskich geopolityków współczesne konflikty polegają przede wszystkim na planowym i zamierzonym oddziaływaniu na przeciwnika w celu opanowania jego przestrzeni informacyjnej, w myśl zasady, że ten, kto kontroluje źródła informacji i infrastrukturę informacyjną znajdujące się na danym terytorium, jest w stanie panować nad nim wraz z jego zasobami[1]. Jest to możliwe dzięki długotrwałemu i systematycznemu oddziaływaniu informacyjnemu i informacyjno-psychologicznemu na poszczególne grupy społeczne. Celem tych działań jest takie ukształtowanie systemu wartości i sposobów postrzegania świata przez ludzi, aby od wewnątrz doprowadzić do rozbicia społeczeństwa przeciwnika i stworzyć warunki do realizacji celów agresora. Oddziaływanie informacyjne może również stanowić wstęp do podjęcia bardziej zaawansowanych przedsięwzięć o charakterze dyplomatycznym, ekonomicznym i militarnym[2].

Jedną z takich doktryn jest rosyjska teoria wojny sieciowej (ros. *сетевая война*) i sieciocentrycznej (ros. *сетецентрическая война*). Jej twórcą jest Aleksandr Dugin – wpływowy intelektualista, teoretyk rosyjskiej geopolityki i neoeurazjanizmu. W opinii autora ta doktryna stanowi odpowiedź na amerykańską teorię wojny sieciowej (ang. *Netwar*), którą sformułowali specjaliści z think tanku RAND Corporation – John Arquilla i David Ronfeldt. Pojęcie *Netwar* („netwojna", wojna sieciowa) wprowadzono w 1993 r. Według amerykańskich analityków ten termin odnosi się do nowej, wyłaniającej się formy konfliktu (i przestępczości) na poziomie społecznym, w której wykorzystuje się środki na poziomie poniżej progu regularnej, otwartej wojny dającego się w miarę jednoznacznie zidentyfikować, jak również sieciowe formy doktrynalne, organizacyjne i komunikacyjne. Strony uczestniczące w takich konfliktach składają się zazwyczaj z rozproszonych, często niewielkich grup nierzadko bez określonego scentralizowanego przywództwa oraz stosują odpowiadające im formy komunikacji, koordynacji i działań sieciowych. Walkę sieciową, z uwagi na wykorzystywanie środków niemilitarnych (m.in. informacji i narzędzi

[1] О.С. Ипатов, И.Ф. Кефели, И.М. Левкин, *Информационная геополитика на службе российского государства*, „Геополитика и безопасность" 2016, nr 2, s. 25.

[2] Ю.В. Косов, Ю.В. Вовенда, *Геополитические концепции информационного противоборства в российской общественной мысли*, „Управленческое консультирование" 2015, nr 10, s. 95–100; Л.Н. Кунакова, *Информационная война как объект научного анализа (понятие и основные характеристики информационной войны)*, „Альманах современной науки и образования" 2012, nr 6, s. 93–96; Л.В. Савин, *Горизонты войны*, w: *Геополитика. Информационно-аналитическое издание. Выпуск XXI: Война*, Л.В. Савин (red.), Москва 2013, s. 22–35; J. Potulski, *Współczesne kierunki rosyjskiej myśli geopolitycznej: między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, s. 275–292.

cybernetycznych) oraz zaangażowanie niescentralizowanych jednostek i grup niebędących reprezentantami ugrupowań, partii lub organizacji, nazywa się „konfliktem o niskiej intensywności”[3].

Wojna sieciowa może być prowadzona zarówno przez rządy i ich służby specjalne przeciwko wrogim grupom, jak i przez organizacje społeczne lub ugrupowania terrorystyczne przeciwko rządom i strukturom państwowym. Mogą ją toczyć również podmioty niepaństwowe, co wzbudza zainteresowanie i niepokój elit przywódczych państw, a także bloków o charakterze polityczno-militarnym. Tego rodzaju konflikt zakrojony na szeroką skalę może bowiem wpływać na interesy narodowe państw, nawet jeśli nie są one w niego bezpośrednio zaangażowane[4]. Należy podkreślić, że koncepcja Dugina nawiązuje również do teorii działań wojennych prowadzonych metodą sieciocentryczną (ang. *Network Centric Warfare*, NCW), która polega na transformacji przewagi informacyjnej, wspartej zaawansowaną technologią, w przewagę militarną, co odbywa się przez stworzenie i zastosowanie sieciowych struktur łączności między oddziałami wojskowymi prowadzącymi działania na dużej przestrzeni geograficznej. Tę teorię opracował w 1998 r. wiceadmirał Arthur Karl Cebrowski[5].

Głównym celem koncepcji opracowanej przez A. Dugina i związanych z nim ekspertów jest stworzenie „sieci eurazjańskiej”, która ma stanowić symetryczną odpowiedź na „sieć atlantycką” – czyli struktury i podmioty, których działania, w jego opinii, godzą w geopolityczne interesy Rosji. Według Dugina „sieć eurazjańska” ma być skutecznym narzędziem wojny sieciowej prowadzonej przeciwko Zachodowi. Za pomocą tego narzędzia będzie można zrealizować cele geopolityczne Federacji Rosyjskiej, którymi są: geopolityczne zneutralizowanie obszaru Europy Środkowo-Wschodniej z północną częścią Bałkanów, wyparcie wpływów Stanów Zjednoczonych z Europy, dążenie do podważenia integralności i skuteczności NATO oraz osłabienie spójności Unii Europejskiej na rzecz układów bilateralnych (np. Moskwa – Berlin, Moskwa – Paryż)[6].

Intencją autora niniejszego opracowania jest przedstawienie rosyjskiej koncepcji wojny sieciowej stworzonej przez Aleksandra Dugina oraz metod i środków, za których pomocą ta koncepcja jest realizowana w praktyce, co ma miejsce szczególnie w krajach członkowskich Paktu Północnoatlantyckiego. W artykule wykorzystano głównie publikacje rosyjskie dotyczące teorii wojny sieciowej, których autorami są A. Dugin i jego bliscy współpracownicy. Zawartą w nich treść starano się skonfrontować z analizami oraz różnorodnymi materiałami, które zamieszczono w prasie lub na portalach internetowych. Należy jednak pamiętać, że czerpana z nich wiedza często jest niepełna. Bywa też zniekształcana przez emocje towarzyszące debacie publicznej i elementy walki informacyjnej, w której biorą udział wszystkie strony konfliktu.

---

[3] E. Posłuszna, *Terroryzm w czasach globalizacji. Przyczynek do rozważań nad wojnami czwartej generacji*, „Przegląd Bezpieczeństwa Wewnętrznego” 2016, nr 15, s. 181; J. Arquilla, D. Ronfeldt, *Cyberwar is Coming!* „Comparative Strategy” 1993, nr 12, z. 2, s. 141–165. Por. J. Arquilla, D. Ronfeldt, *The Adwent of Netwar*, Santa Monica 1996, s. 5–6; R. Brose, *Cyberwar, Netwar, and the Future of Cyberdefense*, w: *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, M. Maybaum, A.M. Osula, L. Lindström (red.), Tallin 2015, s. 25–38; J. Arquilla, *To Build a Network*, „PRISM” 2014, nr 5, s. 22–34.

[4] K. Liedel, P. Piasecka, *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe” 2011, nr 1, s. 23.

[5] Odnośnie do NCW zob. A. Cebrowski, J. Garstka, *Network Centric Warfare: Its Origin and Future*, „US Naval Institute Proceedings Magazine” 1998, nr 124, z. 1, s. 28–35; J.R. Blaker, *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare*, London 2007, s. 21–129.

[6] А.Г. Дугин, *Геополитика постмодерна. Времена новых империй. Очерки геополитики XXI века*, Санкт-Петербург 2007, s. 338–339; А.Г. Дугин, *Принципы и стратегия грядущей войны* [online], http://katehon.com/ru/article/principy-i-strategiya-gryadushchey-voyny [dostęp: 2 XII 2016].

Teoria wojny sieciowej w ujęciu Aleksandra Dugina i jego współpracowników w latach 2008–2015

Aleksandr Dugin uchodzi za reprezentanta kremlowskich elit, którym jest bliska idea odbudowy Imperium Rosyjskiego. Ta idea stała się motywem przewodnim jego wieloletniej działalności politycznej, naukowej i publicystycznej. Ważnym wątkiem w biografii A. Dugina są jego powiązania z wysokimi rangą przedstawicielami resortów siłowych FR i administracji prezydenta Władimira Putina. Dugin oficjalnie przyznaje, że wiele projektów geopolitycznych przygotowywał na polecenie władz[7]. Wydaje się, że tę wypowiedź można odnieść także do projektu rosyjskiego modelu wojny sieciowej. Przedmiotowa koncepcja została zaprezentowana przez Dugina w 2008 r. w książce pt. *Geopolityka postmoderny* oraz w cyklu artykułów, który ukazał się na łamach kwartalnika „Wojny Informacyjne" («Информационные войны»). Oprócz A. Dugina autorami tych opracowań są jego bliscy współpracownicy: Gieorgij Gawrisz, Walerij Korowin i Paweł Zarifullin. Warto podkreślić, że są oni jednocześnie teoretykami i praktykami walki informacyjnej i należą do takich organizacji, jak Międzynarodowy Ruch Eurazjański (ros. Международное Евразийское движение, МЕД), Eurazjański Związek Młodzieży (ros. Евразийский союз молодёжи, ECM) i Klub Izborski (ros. Изборский клуб)[8].

Należy jednak pamiętać, że adaptując zachodnie teorie, Rosjanie kierują się własnymi założeniami i logiką, przystosowując je do własnych potrzeb. Taki zabieg umożliwia z jednej strony maskowanie metod doskonalonych przez dziesięciolecia przez radzieckie służby specjalne, a z drugiej – ich sankcjonowanie dzięki zapożyczaniu zachodnich osiągnięć i przysposabianiu ich do własnych celów, co zarazem podkreśla stosowanie przez Rosję nowoczesnych metod i środków walki oraz utrwala pogląd, jakoby była ona ofiarą agresji informacyjnej Zachodu[9].

---

[7] А.Г. Дугин, *Стратегические выводы Прямой Линии Путина* [online], http://evrazia.org/article/2505 [dostęp: 2 XII 2016]. Por. A. Umland, *Aleksandr Dugin's Transformation from a Lunatic Fringe Figure into a Mainstream Political Publicist, 1980–1998: A Case Study in the Rise of Late and Post-Soviet Russian Fascism*, „Journal of Eurasian Studies" 2010, nr 1, s. 144–152; M. Wojnowski, *Aleksandr Dugin a resorty siłowe Federacji Rosyjskiej. Przyczynek do badań nad wykorzystaniem geopolityki przez cywilne i wojskowe służby specjalne we współczesnej Rosji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 11–38. Szerzej na temat kierowanych przez Dugina instytucji naukowych, think tanków i realizowanych tam projektów badawczych zob. V. Rossman, *Moscow State University's Department of Sociology and the Climate of Opinion in Post–Soviet Russia*, w: *Eurasianism and the European Far Right: Reshaping the Europe – Russia Relationship*, M. Laruelle (red.), London 2015, s. 55–77; M. Laruelle, *The Izborsky Club, or the New Conservative Avant-Garde in Russia*, „The Russian Review" 2016, nr 75, s. 626–644.

[8] А.Г. Дугин, *Геополитика постмодерна*…, s. 321–346. Por. А.Г. Дугин, *Теоретические основы сетевых войн*, „Информационные войны" 2008, nr 1, s. 2–10; tenże, *Сетецентричные войны*, „Информационные войны" 2008, nr 1, s. 10–17; Г.Б. Гавриш, *Трансформация механизмов обеспечения национальной безопасности в условиях постмодерна. Институциональные аспекты*, „Информационные войны" 2008, nr 2, s. 24–37; П. Зарифуллин, *Сетевая война на Северном Кавказе*, „Информационные войны" 2008, nr 2, s. 37–42; В. Коровин, *Сетевая война Америки против России на примере Чечни,* „Информационные войны" 2008, nr 2, s. 42–47. Kwartalnik jest wydawany od 2007 r. przez Akademię Informacyjnej Samoobrony wespół z Rosyjską Akademią Nauk i Akademią Nauk Wojskowych, która ściśle współpracuje z Ministerstwem Obrony i Sztabem Generalnym Sił Zbrojnych FR. Periodyk jest bezpłatnie dystrybuowany do instytucji państwowych i wojskowych. W skład rady naukowej i kolegium redakcyjnego kwartalnika, oprócz Aleksandra Dugina, wchodzą także wysocy rangą wojskowi i przedstawiciele służb specjalnych (m.in. generał armii Mahmut Gariejew i Władimir Szulc, który w latach 1999–2000 był naczelnikiem Akademii FSB, następnie do 2003 r., pełnił funkcję sekretarza stanu i zastępcy dyrektora FSB). Zob. M. Wojnowski, *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 15.

[9] J. Darczewska, *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*,

Aby zrozumieć rosyjską koncepcję wojny sieciowej, konieczne jest najpierw przedstawienie jej podstaw filozoficznych. Według A. Dugina stosunki społeczne we wszystkich cywilizacjach opierają się na przeciwieństwie dwóch paradygmatów: hierarchii i entropii. Pojęcie hierarchii rosyjski geopolityk odnosi do wszelkich form organizacji społeczeństw, państw i cywilizacji, które tworzą jednolite, zamknięte, hierarchiczne i scentralizowane systemy. Przeciwieństwo paradygmatu hierarchii stanowi paradygmat entropii, który jest miarą stopnia nieuporządkowania, chaosu i niejednolitego charakteru danego systemu społecznego oraz zachodzących w nim spontanicznych (samorzutnych) procesów. Paradygmat entropii określa wszelkie procesy i zjawiska mające na celu destrukcję hierarchii. Dlatego też, zdaniem A. Dugina, sieć należy rozpatrywać przez paradygmat entropii, ponieważ jest on elastyczną formą współdziałania różnych komórek (ludzie, grupy społeczne, organizacje, stowarzyszenia itp.) charakteryzującą się stałą wymianą informacji i, w odróżnieniu od struktur hierarchicznych, ciągłą zdolnością do transformacji. Sieci stanowią więc informacyjno-techniczną i informacyjno-psychologiczną przestrzeń, w której następuje pozyskiwanie, obróbka i wymiana informacji. W opinii A. Dugina sieć jest postmodernistycznym, postindustrialnym bytem, który zastępuje zarówno hierarchiczne struktury tradycyjnych społeczności, jak i formy organizacji społeczeństw modernistycznych, utożsamianych m.in. przez państwo i jego instytucje. Sieć wpisuje się w paradygmat entropii także dlatego, że jest związana z rozprzestrzenianiem się destrukcyjnych wzorców, które niszczą porządek państwa. Istotą wojny sieciowej jest zatem uzyskanie kontroli nad przestrzenią informacyjno-techniczną i informacyjno-psychologiczną nieprzyjaciela za pomocą sieci funkcjonujących w jego społeczeństwie, co umożliwia skłonienie go do podjęcia działań korzystnych dla agresora. To z kolei może w przyszłości doprowadzić do osiągnięcia ostatecznego celu wojny sieciowej, czyli uzyskania kontroli nad obszarem, który de facto należy do wroga.

Według Dugina do prowadzenia wojny sieciowej niezbędne jest pozyskanie, kontrolowanie lub stworzenie następujących rodzajów sieci:

1) sieci pierwotnych, które tworzą grupy przestępcze, mniejszości etniczne i religijne. Do tej kategorii zaliczają się także sekty i związki wyznaniowe, które nie mają jasno określonego statusu prawnego, co pozwala skutecznie maskować ich destrukcyjną działalność,
2) sieci wtórnych, czyli organizacji pozarządowych, fundacji, „fabryk myśli", organizacji zajmujących się obroną praw człowieka, stowarzyszeń i organizacji o charakterze naukowo-badawczym oraz ruchów młodzieżowych. Są one dopełnieniem sieci pierwotnych. Zaletą tych sieci jest to, że ich oficjalna działalność, pomimo wsparcia finansowego i logistycznego otrzymywanego z zagranicy, mieści się w granicach prawa, co znacznie utrudnia zdemaskowanie ich wywrotowej aktywności,
3) sieci agentury wpływu, które powinny funkcjonować bez konieczności werbunku poszczególnych osób. W warunkach wojny sieciowej funkcję agentury wpływu często pełni tzw. aktywna mniejszość (ros. *активное меньшинство*) wchodząca w skład danej sieci. Jej działania aktywizuje się np. przez symulowanie zainteresowania jej liderem lub grupą przywódczą, zamieszczając wzmianki na ich temat w lokalnej prasie, zapraszając na konferencje naukowe lub okazując

Warszawa 2015, s. 14–15; T.L. Thomas, *The Russian Understanding of Information Operations and Information Warfare*, w: *Volume III of Information Age Anthology: The Information Age Military*, D.S. Alberts, D.S. Papp (red.), Washington 2001, s. 783.

zainteresowanie pomysłami lub ideami, które są dla nich cenne itd. Te działania wpisują się w proces kreowania tzw. sztucznej uwagi. To pozwala zyskiwać przychylność osób lub grup przydatnych dla agresora bez potrzeby ich werbowania. Następnie poddaje się ich indoktrynacji ideologicznej za pomocą idei korzystnych z punktu widzenia celów i interesów podmiotu prowadzącego wojnę sieciową. Takie działanie utwierdza ludzi w przekonaniu, że postępują słusznie, realizując zamiary agresora. Nie oznacza to wcale rezygnacji z klasycznej agentury wpływu[10].

A. Dugin podkreśla, że główną cechą wojny sieciowej jest dążenie do maksymalnej synchronizacji działań, środków i metod. Operacje charakterystyczne dla tej formy konfliktu są prowadzone jednocześnie w czterech przestrzeniach, tj.:

1) w przestrzeni fizycznej, czyli tradycyjnym obszarze działań wojennych obejmującym środowisko geograficzne: ląd, morze, ziemię, powietrze i kosmos,
2) w przestrzeni informacyjnej, w której informacje są generowane, następnie przekształcane i dystrybuowane. Obejmuje ona także wszelką infrastrukturę informatyczną, mechanizmy zdobywania lub pozyskiwania informacji oraz matematyczne modele jej obróbki itp.,
3) w przestrzeni kognitywnej, obejmującej indywidualną i grupową świadomość, procesy poznawcze, mechanizmy podejmowania decyzji i motywacje działań zarówno poszczególnych osób, jak i grup społecznych,
4) w przestrzeni społeczno-kulturowej, która jest polem współdziałania ludzi, organizacji społecznych i politycznych. To pole jest oparte na historycznych, kulturowych i religijnych wartościach, które mogą być kształtowane przez stronę prowadzącą wojnę sieciową. W opinii rosyjskich teoretyków sfera kognitywna i społeczno-kulturowa są najważniejsze dla powodzenia operacji[11].

Zdobycie przewagi w tych przestrzeniach jest gwarantem osiągnięcia zwycięstwa w wojnie sieciowej. Według A. Dugina i jego współpracowników Rosja może skutecznie przeciwstawić się wojnie sieciowej Zachodu, jeśli zostaną spełnione dwa warunki. Po pierwsze, należy stworzyć „sieć eurazjańską", która ma być symetryczną odpowiedzią na „sieć atlantycką". W tym celu rosyjski geopolityk w 2008 r. postulował powołanie specjalnej grupy, w której skład powinni wejść wysocy rangą urzędnicy państwowi, najlepsze (tzw. posłannicze, zaangażowane) kadry wywodzące się z rosyjskich służb specjalnych oraz autorytety – intelektualiści, uczeni, politolodzy, dziennikarze, artyści i działacze kultury. Model „sieci eurazjańskiej", przeciwstawiany „sieci atlantyckiej", powinien łączyć podstawowe cechy amerykańskiego postmodernizmu i środki walki prowadzonej metodą sieciocentryczną z rosyjską specyfiką. Symetryczne do atlantycko-amerykańskich wektory „rażenia informacyjnego" powinny być zorientowane

[10] А.Г. Дугин, В. Коровин, А. Бовдунов, *Сетевые войны*…, s. 55–57; А.Г. Дугин, *Русская война*…, s. 204–207; tenże, *Теоретические основы сетевых войн*…, s. 6–7. Por. О.С. Андреева, *Неправительственные организации как инструмент глобальной политики*, „Власть" 2009, nr 4, s. 54–57; А.О. Наумов, *Международные неправительственные организации и проблемы глобального управления*, „Государственное управление" 2013, nr 9, s. 49–76. Na temat manipulacji świadomością społeczną przez sekty i grupy o charakterze okultystycznym zob. В.Е. Лепский, А.М. Степанов, *Особенности рефлексивных процессов в культовых организациях*, „Рефлексивные процессы и управление" 2002, nr 2, s. 59–73.

[11] А.Г. Дугин, В. Коровин, А. Бовдунов, *Сетевые войны*…, s. 49–51; А.Г. Дугин, *Русская война*…, s. 187–191. Por. Л.В. Савин, *Сетецентричные войны – от концепции к спецоперациям*, w: *Геополитика. Информационно-аналитическое издание. Выпуск IV: Безопасность*, Л.В. Савин (red.), Москва 2010, s. 70–78.

w dokładnie przeciwnym kierunku. Warunkiem skuteczności modelu ma być „postmodernizacja" rosyjskich sił zbrojnych, służb specjalnych, instytucji państwowych, systemów informacyjnych, komunikacyjnych itp. Dugin podkreśla, że bez tego wysiłku Rosja jest skazana na kolejne klęski, ponieważ wojnę sieciową można wygrać tylko środkami sieciowymi, adaptując je do własnych realiów i celów oraz skutecznie wykorzystując nowoczesne technologie[12].

Po drugie, na szczeblu międzynarodowym i regionalnym należy wdrożyć realizację rosyjskiego projektu światopoglądowego, który byłby uniwersalny, czyli możliwy do przyjęcia przez inne narody, oraz stanowiłby alternatywę dla liberalnej ideologii lansowanej przez Stany Zjednoczone i Unię Europejską oraz amerykańskiego mitu o „wolności i demokracji"[13]. Rosyjscy eksperci podkreślają, że w warunkach społeczeństwa informacyjnego takie „platformy wartości" (ros. *ценностные платформы*) pełnią funkcję systemów operacyjnych, na których podstawie formułuje się kody geopolityczne poszczególnych państw, tworzy się informacyjną, kognitywną i społeczno-kulturową przestrzeń, w której funkcjonują sieci społeczne i różne organizacje. To pozwala konsolidować społeczeństwo na podstawie wspólnego światopoglądu i systemu wartości. Według Gieorgija Gawrisza „platforma wartości" dla „geopolitycznej międzynarodówki" z Rosją stojącą na jej czele powinna bazować na takich wartościach, jak: geopolityczna koncepcja świata wielobiegunowego (w opozycji do wizji świata jednobiegunowego, reprezentowanej przez USA), konserwatyzm, eurazjatycka kultura i tożsamość religijna (jako alternatywa dla „zachodniego nihilizmu i indywidualizmu") oraz antyglobalizm (jako sprzeciw wobec ekspansjonistycznych dążeń „atlantyckiej oligarchii")[14].

Do stworzonej przez A. Dugina koncepcji wojny sieciowej nawiązał w 2015 r. Aleksandr Bowdunow – działacz Eurazjańskiego Związku Młodzieży. Jego opracowanie pt. *Cywilizacyjne porachunki* zasługuje na szczególną uwagę. Zawiera ono rozważania autora na temat możliwości prowadzenia wojny sieciowej przez Rosję w Europie oraz zalecenia, w jaki sposób państwo rosyjskie może ją wykorzystać do realizacji własnych celów geopolitycznych:

> Nie ma żadnej wątpliwości, że w chwili obecnej wojnę sieciową są zdolne prowadzić tylko Stany Zjednoczone przeciwko całej reszcie świata. Nie oznacza to jednak, że żaden inny ośrodek geopolityczny nie jest zdolny do sieciowej odpowiedzi. Rozpatrzmy możliwości prowadzenia wojny sieciowej przez Rosję w Europie i zbadajmy, w jaki sposób nasz kraj może wykorzystać daną technologię. Po pierwsze, do prowadzenia wojen sieciowych niezbędne są dla nas sieci organizacyjne i informacyjne. Skąd je wziąć? Można wykorzystać posiadane już sieci. W tym przypadku ograniczeni będziemy pewnymi ideami, znajdującymi się u podstaw danych sieci. Trzeba będzie te sieci dopiero podporząd-

[12] А.Г. Дугин, *Геополитика постмодерна*…, s. 338–340; А.Г. Дугин, В. Коровин, А. Бовдунов, *Сетевые войны*…, s. 66–67; А.Г. Дугин, *Русская война*…, s. 253–260.

[13] А.В. Манойло, *Ценностные основы управления межцивилизационными конфликтами: российская модель*, „Международные отношения" 2012, nr 1, s. 32–43; О.Г. Карпович, А.В. Манойло, Г.Ю. Филимонов, *Технологии «мягкой» силы на вооружении США: ответ России*, Москва 2015, s. 475–484.

[14] Г.Б. Гавриш, *Трансформация механизмов*…, s. 34–35. Szerzej ta problematyka została omówiona przez autora w następujących opracowaniach: Г.Б. Гавриш, *«Философия неоевразийства в контексте парадигм «пространства» и «времени»* [online], http://evraz-info.narod.ru/30.htm [dostęp: 10 XII 2016]; tenże, *Онтология неоевразийского политико-правового дискурса*, Ростов-на-Дону 2006. Por. *Русская доктрина. Государственная идеология эпохи Путина*, А.Б. Кобяков, В.В. Аверьянов (red.), Москва 2016, s. 83–87, 152–194; О.Н. Яницкий, *Идеология и сеть*, „Власть" 2016, nr 1, s. 30–36.

kować naszej kontroli. Można spróbować tworzyć własne sieci na terytorium przeciwnika, co jest trudniejsze, ale będą to już nasze sieci, od początku przez nas kontrolowane. Aby wyjaśnić, do jakich celów dążymy, i zrozumieć, co znajdzie się u podstaw doktrynalnego poziomu naszej wojny w Europie, należy pojąć znaczenie toczącej się wojny, istotę konfliktu. Konflikt pomiędzy Rosją i Zachodem posiada dwa najistotniejsze wymiary: geopolityczny i cywilizacyjny. Rola wymiaru cywilizacyjnego w ostatnim czasie wzrosła tak, że coraz częściej mówi się o konflikcie pomiędzy cywilizacjami. W związku z absolutną niezgodnością podstawowych założeń cywilizacyjnych, ostatecznym rozwiązaniem tego konfliktu może być tylko zniszczenie jednego z jego uczestników. W tym przypadku pomińmy same przesłanki konfliktu. A zatem, stwierdzając cywilizacyjny charakter konfliktu pomiędzy Rosją i Zachodem, stawiamy sobie za cel zniszczenie Zachodu w jego współczesnym kształcie jako cywilizacji[15].

Rosyjska koncepcja wojny sieciowej została oparta na fundamencie ideologicznym, który stanowią różnice między „rosyjską cywilizacją eurazjatycką" a „cywilizacją atlantycką" utożsamianą przez Stany Zjednoczone i ich sojuszników. Rosyjska polityka informacyjna polega na kreowaniu i promowaniu narracji, w której światu zagraża z jednej strony radykalizm religijny i polityczny (islamiści, faszyści, nacjonaliści), a z drugiej – postmodernistyczny liberalizm Zachodu, za którym kryją się amerykańskie dążenia do panowania nad światem. W tej narracji Rosja jest prezentowana jako główny obrońca stabilnego ładu międzynarodowego, suwerenności państwowej, religii i tradycyjnego modelu rodziny[16].

Paradygmat ideologiczny odgrywa więc najważniejszą rolę w działaniach opisywanych przez Bowdunowa. Jego zdaniem, aby skutecznie prowadzić wojnę sieciową w Europie, należy wykorzystać sieci pierwotne, które są ukierunkowane na destrukcję współczesnej europejskiej tożsamości cywilizacyjnej. W tym celu trzeba wspierać i wykorzystywać wszelkie tendencje i ruchy separatystyczne, ugrupowania o charakterze neonazistowskim, rasistowskim, antyglobalistycznym, a także grupy ekologów, eurosceptyków, izolacjonistów, nielegalnych emigrantów, sekty oraz organizacje mniejszości narodowych i etnicznych. Jak już powiedziano, sieć stanowi przeciwieństwo państwa jako struktury hierarchicznej, od której stara się przejąć część suwerenności. Według rosyjskiego eksperta ten czynnik może być najistotniejszy dla rosyjskich działań w Europie, ponieważ antypaństwowość sieci jest wpisana w ideologię wielu „antysystemowych" organizacji i grup. Znajduje ona świadomą akceptację osób należących do tych grup, co powoduje, że w imię ideologii są oni w stanie zniszczyć własne państwo. Dlatego też z punktu widzenia Rosji konieczne jest, aby to przekonanie ugruntowywać przez implementowanie go do świadomości osób tworzących daną sieć wirtualnej ideologii opartej na założeniu, że państwo, do którego należą, ma charakter opresyjny. Aby osiągnąć ten cel, powinno się zastosować np. ideologię „okupacyjnego rządu syjonistycznego" (ros. *сионистское оккупационное правительство*), co jest szczególnie skuteczne

[15] Cyt. za: А. Бовдунов, *Цивилизационные разборки* [online], http://evrazia.org/article/230 [dostęp: 10 XII 2016].

[16] W. Rodkiewicz, J. Rogoża, *Potiomkinowski konserwatyzm. Ideologiczne narzędzie Kremla*, Warszawa 2015, s. 19–20; Д.А. Коновалов, И.В. Мельникова, *Сравнительный анализ направлений современной российской консервативной общественно-политической мысли*, „Вестник Омского университета" 2013, nr 1, s. 181–188; О.Б. Подвинцев, *О моде на консерватизм в постсоветской России и разнообразии её природы*, „Вестник Пермского Университета" 2015, nr 2, s. 27–33.

wobec organizacji prawicowych i skrajnie prawicowych. W ten sposób w świadomości członków takich grup tworzy się obraz każdej „obecnej władzy", która jest postrzegana jako narzędzie realizujące interesy Żydów, masonów i różnych mafii politycznych[17]. Następnie wobec tak określonego przeciwnika, którym w świadomości tych ludzi staje się ich własne państwo, „operatorzy sieci" kierujący operacjami w ramach wojny sieciowej sugerują członkom kontrolowanych przez nich struktur stosowanie działań mieszczących się w ramach strategii oporu niekierowanego. Jej istota polega na tym, że system organizacyjny opiera się na autonomicznie funkcjonujących komórkach, bez centralnej kontroli i centralnego zarządzania. Wszystkie jednostki i komórki działają niezależnie od siebie i nigdy nie zgłaszają się do centrali lub przywódcy po instrukcje. Warunkiem funkcjonowania takiej sieci jest to, że zaangażowane w nią osoby muszą dokładnie wiedzieć, jakie działania i przeciwko komu mają podejmować. Dlatego też te osoby mają podobny światopogląd, ten sam cel i są zwolennikami tej samej ideologii[18].

W odróżnieniu od prawicy lewica interpretuje sieć jako alternatywę wobec analogicznych sieci globalistycznych, przedstawionych choćby w książce pt. *Imperium* autorstwa marksistów Antonia Negri i Michaela Hardta[19]. Jak zauważa A. Bowdunow, prowadzenie wojny sieciowej ułatwiają procesy dezintegracyjne zachodzące w UE. Warto podkreślić, że frakcje Parlamentu Europejskiego łączą przedstawicieli różnych krajów o podobnych przekonaniach politycznych, jednak nie wszystkie te sieci akceptują Unię Europejską w jej obecnym kształcie, odmawiając poparcia dla jej polityki. W opinii Bowdunowa w Parlamencie Europejskim istnieje silna frakcja sieci złożonych z deputowanych o przekonaniach eurosceptycznych lub wrogich wobec UE, która ma wpływ na całokształt jej polityki. Rosyjski geopolityk przyznaje, że byłoby wręcz niezrozumiałe, aby nie spróbować jej wykorzystać[20].

Po drugie, według Bowdunowa należy tworzyć sieci wtórne (informacyjne i organizacyjne) na podstawie specjalnie do tego celu przygotowanej ideologii. Chodzi o stworzenie tożsamości łączącej ich członków. W opinii Bowdunowa ważne jest doświadczenie zdobyte podczas tworzenia sieci ruchu eurazjańskiego w Europie, co zapoczątkował Międzynarodowy Ruch Eurazjański. Zdaniem rosyjskiego geopolityka eurazjanizm jest ideologią znaną w środowisku międzynarodowym, dlatego też może zostać zaakceptowany przez współczesnego Europejczyka. W związku z tym, że ideologia eurazjańska stanowi platformę ideową, na której opiera się tożsamość sieci eurazjańskich, to sieci te rozmywają tożsamość europejską, tworząc „piątą kolumnę" Rosji na Zachodzie.

[17] Tamże. Ideologia okupacyjnego rządu syjonistycznego – zbiór idei i wyobrażeń kształtujących światopogląd danej grupy ludzi na podstawie teorii spiskowych. Zakłada ona, że rzeczywistość polityczna, ekonomiczna i społeczna jest kreowana przez żydowskie, masońskie i okultystyczne organizacje działające na rzecz Nowego Porządku Świata (ang. *New World Order*, NWO). Przykładowo, w USA członkowie grup „patriotycznych" wierzą m.in. w tworzenie na terenie Stanów Zjednoczonych obozów koncentracyjnych mających w bliżej nieokreślonej przyszłości pomieścić „niepokornych obywateli". Te osoby dają także wiarę fantastycznym teoriom dotyczącym zatruwania żywności, wody i powietrza psychoaktywnymi substancjami, co ma ułatwić ogłupienie nieświadomej spisku większości. Niechęć tych grup jest skierowana ku administracji, rządowi i państwu jako systemowi opresji. Rezultatem tego przekonania jest m.in. tworzenie klubów strzeleckich i milicji obywatelskich skupiających aktywistów, którzy doskonalą sposoby walki na wypadek konfrontacji z rządem. Zob. J. Kaplan, *Encyclopedia of White Power: A Sourcebook on the Radical Racist Right*, Walnut Creek–Lahnam–New York–Oxford 2000, s. 367–374.

[18] P.W. Gray, *Leaderless Resistance, Networked Organization, and Ideological Hegemony*, „Terrorism and Political Violence" 2013, nr 25, s. 655–671. Por. L.R. Beam, *Leaderless Resistance*, „The Seditionist" [online] 1992, nr 12, http://www.louisbeam.com/leaderless.htm [dostęp: 16 II 2017].

[19] M. Hardt, A. Negri, *Empire*, Cambridge–London 2000, s. 160–183, 260–280.

[20] А. Бовдунов, *Цивилизационные разборки*…

Aby je stworzyć, należy pozyskać europejskich intelektualistów, którzy mają zdolności opiniotwórcze. Zdaniem rosyjskich geopolityków najbardziej perspektywiczne w tym względzie są organizacje i ruchy polityczne noszące wspólne miano „Nowej Prawicy" (reprezentowane przez np. Alaina de Benoista, Roberta Steuckersa i innych). Mimo że ich oblicze ideowe ma korzenie europejskie, co czyni te organizacje wiarygodnymi w ojczystych krajach, to są one prorosyjskie i antyamerykańskie. Dlatego też mogą być dla Rosji źródłem lub nośnikiem narracji dla niej pożądanej, której przekazywanie będzie ugruntowywać ideową tożsamość członków sieci, co pozwoli manipulować jej działalnością w sposób korzystny dla FR[21].

Nie mniej perspektywiczne jest włączenie do tego rodzaju działalności także intelektualistów lewicowych. Oprócz ideologii równie istotnym czynnikiem integrującym członków sieci są utrwalane w ich świadomości wyobrażenia i mity. Należy konsekwentnie operować takimi pojęciami i obrazami, jak „człowiek legenda" (np. Ian Stuart Donaldson dla skrajnej prawicy lub Ernesto Che Guevara dla lewicy), i tworzyć takie ikony. Bardzo pomocne jest także tworzenie anegdot, rozpowszechnianie plotek, bajek i różnorakich wymysłów na temat przeciwnika, co stanowi element poziomu narracyjnego wojny sieciowej. Manipulowanie tożsamością jest jednym z najważniejszych zabiegów stosowanych w tego rodzaju konflikcie. Aby manipulacja była skuteczna, jej obiekt musi zostać przeniesiony ze środowiska realnego do wirtualnej przestrzeni, gdzie istnieje możliwość jego modyfikacji. Taka sfabrykowana tożsamość nie powinna być związana ze skomplikowanymi ideologiami. Nie powinna też odwoływać się do racjonalnego myślenia, lecz odpowiadać mentalności współczesnego człowieka, tzn. uosabiać świat gier komputerowych, filmów itp. W tym przypadku ideologię należy zastąpić modą, marką i stylem. Mani-

[21] Tamże. Por. A. Умланд, *Заблуждения западных апологетов Путина: пугало «русофобии» и внешняя критика нынешнего руководства Кремля*, „Форум новейшей восточноевропейской истории и культуры" 2015, nr 2, s. 261–267. Temu celowi służą również Czwarta Teoria Polityczna (dalej: 4 TP) i tzw. dynamiczny konserwatyzm – wirtualne ideologie tworzone w celu pozyskania dla Rosji zachodniego audytorium, aktywizacji „pożytecznych idiotów" itd. 4 TP stanowi realizowany przez A. Dugina projekt uniwersalnej ideologii, która łączy wszelkie nurty i ruchy przeciwne liberalizmowi, postmodernizmowi, społeczeństwu postindustrialnemu i globalizmowi wraz z jego podstawami logistycznymi i technologicznymi. 4 TP ma jasno sprecyzowany paradygmat geopolityczny: wspomniane wartości utożsamia ze Stanami Zjednoczonymi i NATO, stanowiąc próbę wykorzystania wszelkich podmiotów sprzeciwiających się polityce bloku atlantyckiego, bez względu na ich oblicze ideowe i cele, co w praktyce służy geopolitycznym interesom Rosji. W konfrontacji z liberalną cywilizacją atlantycką Rosja została usytuowana na pozycjach „konserwatywnych". Według Dugina „konserwatystą" jest bowiem każdy, kto sprzeciwia się „atlantyckiej hegemonii". W ramy 4 TP wpisują się więc wszelkie prawicowe, lewicowe, metapolityczne ideologie, które kontestują obecny układ stosunków międzynarodowych („hegemonia Stanów Zjednoczonych"), w tym eurazjanizm i narodowy bolszewizm. Zob. А.Г. Дугин, *Четвёртая политическая теория. Россия и политические идеи XXI века*, Санкт-Петербург 2009, s. 14–19, 78–80, 93–94, 98–100; tenże, *Философия глобализма – философия контрглобализма (доклад на международной конференции «Глобализм и глобальная безопасность», г. Москва, декабрь 2000 г., Храм Христа Спасителя)*, w: *Основы евразийства*, А.Г. Дугин (red.), Москва 2002, s. 548–557. Jak ujawnił na swoim blogu Anton Szechowcow, były członek Eurazjańskiego Związku Młodzieży, sam Dugin nie wierzy w 4 TP, traktując ją jako narzędzie realizacji konkretnych celów geopolitycznych. Zob. A. Shekhovtsov, *Russian Fascist Aleksandr Dugin's Dreams of Dictatorship in Russia* [online], http://anton-shekhovtsov.blogspot.com/2014/02/russian-fascist-aleksandr-dugin-is.html [dostęp: 11 XII 2016]. Dynamiczny konserwatyzm jest natomiast terminem stosowanym przez kremlowskich polittechnologów dla określenia wszelkich form konserwatyzmu, i podobnie jak 4 TP jest atrakcyjną ofertą ideologiczną skierowaną do europejskich elit o nastawieniu eurosceptycznym, antyamerykańskim oraz antyglobalistycznym, broniących tradycyjnych wartości chrześcijańskich. Zob. В.В. Аверьянов i in., *Другая холодная война. Стратегия для России*, „Изборский клуб" 2014, nr 10, s. 40.

pulując taką chwiejną tożsamością opartą tylko na komercji i sposobie życia, można wpływać na zachowanie ludzi i programować ich czyny w celu pożądanym przez podmioty prowadzące operacje sieciowe[22].

Po trzecie, jak postuluje Bodunow, należy systematycznie rozbudowywać i doskonalić infrastrukturę sieciową. Sieć składa się z wielu komórek, z których każda wypełnia swoje – nieraz bardzo precyzyjnie określone, wymagające specjalistycznych umiejętności – zadanie. Najbardziej rozpowszechnioną formą działania w wojnach sieciowych jest taktyka „roju", która polega na zsynchronizowanym ataku wielu elementów sieci na przeciwnika z uwzględnieniem celu, miejsca i czasu. Taktyka „roju" może być stosowana zarówno dyspersyjnie, jak i centralnie, co oznacza, że atak informacyjny może być prowadzony z różnych stron internetowych albo z jednej. Dyspersyjna forma ataku jest bardziej skuteczna, ponieważ wśród postronnych obserwatorów i samych członków sieci wywołuje iluzję niezależności. Dlatego też sieci powinny być zróżnicowane, dzięki czemu jest możliwe „podłączenie" (od ros. *осетевить*, dosł. 'opleść siecią') do nich jak największej liczby osób, grup i organizacji. Aby to osiągnąć, konieczne jest tworzenie struktur według kryterium zróżnicowania społecznego. Dlatego też tworzy się sieci złożone z przedstawicieli elit, świata nauki, ugrupowań politycznych, a także zwykłych ludzi, subkultur, ruchów młodzieżowych itd. Równocześnie należy rozwijać główne atuty takiej struktury: wymianę informacji, jej interaktywność i zaangażowanie wszystkich jej podmiotów. W tym celu jako uzupełnienie istniejących już sieci i sposobów ich komunikacji należy tworzyć wciąż nowe. To dotyczy głównie stron internetowych i interaktywnych agencji sieciowych. Należy samodzielnie tworzyć takie agencje, w których autorami materiałów są sami członkowie sieci. To zwiększa zaufanie wobec agencji ze strony osób tworzących sieć i ich integruje (poziom społeczny wojny sieciowej), a także umożliwia twórcom agencji i stron internetowych oraz samym członkom sieci dotarcie do zawsze aktualnych informacji. Według Bowdunowa przykładem tego typu działań jest organizowanie portali i forów różnych ugrupowań, których wspólną cechą jest np. niezadowolenie i kontestowanie otaczającej rzeczywistości, sytuacji politycznej w danym państwie lub regionie itp. Wygoda prowadzenia takiej działalności w Europie polega na tym, że Internet jest tam powszechnie dostępny. Oprócz tego – stwierdza Bowdunow – do kontaktów w sieci Europejczycy z zasady wykorzystują często jeden język – angielski, co bardzo ułatwia prowadzenie działalności. Istotne jest jednak wykorzystywanie wszystkich języków europejskich. Szczególnie dotyczy to „pracy" nad aktywizacją i radykalizacją ruchów separatystycznych, ponieważ niezbędne jest tu używanie języków narodowych. Portale, które łączą różne ruchy separatystyczne, powinny być natomiast prowadzone co najmniej w kilku językach narodowych oraz w języku angielskim. Dookoła „efektywnej" i „obiecującej" witryny internetowej powinny powstać nie tylko sieć, lecz także trend w życiu politycznym i kulturalnym. Dlatego też sfera informacyjna wojny sieciowej jest tak ważna, od działań informacyjnych bowiem zależy skuteczność ich rezultatów w sferze kognitywnej i społeczno-kulturowej[23].

---

[22] А. Бовдунов, *Цивилизационные разборки*… Por. Д.С. Мартьянов, *Виртуальные ценности: структура, динамика, противоречия*, „Труды Санкт-Петербургского государственного института культуры и искусств" 2015, nr 206, s. 319–327; А.Г. Дугин, *Логос и мифос. Социология глубин*, Москва 2010, s. 236–237; tenże, *Четвёртая политическая теория*…, s. 91–92.

[23] А. Бовдунов, *Цивилизационные разборки*…. Por. А.В. Манойло, *Сепаратизм как вызов и угроза международной безопаности*, „Геополитический журнал" 2014, nr 7, s. 11–24.

Należy podkreślić, że „sieć eurazjańska" tworzona przez Aleksandra Dugina i jego współpracowników ma charakter międzynarodowy, co umożliwia szerokie oddziaływanie na szczeblu globalnym. Prawdopodobnie takie organizacje, jak Międzynarodowy Ruch Eurazjański, Eurazjański Związek Młodzieży oraz struktury skrajnej prawicy i lewicy w Europie, wymienione przez Bowdunowa jako „perspektywiczne", stanowią jedynie podsystem nowej, większej struktury sieciowej, która nosi nazwę Globalnego Sojuszu Rewolucyjnego (ang. Global Revolutionary Alliance, ros. Глобальный революционный альянс), czyli swoistej „organizacji bez organizacji"[24].

Globalny Sojusz Rewolucyjny (dalej: GSR) jest organizacją nowego typu, co podkreślają jego twórcy w manifeście opublikowanym w Internecie:

> Podmiotem nowej światowej rewolucji musi być światowa kontrelita. Przeznaczeniem tej kontrelity jest sformować Globalny Sojusz Rewolucyjny (GSR) jako krystalizację wywrotowych działań destrukcyjnych, nakierowanych na zdemolowanie dzisiejszego systemu światowego i pozbawienie władzy światowej oligarchii i jej świty. GSR powinien być organizacją nowego typu, właściwą dla warunków XXI wieku. Ani partią, ani ruchem, ani zakonem, ani lożą, ani sektą, ani wspólnotą religijną, ani grupą etniczną lub kastą – jako że formy organizacji zbiorowej poprzednich epok nie mogą służyć za model dla jego struktury. GSR powinien być strukturą sieciową, bez jednego centrum kontrolnego, bez określonego zespołu stałych członków, żadnej sterującej grupy lub stałego personelu, bez jasno zdefiniowanego algorytmu działania. GSR powinien być spontaniczny, organicznie wpisany w logikę globalnych procesów, nigdy nie powinien być zaplanowany z wyprzedzeniem, ani związany z określonym miejscem lub czasem. Tylko taka mobilna obecność zapewni Sojuszowi efektywność i odporność na politykę globalnego systemu opresyjnego. Aktywność Sojuszu powinna być oparta na zrozumieniu zespołu wspólnych zasad, celów walki, tożsamości wroga, rozpoznaniu status quo jako katastrofalnego, niemożliwego do tolerowania i wymagającego całkowitego zniszczenia, podobnie jak zrozumieniu przyczyn tej sytuacji, stadium jej rozwoju oraz instrumentalnych procesów, które czynią ją możliwą i rzeczywistą. Każdy, kto to rozumie, kto nie akceptuje bieżącej sytuacji i kto jest gotowy działać w zgodzie z tym rozumowaniem, jest członkiem GSR. Oto dlaczego GSR musi być policentryczny. Nie powinien mieć pojedynczego terytorialnego, narodowego, religijnego lub innego centrum. Sojusz powinien operować wszędzie, niezależnie od granic, ras i religii, w oparciu o wewnętrzne przekonanie i spontanicznie otwierające się okna możliwości. W istocie to właśnie nieobecność generalnej strategii jest osią strategii rewolucyjnej, oraz nieobecność określonego przestrzennie, hierarchicznie jednolitego centrum nerwowego – dominującym modelem jego operacji (…) GSR powinien być rozmyślnie asymetrycznym – mógłby potencjalnie być częściowo reprezentowany przez państwa, siły społeczne, partie polityczne, ruchy, grupy, aż do poszczególnych jednostek. Wszystko to, co opiera się w stopniu skrajnym lub umiarkowanym, frontalnie lub w bezpośredniej styczności władzy światowej oligarchii musi zostać uznane za terytorium GSR. Ten obszar może być warunkowy lub konkretny, narodowy lub cybernetyczny, naturalny lub sieciowy. Jeśli jakikolwiek kraj na świecie – duży lub mały – działa przeciwko globalnej dominacji Stanów Zjednoczonych, NATO, zachodnich globalistów i światowego

[24] L. Sykulski, *Koncepcja Radykalnego Podmiotu i „czwarta teoria polityczna" Aleksandra Dugina w kontekście bezpieczeństwa Polski i Unii Europejsk*iej, „Przegląd Geopolityczny" 2014, nr 8, s. 238. Dugin podkreśla jednak, że GSR jest jedynie skrzydłem Międzynarodowego Ruchu Eurazjańskiego. Zob. A.G. Dugin, *Putin vs Putin: Vladimir Putin Viewed from the Right*, London 2014, s. 279.

> liberalnego systemu finansowego, wówczas państwo takie powinno być uważane za część GSR i należy je wspierać na wszelkie sposoby, niezależnie od tego czy podzielamy wartości tego państwa, czy rządzący nim są atrakcyjni czy odpychający, czy jego obecny system jest skorumpowany czy sprawiedliwy (…) Ta sama zasada stosuje się do oceny ruchów, partii, organizacji religijnych, narodowych i politycznych (…) Ważne jest co innego: czy walczą one ze Stanami Zjednoczonymi i światową oligarchią, czy niszczą istniejący system, lub przeciwnie, podtrzymują go, służą mu i wspierają jego funkcjonowanie[25].

Globalny Sojusz Rewolucyjny jest sieciowym, ponadnarodowym, eksterytorialnym ośrodkiem konsolidacji wszelkich podmiotów, szczególnie zaś intelektualistów wrogich USA i NATO, których łączy w jedną światową, rewolucyjną kontrelitę. Ta konsolidacja odbywa się na podstawie „platformy wartości" opartej na 4 TP przez infiltrację kulturowo-ideologiczną ośrodków akademickich oraz przedstawicieli wszelkich zawodów i profesji mających wpływ na kształtowanie opinii w swoich środowiskach. Dzięki tym działaniom globalna kontrelita może zdobyć tzw. hegemonię. Jest to nawiązanie do koncepcji włoskiego komunisty Antonia Gramsciego, która zakłada, że zdobycie władzy politycznej jest możliwe dzięki opanowaniu kultury, sposobu myślenia i systemu wartości[26]. Hegemonia w ujęciu Gramsciego to moralne i intelektualne panowanie elity nad społeczeństwem obywatelskim przejawiające się w tym, że jej światopogląd, ideały oraz wyznawane przez nią wartości zaczynają się jawić temu społeczeństwu jako prawdziwe, sprawiedliwe i uniwersalne. Hegemonię zdobywa się przez prawne lub bezprawne, otwarte lub niejawne, stopniowe narzucanie światopoglądowych, ontologicznych paradygmatów tworzonych przez kręgi intelektualistów[27].

GSR jest zatem globalną strukturą będącą nośnikiem ideologii tworzonych w Moskwie i pełniącą funkcję narzędzia polityki Kremla, której celem jest wyparcie Stanów Zjednoczonych z Europy („obalenie hegemonii USA") i stworzenie korzystnego dla Rosji geopolitycznego ładu wielobiegunowego. W tym kontekście niezwykle interesujące są metody zawarte w manifeście GSR charakterystyczne dla opisanej koncepcji wojny sieciowej, które powinni stosować wszyscy identyfikujący się z przesłaniem ideowym Sojuszu:

> Nowe warunki wymagają od nas udoskonalenia umiejętności klasycznego prowadzenia walki, podobnie jak opanowania nowych obszarów prowadzenia wojny – włączając w to sfery sieciową, cybernetyczną i wirtualną. Opanowanie tych obszarów jest najważniejsze dla frontu antyamerykańskiego, ponieważ pole sieci wirtualnej pozwala efektyw-

[25] Global Revolutionary Alliance. Manifesto, Program, Principles, Strategy [online], http://www.granews.info/content/part-6-structure-global-revolutionary-alliance [dostęp: 11 XII 2016]. Tekst manifestu został zamieszczony także w publikacji: A.G. Dugin, *Eurasian Mission: An Introduction to Neo-Eurasianism*, London 2014, s. 129–166. Przetłumaczono go również na język polski. Przekład, dokonany w całości przez redakcję portalu Xportal.pl., jest dostępny na stronie: Globalny Sojusz Rewolucyjny: Manifest [online], http://xportal.pl/?p=1268 [dostęp: 28 I 2017].

[26] R.W. Cox, *Gramsci, Hegemony and International Relations: An Essay in Method*, „Millennium – Journal of International Studies" 1983, nr 12, s. 162–175.

[27] Н.В. Мелентьева, *Контргегемония по горизонтали и по вертикали (пролегомены к Евразийской версии)*, w: *Левиафан: Контргегемония и евроцентризм*, А.Г. Дугин (red.), Москва 2013, s. 55, 64–65. Por. A. Umland, *Kulturhegemoniale Strategien der russischen extremen Rechten: Die Verbindung von faschistischer Ideologie und metapolitischer Taktik im „Neoeurasimus" des Aleksandr Dugin*, „Österreichische Zeitschrift für Politikwissenschaft" 2004, nr 33, s. 437–454; G. Cospito, *Egemonia/egemonico nei "Quaderni del carcere" (e prima)*, „International Gramsci Journal" 2016, nr 2, s. 49–88.

> nie posługiwać się asymetrycznymi formami operacji militarnych (…). Jeśli siła wojskowa w sensie tradycyjnych form uzbrojenia czyni zasoby globalnej hierarchii i jej amerykańskich i NATO-wskich narzędzi nieporównywalnie silniejszymi niż cała moc jej potencjalnych adwersarzy, to w tym obszarze frontalnej konfrontacji zwycięstwo byłoby bardzo trudne. Jednak w obszarze wojny sieciowej i cyberstrategii decydują odmienne czynniki. Niemałą rolę odgrywają tu kreatywność, niekonwencjonalne myślenie, wynalazczość i zdolność działania poza ustalonymi ramami. W cyberprzestrzeni, na odpowiednim poziomie, siły światowej oligarchii i rewolucyjnej kontrelity mogą zostać wyrównane chociażby przejściowo; w ramach ponownie otwartego obszaru, strefy lub technologii, twórcze podejście samotników jest porównywalne z głównymi konstrukcjami budżetowymi transnarodowych korporacji. W ten sposób osobista strona internetowa lub stylowy blog utalentowanego samotnika może przyciągnąć uwagę i wywierać wpływ porównywalny do oficjalnego rządowego źródła informacji danego kraju, lub takiego o dużej skali, utworzonego przez globalistyczne źródło środków przekazu. W wypadku opanowania strategii prowadzenia wojny sieciowej staje się możliwe prowadzenie profesjonalnej i dynamicznej wojny sieciowej ze światową oligarchią – włączając w to wirusy, rewolucyjny trolling, flaming, flooding, spamming, a także użycie botów internetowych, tworzenie fałszywych osobowości i przyjmowanie fałszywych tożsamości (*socket-puppet strategies*). W związku z tym, antyamerykański front globalnej kontrelity potrzebuje zarówno instruktorów wojskowych i weteranów wojen lokalnych, żołnierzy-hakerów, programistów, administratorów systemów informatycznych, jak i pojedynczych osób w globalnej sieci oporu. Cała rzeczywistość jest dziś polem konfliktu – zarówno ta zlokalizowana poza siecią, jak i związana ze światem wirtualnym. Musimy być przygotowani do poprowadzenia wszystkich globalnych wojen, rozciągając strefę operacyjną na wszystkie współczesne poziomy – od powszechnych zachowań, stylów życia, mody, pracy i odpoczynku, do ideologii, przepływu informacji, technologii, sieci społecznych i wirtualnych światów. Musimy starać się zadać jak największe szkody światowej oligarchii oraz interesom Stanów Zjednoczonych i NATO na wszystkich dostępnych poziomach – osobistym, militarnym, ekonomicznym, kulturowym, informatycznym, sieciowym, w przestrzeni wirtualnej etc.[28]

Instrukcja prowadzenia wojny sieciowej zawarta w manifeście jest skierowana przede wszystkim do podmiotów funkcjonujących w świecie zachodnim, dlatego też aby uczynić ją zrozumiałą dla członków sieci realizujących interesy Rosji w krajach NATO, kremlowscy ideolodzy posłużyli się znaną w Europie i popularną w kręgach „antysystemowych" koncepcją strategii oporu niekierowanego i zachodnim dyskursem „działań asymetrycznych".

Budowa „sieci eurazjańskiej" w Europie – metody, środki, ludzie, struktury i działania

Rosyjska koncepcja wojny sieciowej polega więc na zaktywizowaniu warstw niezadowolonych za pośrednictwem środków informacyjno-psychologicznych i zbudowaniu z nich oddolnego ruchu o zasięgu globalnym w celu posłużenia się nim do realizacji określonych celów geopolitycznych. Jak już powiedziano, szczególnie pomocne w realizacji tego zamiaru są wszelkie partie i ruchy skrajnie prawicowe i lewicowe, które łączy

[28] Global Revolutionary Alliance... Por. A.G. Dugin, *The Multipolar World and the Postmodern*, „Journal of Eurasian Affairs" 2013, nr 1, s. 8–13.

sprzeciw wobec relacji euroatlantyckich, liberalizmu i globalizmu. Dlatego też stają się one ważnym sojusznikiem geopolitycznym Rosji. Działania FR polegają na wspieraniu tych środowisk wszelkimi możliwymi sposobami przy jednoczesnym, cynicznym wykorzystywaniu ich jako narzędzi dezinformacji i propagandy. Co więcej, Rosja prowadzi działania polegające na kształtowaniu świadomości zachodnich społeczeństw w taki sposób, aby wytworzyć postawy aprobujące politykę skrajnej prawicy, co w dalszej perspektywie pozwoli na przejęcie przez nią władzy w państwach UE[29]. Kontakty wspomnianych wyżej ruchów i organizacji z władzami Rosji odbywają się za pośrednictwem administracji prezydenta i ideologów bliskich Kremlowi, jak np. Aleksandr Dugin. Według raportu czeskiej Informacyjnej Służby Bezpieczeństwa (Bezpečnostní informační služba), który zawiera informacje o jej działalności w 2014 r., rola rosyjskiego geopolityka w tych działaniach jest ogromna. Jak stwierdzają autorzy raportu, za pomocą wspomnianych partii Rosja buduje strukturę podobną do Międzynarodówki Komunistycznej. Jej konstrukcja opiera się bowiem na ekspansywnym eurazjanizmie Dugina[30].

Przykładem tego typu działań jest zorganizowanie Międzynarodowego Rosyjskiego Forum Konserwatywnego, które odbyło się 22 marca 2015 r. w Sankt Petersburgu. Zaproszono tam rosyjskich i europejskich przedstawicieli ugrupowań szowinistycznych oraz neonazistowskich, w większości marginalnych. Wśród uczestników byli m.in. przedstawiciele greckiego Złotego Świtu (Χρυσή Αυγή), włoskiej Nowej Siły (Nuova Forza) oraz eurodeputowany Udo Voigt, były przywódca Narodowodemokratycznej Partii Niemiec (Nationaldemokratische Partei Deutschlands, NPD) i Nick Griffin, były lider Brytyjskiej Partii Narodowej (British National Party, BNP). Większość reprezentowanych ugrupowań jest skupiona w Sojuszu na rzecz Pokoju i Wolności, którego pierwszy kongres odbył się w lutym 2015 r. w Parlamencie Europejskim. Ze strony rosyjskiej przybyli przedstawiciele zarówno środowisk nacjonalistycznych i monarchistycznych, jak i kręgów eksperckich. Organizatorem wydarzenia była nacjonalistyczna partia Rodina, na spotkaniu zabrakło jednak jej kierownictwa i wicepremiera Dmitrija Rogozina – założyciela i politycznego patrona partii. Rezolucja zjazdu powtarza hasła rosyjskiej propagandy: konfrontację z globalną hegemonią USA, obecnym kształtem Unii Europejskiej oraz ideologią liberalną, a także konieczność pogłębiania integracji Rosji z Europą przez budowę wspólnego europejskiego systemu bezpieczeństwa oraz zniesienie sankcji przeciw Rosji[31].

Obrady forum przyczyniły się do zawarcia międzynarodowego sojuszu przez uczestniczące w nim partie. Funkcjonuje on pod nazwą Światowy Ruch Narodowo-Konserwatywny (dalej: ŚRNK). Jego koordynatorem jest Jurij Lubomirskij, prominentny członek partii Rodina. Koalicja partii i ruchów tworzących ŚRNK jest imponująca. Organizatorzy zaprosili do udziału aż 58 organizacji z Europy i różnych stron świa-

[29] A. Polyakova, *Putinism and the European Far Right* [online], http://imrussia.org/en/analysis/world/2500-putinism-and-the-european-far-right [dostęp: 12 XII 2016]; P. Pomerantsev, M. Weiss, *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, London 2014, s. 19–21; A. Shekhovtsov, *Moskau und die Rechten. Wie radikale Gruppierungen Unterstützung von Moskau erhalten*, „Die Politische Meinung" 2016, nr 509, s. 99–103.

[30] *Výroční zpráva Bezpečnostní informační služby za rok 2014* [online], https://www.bis.cz/pdf/2014-vz-cz.pdf, s. 10 i 11 [dostęp: 8 XII 2016].

[31] A. Shekhovtsov, *The Far-Right "International Russian Conservative Forum" to Take Place in Russia*, „The Interpreter" [online] z 10marca 2015 r., http://www.interpretermag.com/the-far-right-international-russian-conservative-forum-to-take-place-in-russia/ [dostęp: 12 XII 2016]; J. Rogoża, *Kreml „zagospodarowuje" europejską skrajną prawicę* [online], https://www.osw.waw.pl/pl/publikacje/analizy/2015-03-25/kreml-zagospodarowuje-europejska-skrajna-prawice [dostęp: 12 XII 2016].

ta. Większość z nich pochodzi z Europy i Stanów Zjednoczonych, ale są też organizacje z Chile, Japonii, Mongolii, Syrii i Tajlandii. Oblicze polityczne większości z tych partii i organizacji wskazuje, że struktura tworzona pod egidą Rosji skupia głównie podmioty skrajnie prawicowe, nacjonalistyczne i konserwatywne. Do udziału w ŚRNK zaproszono m.in.: Partię Duńską (Danskernes Parti), Złoty Świt z Grecji, Narodowodemokratyczną Partię Niemiec, Nową Prawicę (Noua Dreaptă) z Rumunii, brytyjską Jedność (Unity) oraz węgierski Ruch na rzecz Lepszych Węgier (Jobbik Magyarországért Mozgalom, Jobbik). Według A. Szechowcowa głównym celem ŚRNK jest stworzenie prorosyjskiej sieci informacyjnej złożonej z portali i sieci społecznościowych, mającej stanowić platformę wymiany informacji i opinii dotyczących takich zagadnień, jak obrona prześladowanych działaczy narodowo-konserwatywnych, (...) *pomoc humanitarna dla Serbów w Kosowie, chrześcijan na Bliskim Wschodzie i mieszkańców Noworosji*. Szczególnie interesującą inicjatywą ŚRNK jest organizowanie (...) *wspólnych obozów dla szkolenia wojskowego i sportowego*. Za tym określeniem kryją się szkolenia wojskowe przeznaczone dla ochotników zgłaszających chęć uczestniczenia w walkach na terytorium południowo-wschodniej Ukrainy, a także w Syrii. Warto zwrócić uwagę, że jedną z organizacji zaproszonych do ŚRNK jest Unité Continentale, założona w lecie 2014 r. przez francuskich i serbskich ultranacjonalistów, którzy zgłosili się do udziału w walkach po stronie separatystów[32].

Należy podkreślić, że większość partii i organizacji skupionych w ŚRNK od lat jest infiltrowana przez środowisko A. Dugina, które stopniowo i systematycznie wciągało je w orbitę rosyjskich wpływów. Do powstania struktur „sieci eurazjańskiej" przyczyniły się osobiste kontakty Aleksandra Dugina z działaczami skrajnej prawicy i lewicy, które nawiązał podczas swoich podróży do Francji, Hiszpanii i Włoch w latach 1989–1990 i w roku 1994. We Francji rozpoczął współpracę z przedstawicielami francuskiej tzw. Nowej Prawicy (La Nouvelle Droite française), do których należy m.in. Alain de Benoist − filozof i jej ideowy twórca kierujący stowarzyszeniem Grupa Badań i Studiów nad Cywilizacją Europejską (Groupement de recherche et d'études pour la civilisation européenne, GRECE) oraz obywatel Belgii Robert Steuckers. Warto podkreślić, że do dziś wspierają oni 4 TP Dugina. W Hiszpanii rosyjski polityk rozpoczął współpracę z Hiszpańskim Kręgiem Przyjaciół Europy (El Círculo Español de Amigos de Europa, CEDADE) – prawdopodobnie najstarszą w Europie modernistyczną organizacją neonazistowską. Z kolei we Włoszech nawiązał bliskie relacje z filozofem i badaczem idei Juliusa Evoli – Claudiem Muttim, powiązanym z organizacją Straż Narodowa (Avanguardia Nacionale), która jest odpowiedzialna za zorganizowanie terrorystycznych zamachów bombowych na Piazza Montana w Mediolanie 12 października 1969 r. Drugi etap tworzenia „sieci eurazjańskiej" przez Dugina przypada na pierwsze dziesięciolecie XXI w. Wówczas zyskał on znaczne wpływy w kręgu węgierskiej skrajnej prawicy. Przywódca partii Ruch na Rzecz Lepszych Węgier Gábor Vona otwarcie wspiera ideę eurazjanizmu. Oprócz tego Dugin utrzymuje ożywione kontakty ze „środowiskami antysystemowymi" w Niemczech, a szczególnie z dziennikarzem Manuelem Ochsenreiterem, redaktorem czasopisma „Zuerst!" powiązanym z ruchem Nowego Oporu. Dzięki tej znajomości rosyjski geopolityk umocnił swój autorytet w kręgach antyglobalistycznych. Trzy orga-

[32] A. Shekhovtsov, *Russian Politicians Building an International Extreme Right Alliance*, „The Interpreter" [online] z 15 września 2015 r., http://www.interpretermag.com/russian-politicians-building-an-international-extreme-right-alliance/ [dostęp: 12 XII 2016]; tenże, *French Eurasianists join (pro-)Russian extremists in Eastern Ukraine* [online], http://euromaidanpress.com/2014/08/27/french-eurasianists-join-pro-russian-extremists-in-eastern-ukraine/ [dostęp: 12 XII 2016].

nizacje sieciowe o tym profilu, tj. Open Revolt, Green Star i New Resistance weszły w skład Globalnego Sojuszu Rewolucyjnego. Na portalach tych struktur można odnaleźć teksty Aleksandra Dugina, przeznaczone dla odbiorców brytyjskich i amerykańskich[33].

Kulisy działań mających na celu proces infiltracji, werbunku i konsolidowania ekstremistycznych partii politycznych, organizacji i ruchów młodzieżowych światowa opinia publiczna mogła poznać dzięki hakerom z grupy „Anonimowa Międzynarodówka" («Анонимный интернационал»), znanej także pod nazwą «Шалтай-Болтай»[34]. Obiektem ataku przeprowadzonego przez hakerów z tej grupy 27 listopada 2014 r. stała się skrzynka mejlowa Gieorgija Gawrisza. W latach 2012–2013 Gawrisz jako pracownik rosyjskiej ambasady przebywał w Grecji, gdzie pomagał Duginowi nawiązywać kontakty z członkami tamtejszych „antysytemowych" partii i organizacji. Po powrocie do Moskwy umożliwił Duginowi podjęcie współpracy z biznesmenem Konstantinem Małofiejewem. Małofiejew, blisko powiązany z Patriarchatem Moskiewskim i administracją prezydenta, brał udział m.in. w przygotowaniu operacji wojskowych w Donbasie. Wkrótce do Dugina i Małofiejewa dołączyli jeszcze Aleksandr Trubieckoj – zamieszkały we Francji partner biznesowy Małofiejewa – i biznesmen Siergiej Rudow. Najważniejszą postacią i głównym sponsorem działań tej grupy był jednak Igor Szczegolew[35], który pod koniec lat 80. XX w. pełnił służbę w I Zarządzie Głównym KGB. W latach 90. XX w. Szczegolew pracował jako redaktor i korespondent ITAR-TASS (Informacyjna Telegraficzna Agencja Rosji TASS) w krajach Europy Wschodniej i we Francji. Obecnie zaś pełni funkcję doradcy prezydenta Putina ds. środków masowej informacji i e-administracji. Związek pomiędzy działalnością Dugina a prowadzeniem walki informacyjnej przez Rosję przeciwko Europie jest więc oczywisty[36].

W jaki sposób odbywała się infiltracja środowisk politycznych potrzebnych Rosjanom? Miała ona charakter działań wyczerpujących znamiona kreowania tzw. sztucznej uwagi. Najpierw, w imieniu Małofiejewa, Trubieckiego i Rudowa wysyłano zaproszenia na konferencje o nazwie „Szlachetne Zgromadzenia" (ros. «Благородные собрания»), podczas których nawiązywano kontakty z przedstawicielami prawicowych i konserwatywnych partii politycznych. Te spotkania stwarzały również znakomitą okazję do indoktrynowania zagranicznych gości, czym zajmował się głównie Aleksandr Dugin, który wygłaszał wykłady z cyklu *Czwarta Teoria Polityczna. Po drugiej stronie liberalizmu, komunizmu i faszyzmu. Nowa ideologia dla Rosji*. Celem tych spotkań było także utwierdzenie ich uczestników w przekonaniu, że Rosja jako „obrońca konserwatywnych wartości" stanowi jedyną alternatywę dla „zgniłego" Zachodu. Jedna z takich imprez odbyła się pod koniec maja 2014 r. w Pałacu Liechtenstein w Wiedniu. Wśród uczest-

[33] M. Laruelle, *Dangerous Liaisons: Eurasianism, The European Far Right, and Putin's Russia*, w: *Eurasianism and the European Far Right: Reshaping the Europe – Russia Relationship*, M. Laruelle (red.), London 2015, s. 11–15.

[34] *Черный Интернационал: Малофеев и Дугин* [online], https://b0ltai.org/2014/11/27/черный-интернационалмалофеев-и-дуги/ [dostęp: 11 XII 2016]. Por. *«Шалтай» слил письма коллег Малофеева и Дугина: Донбасс и евразийство* [online], http://medialeaks.ru/2711yt_dugin [dostęp: 11 XII 2016].

[35] *Щёголев Игорь Олегович* [online], http://www.vseportrety.ru/info-shegolev.html [dostęp: 11 XII 2016].

[36] *«Черный интернационал». Как Москва кормит правые партии по всему миру* [online], http://theins.ru/politika/2113 [dostęp: 11 XII 2016]. Szerzej na temat działalności Konstantina Małofiejewa zob. C.A. Fitzpatrick, *With Cash and Conspiracy Theories, Russian Orthodox Philanthropist Malofeyev is Useful to the Kremlin*, „The Interpreter" [online] z 28 kwietnia 2015 r., http://www.interpretermag.com/with-cash-and-conspiracy-theories-russian-orthodox-philanthropist-malofeyev-is-useful-to-the-kremlin/ [dostęp: 11 XII 2016]; Ф. Рустамова, И. Цой, А. Самуилкина, *Как фонд Константина Малофеева помогает Новороссии* [online], http://www.rbc.ru/politics/08/09/2014/ [dostęp: 11 XII 2016].

ników byli obecni m.in. Marion Maréchal-Le Pen, wnuczka charyzmatycznego lidera Frontu Narodowego Jean-Marie Le Pena, przewodniczący Wolnościowej Partii Austrii (Freiheitliche Partei Österreichs, FPÖ) Heinz-Christian Strache i lider bułgarskich nacjonalistów Wolen Siderow. Podczas spotkania Dugin wezwał do utworzenia (…) *piątej kolumny prorosyjskich intelektualistów, którzy, podobnie jak my, chcą wzmocnić tożsamość narodową. Podobnym sposobem będziemy mogli podbić Europę i jej obywateli połączyć z nami*. Promowanie wartości „konserwatywnych" odbywało się także podczas konferencji zatytułowanej „Duża rodzina i przyszłość ludzkości", zorganizowanej przez Małofiejewa w Moskwie, w dniach 10–11 września 2014 r. Wzięło w niej udział 169 gości z całego świata, reprezentujących głównie prawicowe, antyaborcyjne organizacje i stowarzyszenia[37].

Pozyskiwaniem zwolenników rosyjskiej polityki we Francji na użytek działań o charakterze informacyjnym zajmował się także Aleksandr Trubieckoj. Chodziło przede wszystkim o dotarcie do osób publicznych i wpływowych, jak np. Jean-Paul Dupré – członek Komisji Spraw Zagranicznych Zgromadzenia Narodowego Republiki Francuskiej, który skrytykował PE „za brak logiki" w kwestii sankcji wobec Rosji[38]. Bardzo interesujące informacje dotyczące projektu stworzenia sieci wpływu informacyjnego znalazły się na jednym z dokumentów przechowywanych w skrzynce Gieorgija Gawrisza. Nosi on tytuł: *Kraje i osoby, gdzie istnieją podstawy do stworzenia elitarnego klubu i/lub grupy informacyjnego wpływu po linii Rossija Siegodnia* (tłum. aut.). Widnieje tam następujący dopisek: *Z nimi wszystkimi Aleksandr Geliewicz Dugin lub jego przedstawiciele spotkali się osobiście, pośrednio lub bezpośrednio, wpływając na możliwość ich udziału w inicjatywie organizacyjnej i/lub informacyjnej o prorosyjskim charakterze* (tłum. aut.). W tym dokumencie wymieniono imiona i nazwiska osób oraz nazwy portali internetowych z Rumunii, Polski, Turcji, Węgier, Argentyny, Francji, Chorwacji, Słowacji, Serbii, Grecji, Libanu, Włoch, Niemiec, Chile i Malezji[39]. Według materiałów ujawnionych przez hakerów z grupy „Anonimowa Międzynarodówka" pozyskiwanie ludzi, których można byłoby wykorzystać w celach propagandowych, przebiegało w różny sposób. Szczególnie interesujący jest przypadek Charlesa Bausmana – redaktora wpływowego anglojęzycznego portalu Russia Insider i regularnego komentatora kanału Russia Today, który z własnej inicjatywy zgłosił się do Aleksieja Komowa – jednego ze współpracowników Konstantina Małofiejewa – po pieniądze. Według Komowa, główne kryteria oceny portalu prowadzonego przez Bausmana stanowiły przede wszystkim jego *wysoka jakość, popularność i prorosyjskość*[40].

---

[37] *«Черный интернационал»…*; B. Odehnal, *Gipfeltreffen mit Putins fünfter Kolonne* [online], http://www.tagesanzeiger.ch/ausland/europa/Gipfeltreffen-mit-Putins-fuenfter-Kolonne/story/30542701 [dostęp: 11 XII 2016].

[38] *«Черный интернационал»…*; Por. A. Shekhovtsov, *Pro-Kremlin "Re-information" Efforts: Structural Relations between the Russian Media and the European Far Right* [online], http://www.integrityinitiative.net/articles/496 [dostęp: 11 XII 2016].

[39] О. Зог, *Инструменты Кремля: эксклюзивный список агентов российского влияния в европейских странах* [online], http://argumentua.com/stati/instrumenty-kremlya-eksklyuzivnyi-spisok-agentov-rossiisko-go-vliyaniya-v-evropeiskikh-stranakh [dostęp: 11 XII 2016]. Por. И. Ткачёв, Г. Макаренко, А. Сухаревская, *Наши в Европе. Откуда берутся союзники Кремля за рубежом*, „Ежедневная деловая газета РБК" 2015, nr 130, s. 1–4.

[40] A. Shekhovtsov, *Is Russia Insider sponsored by a Russian Oligarch with the Ties to the European Far Right?* „The Interpreter" [online] z 23 września 2015 r., http://www.interpretermag.com/is-russia-insider-sponsored-by-a-russian-oligarch-with-ties-to-the-european-far-right/ [dostęp: 11 XII 2016]. Por. A. Foxall, *Putin's Useful Idiots: Britain's Left, Right and Russia*, „Policy Paper" 2016, nr 10, s. 8.

Oprócz mediów głównym obiektem zainteresowania Dugina i jego zwolenników były kręgi francuskich i niemieckich wojskowych. Jak ujawnił Anton Szechowcow, w raporcie sporządzonym 17 października 2013 r. Dugin opisał przebieg zamkniętego spotkania z członkami stowarzyszenia Obywatelskość, Obrona, Armia, Naród (Civisme Défense Armée Nation, CiDAN), które odbyło się w dniach 2–5 października 2013 r. na zamku Klingenthal pod Strasburgiem. Pomysłodawcą stowarzyszenia, które powstało w 1999 r., był admirał Pierre Lacoste. Działalność CiDAN skupia się na promowaniu (...) *nowoczesnej wizji patriotyzmu i Europy*, zacieśnianiu kontaktów między społeczeństwem i wojskiem, problematyce obrony terytorialnej itp. Do ugrupowania należą wysokiej rangi wojskowi i eksperci. Jest ono finansowane przez Sztab Generalny Republiki Francuskiej oraz współpracuje z armią niemiecką. Do kierownictwa należą: admirał Pierre Lacoste, generał Yves Béraud i pułkownik Jacques Sonnet. Według Dugina na spotkaniu omawiano następujące tematy: przygotowanie francuskiej interwencji wojskowej w Afryce Środkowej, sytuację wojsk francuskich w Mali, problematykę ówczesnych relacji między Syrią a UE (podczas dyskusji nad tym punktem francuscy generałowie ostrożnie popierali politykę Putina, krytycznie natomiast wypowiadali się na temat polityki USA). Następnie Dugin i Michel Grimard ze Związku Organizacji Jedności Europejskiej (Rassemblement pour l'Organisation de l'Unité Européenne, ROUE) wystąpili z wykładem poświęconym Rosji i Unii Eurazjatyckiej. W raporcie Dugin dużo miejsca poświęcił nastrojom, które panują wśród francuskiej generalicji. Zauważył, że wojskowi są bardzo krytycznie ustosunkowani do polityki Stanów Zjednoczonych i prezydenta Francji François Hollande'a. W Putinie upatrują natomiast gwaranta i obrońcę „suwerenności". Są gotowi, według Dugina, podjąć współpracę z Rosją i ruchem eurazjańskim. Dostrzegają w nim bowiem dominującą siłę intelektualną w Rosji. Co ciekawe, w tym samym tonie wypowiadali się także niemieccy generałowie, w tym były dyrektor Federalnej Służby Wywiadowczej (niem. Bundesnachrichtendienst, BND). Swoje spostrzeżenia Dugin podsumował stwierdzeniem, że stowarzyszenie jest prowadzone przez ludzi o orientacji antyatlantyckiej, antyamerykańskiej i prorosyjskiej[41].

Możliwość nawiązania współpracy przez część francuskich wojskowych ze strukturami ruchu eurazjańskiego wydaje się realna. Warto przypomnieć, że w skład Wyższej Rady Międzynarodowego Ruchu Eurazjańskiego wchodził aż do śmierci generał Pierre Marie Gallois – ekspert ds. strategii i geopolityki[42]. Co więcej, wielu przedstawicieli francuskiej myśli geopolitycznej lansuje koncepcję bliskiej współpracy europejsko-rosyjskiej. Według nich za nawiązaniem takiej współpracy przemawiają wspólne interesy obydwu podmiotów. W dużej mierze są one determinowane czynnikami geograficznymi. Podkreślają także znaczenie wspólnej historii, kultury i cywilizacji Rosji oraz Europy. Przykładem takich teorii są koncepcje dwóch francuskich geopolityków: Henriego de Grossouvre'a i Marca Rousseta[43]. Pierwszy z nich – syn François de Grossouvre'a, doradcy prezydenta François Mitterranda – jest autorem książki pt. *Paryż – Berlin – Moskwa – droga do niepodległości i pokoju*. W publikacji zwraca uwagę, że przyczyną osłabienia pozycji Francji i innych potęg europejskich są rosnące wpływy Stanów

[41] A. Shekhovtsov, *Russian Fascist Aleksandr Dugin Gathering Intelligence on the French Military*, „The Interpreter" [online] z 28 września 2014 r., http://www.interpretermag.com/russian-fascist-aleksandr-dugin-gathering-intelligence-on-the-french-military/ [dostęp: 11 XII 2016].

[42] *Руководство Международного Евразийского Движения* [online], http://med.org.ru/article/1908 [dostęp: 11 XII 2016].

[43] L. Sykulski, *Integracja polityczna Eurazji we współczesnej rosyjskiej myśli geopolitycznej*, w: *Studia nad geopolityką XX wieku*, P. Eberhardt (red.), Warszawa 2013, PAN, s. 356.

Zjednoczonych. Autor proponuje prowadzenie polityki zmierzającej do policentryzacji świata. Według niego ma to być sposób na odbudowę międzynarodowej, mocarstwowej pozycji Francji. Fundamentem świata wielobiegunowego ma być silna Europa oparta na sojuszu Francji, Niemiec i Rosji. Oś Paryż – Berlin – Moskwa, którą de Grossouvre nazywa „osią niezależności europejskiej", powinna, jego zdaniem, rozciągać swoje wpływy od kanału La Manche i Morza Północnego do Morza Śródziemnego, włączając w to Maghreb. Francuski geopolityk wskazuje na Rosję jako głównego partnera strategicznego dla Unii Europejskiej i sojuszu na linii Paryż – Berlin. Jego zdaniem tylko sojusz z Moskwą jest w stanie zapewnić Europie równowagę w konkurencji ze Stanami Zjednoczonymi. Podkreśla rolę rosyjskich surowców energetycznych, zasobów naturalnych na Syberii oraz siły militarnej Rosji. Jest krytykiem NATO, które według niego stało się narzędziem w ręku polityków amerykańskich[44]. Podobne postulaty zawiera także myśl geopolityczna Marca Rousseta, postulującego stworzenie unii francusko-niemieckiej. Następnie Rousset proponuje rozszerzyć oś Paryż – Berlin o Moskwę, która stanie się wschodnim zwornikiem Nowej Europy i gwarantem pokoju na obszarze poradzieckim. Geopolityczny byt powstały w wyniku połączenia kontynentu eurazjatyckiego od Atlantyku do Pacyfiku Rousset określa nie tylko mianem Nowej Europy, lecz także Euro-Syberii, wskazując tym na strategiczne znaczenie wschodniej części Federacji Rosyjskiej[45].

Próby stworzenia przez Aleksandra Dugina i jego współpracowników sieci kontaktów we francuskich kręgach wojskowych i opiniotwórczych, czego dowodem jest wspomniana notatka ze spotkania na zamku Klingenthal, znacznie zwiększają prawdopodobieństwo przynajmniej częściowego urzeczywistnienia tych koncepcji.

Głównym celem Federacji Rosyjskiej jest jednak doprowadzenie partii upatrujących w niej sojusznika do zwycięstwa w wyborach zarówno krajowych, jak i europejskich, dzięki czemu mogłaby ona wywierać wpływ na politykę UE. Do zrealizowania takiego scenariusza doszło w Grecji, gdzie w wyniku wyborów parlamentarnych przeprowadzonych 25 stycznia 2015 r. powstała koalicja złożona z całkowicie przeciwstawnych sobie programowo i ideologicznie partii: Koalicji Radykalnej Lewicy Syriza (Συνασπισμός Ριζοσπαστικής Αριστεράς, ΣΥΡΙΖΑ), konserwatywnej, eurosceptycznej partii Niezależni Grecy (Ανεξάρτητοι Έλληνες, ΑΝΕΛ) oraz skrajnie prawicowego Nowego Świtu (Χρυσή Αυγή). Materiały uzyskane przez grupę hakerów «ШАлтай-Болтай» jednoznacznie wskazują na to, że do ukształtowania greckiej sceny politycznej w największym stopniu przyczynili się działacze ruchu eurazjańskiego oraz rosyjskie służby specjalne. Główną rolę w nawiązywaniu kontaktów z tymi partiami odegrał Gieorgij Gawrisz. Zaowocowało to zaproszeniem Dugina na wykłady, które wygłosił 12 kwietnia 2013 r. na Uniwersytecie w Pireusie i Uniwersytecie Panteion. Wystąpienia Dugina były możliwe także dzięki inicjatywie Nikosa Kotziasa, znanego z prorosyjskich sympatii, późniejszego ministra spraw zagranicznych w gabinecie Alexisa Tsiprasa. Co więcej, Panos Kammenos – przywódca partii Niezależnych Greków, dyrektor greckiego Instytutu Badań Geopolitycznych, podpisał porozumienie dotyczące współpracy z Rosyjskim Instytutem Badań Strategicznych (Российский институт стратегических исследований, РИСИ), w którym bywał także Alexis Tsipras, lider Syrizy. Prawdopodobnie w insty-

[44] Tamże, s. 356–357. Por. H. Grossouvre, *Paris-Berlin-Moscou: La voie de l'indèpendance et de la Pax*, Paris 2002, s. 33–40.

[45] L. Sykulski, *Integracja polityczna Eurazji…,* s. 357–358. Por. M. Rousset, *La nouvelle Europe: Paris-Berlin-Moscou – Le continent paneuropéen face au choc des civilisations*, Paris 2009, s. 10–14, 131–133, 197–200.

tucie przygotowywano strategię kampanii wyborczej Syrizy oraz plan wyjścia Grecji z UE i strefy euro. W tym kontekście warto nadmienić, że Rosyjski Instytut Badań Strategicznych początkowo był w strukturach Służby Wywiadu Zagranicznego FR, a obecnie jest związany z administracją prezydenta FR. Do 4 stycznia 2017 r. funkcję dyrektora tego instytutu pełnił generał porucznik Leonid Reszetnikow, który do 2009 r. zajmował stanowisko dyrektora Zarządu Informacyjno-Analitycznego SWZ[46]. Aktualnie działalnością placówki kieruje Michaił Fradkow – dyrektor Służby Wywiadu Zagranicznego FR w latach 2007–2016[47].

Wydaje się, że koalicja pozornie odległych od siebie partii skrajnej prawicy i lewicy została sformowana pod wpływem Rosjan zgodnie z założeniami 4 TP Dugina, która łączy różnorodne, przeciwstawne sobie ruchy, partie i organizacje na podstawie wspólnego celu.

Podsumowanie

W odróżnieniu od amerykańskiej koncepcji wojny sieciowej utożsamianej początkowo z konfliktami o niskiej intensywności, jej rosyjski odpowiednik służy do zdobywania geopolitycznej przewagi na poziomie globalnym w konfrontacji między państwami lub blokami polityczno-militarnymi. W tym względzie nie odbiega on zasadniczo od radzieckiej koncepcji „aktywnych działań" (ros. *активные мероприятия*). Podobnie jak w przypadku rozwiązań opracowanych w ZSRR, podstawą rosyjskiej wojny sieciowej w ujęciu A. Dugina są przede wszystkim działania o charakterze agitacyjno-propagandowym i wywiadowczo-organizacyjnym prowadzone przez podmioty niepaństwowe (w tym przypadku przez sieć różnych organizacji powiązanych z ruchem eurazjańskim) przy nieoficjalnym (niejawnym) wsparciu służb specjalnych i administracji rządowej FR. Te działania polegają na tworzeniu, finansowaniu i kierowaniu działalnością różnego rodzaju organizacji i nielegalnych grup opozycyjnych w celu uzyskania wpływu na szerokie sfery działalności politycznej i społecznej w innych państwach. Jest to realizowane m.in. przez jawne lub tajne wykupywanie lokalnych mediów, indoktrynowanie ekspertów, dziennikarzy i przedstawicieli różnych środowisk politycznych, a następnie przekształcanie ich w świadomą lub nieświadomą agenturę wpływu, co odbywa się na prestiżowych konferencjach naukowych.

Istotne novum jest widoczne przede wszystkim w zastosowaniu nowoczesnych rozwiązań technologicznych i komunikacyjnych (np. Internet), które są nośnikiem dla zbioru idei stanowiących główne narzędzie oddziaływania w sferze kognitywnej i społeczno-kulturowej wojen sieciowych. Komunistyczną ideologię zastąpiono bowiem ideami opartymi na paradygmacie ontologicznym, a nie aksjologicznym, czyli odwołującymi się nie tyle do jasno sprecyzowanych pojęć i doktryn, ile do realizacji ściśle określonych celów. Takie podejście charakteryzuje dorobek ideowy Aleksandra Dugina. Stworzona przez niego Czwarta Teoria Polityczna nadaje nową treść rosyjskiemu imperializmowi, co umożliwia skuteczne oddziaływanie na ideosferę świata zachodniego. Zatem w jego przypadku mamy do czynienia ze zwartym światem ideowym, ujętym

[46] И. Домбровская, *СИРИЗА, Дугин и Камменос: опасные связи или «полезные идиоты»?* [online], http://ru.rfi.fr/rossiya/20150308-opasnye-svyazi-grecheskoi-sirizy-s-moskvoi [dostęp: 11 XII 2016]; М. Лауринавичюс, *Россия при Путине. План Кремля для Европы* [online], http://ru.delfi.lt/v-fokuse/novosti/rossiya-pri-putine-plan-kremlya-dlya-evropy/ [dostęp: 11 XII 2016].

[47] Zob. Михаил Ефимович Фрадков [online], https://riss.ru/profile/fradkov/ [dostęp: 27 I 2017].

w spójną koncepcję filozoficzną, która jest jednak ukryta w różnorodnym i niejednoznacznym aparacie pojęciowym. To powoduje, że jej treść odczytywana przez danego odbiorcę zależy od stopnia jego „ideowego oblicza": antyglobaliści znajdą w niej krytykę neoliberalizmu i amerykanizmu, nacjonaliści – obronę narodowych tożsamości i praw wspólnotowych, rasiści – pojęcia e t n o s u i r a s y, konserwatyści – obronę religii oraz tradycyjnego modelu rodziny. To umożliwia infiltrowanie wszystkich tych środowisk, które indoktrynuje się treściami korzystnymi dla celów rosyjskiej polityki. Taki zabieg pozwala Kremlowi znacznie zwiększyć zakres oddziaływania informacyjno-psychologicznego i pozyskiwać do realizacji swoich celów ciągle nowe grupy.

Należy również wskazać na to, że koncepcja wojny sieciowej stworzona i spopularyzowana przez Dugina i jego współpracowników pełni ważną funkcję propagandową na wewnętrznym froncie walki informacyjnej. Uzasadniając jej powstanie, autorzy ci wskazują na rzekomą słabość państwa rosyjskiego i konieczność budowy własnych koncepcji „wojen informacyjnych" w celu przeciwstawienia się informacyjnej agresji Zachodu. W ich ujęciu rosyjska koncepcja wojen sieciowych stanowi odpowiedź na amerykańskie próby demontażu rosyjskiej państwowości i destabilizacji przestrzeni poradzieckiej, w rzeczywistości jednak, przez umiejętne zastosowanie zachodniej terminologii, skutecznie maskuje rozwiązania stosowane od lat przez radzieckie służby.

Bibliografia:

1. Arquilla J., Ronfeldt D., *Cyberwar is Coming!* „Comparative Strategy" 1993, nr 12, z. 2, s. 141–165.
2. Arquilla J., Ronfeldt D., *The Adwent of Netwar*, Santa Monica 1996, Rand Corporation.
3. Arquilla J., *To Build a Network*, „PRISM" 2014, nr 5, s. 22–34.
4. Beam L.B., *Leaderless Resistance*, „The Seditionist" [online] 1992, nr 12, http://www.louisbeam.com/leaderless.htm. [dostęp: 16 II 2017].
5. Blaker J.R., *Transforming Military Force: The Legacy of Arthur Cebrowski and Network Centric Warfare*, London 2007, Allen & Unwin.
6. Brose R., *Cyberwar, Netwar, and the Future of Cyberdefense*, w: *7th International Conference on Cyber Conflict: Architectures in Cyberspace*, M. Maybaum, A.M. Osula, L. Lindström (red.), Tallin 2015, NATO CCD COE Publications, s. 25–38.
7. Cebrowski A., Garstka J., *Network Centric Warfare: Its Origin and Future*, „US Naval Institute Proceedings Magazine" 1998, nr 124, z. 1, s. 28–35.
8. Cospito G., *Egemonia/egemonico nei "Quaderni del carcere" (e prima)*, „International Gramsci Journal" 2016, nr 2, s. 49–88.
9. Cox R.W., *Gramsci, Hegemony and International Relations: An Essay in Method*, „Millennium. Journal of International Studies" 1983, nr 12, s. 162–175.
10. *«Черный интернационал». Как Москва кормит правые партии по всему миру* [online], http://theins.ru/politika/2113 [dostęp: 11 XII 2016].
11. *Черный Интернационал: Малофеев и Дугин* [online], https://b0ltai.org/2014/11/27/черный-интернационалмалофеев-и-дуги/ [dostęp: 11 XII 2016].
12. Darczewska J., *Diabeł tkwi w szczegółach. Wojna informacyjna w świetle doktryny wojennej Rosji*, Warszawa 2015, Ośrodek Studiów Wschodnich.
13. Dugin A.G., *Eurasian Mission: An Introduction to Neo-Eurasianism*, London 2014, Arktos Media.

14. Dugin A.G., *Putin vs Putin: Vladimir Putin Viewed from the Right*, London 2014, Arktos Media Ltd.
15. Dugin A.G., *The Multipolar World and the Postmodern*, „Journal of Eurasian Affairs" 2013, nr 1, s. 8–13.
16. Fitzpatrick C.A., *With Cash and Conspiracy Theories, Russian Orthodox Philanthropist Malofeyev is Useful to the Kremlin*, „The Interpreter" [online] z 28 kwietnia 2015 r., http://www.interpretermag.com/with-cash-and-conspiracy-theories-russian-orthodox-philanthropist-malofeyev-is-useful-to-the-kremlin/ [dostęp: 11 XII 2016].
17. Foxall A., *Putin's Useful Idiots: Britain's Left, Right and Russia*, „Policy Paper" 2016, nr 10, s. 2–16.
18. Global Revolutionary Alliance. Manifesto, Program, Principles, Strategy [online], http://www.granews.info/ [dostęp: 11 XII 2016].
19. Globalny Sojusz Rewolucyjny: Manifest [online], http://xportal.pl/?p=1268 [dostęp: 28 I 2017].
20. Gray P.W., *Leaderless Resistance, Networked Organization, and Ideological Hegemony*, „Terrorism and Political Violence" 2013, nr 25, s. 655– 671.
21. Grossouvre H., *Paris-Berlin-Moscou: La voie de l'indèpendance et de la Pax*, Paris 2002, L'Age d'Homme,
22. Hardt M., Negri A., *Empire*, Cambridge–London 2000, Harvard University Press.
23. Kaplan J., *Encyclopedia of White Power: A Sourcebook on the Radical Racist Right*, Walnut Creek–Lahnam–New York–Oxford 2000, Rowman and Littlefield Publishers.
24. Laruelle M., *Dangerous Liaisons: Eurasianism, The European Far Right, and Putin's Russia*, w: *Eurasianism and the European Far Right: Reshaping the Europe – Russia Relationship*, M. Laruelle (red.), London 2015, Lexington Books, s. 1–33.
25. Laruelle M., *The Izborsky Club, or the New Conservative Avant-Garde in Russia*, „The Russian Review" 2016, nr 75, s. 626–644.
26. Liedel K., Piasecka P., *Wojna cybernetyczna – wyzwanie XXI wieku*, „Bezpieczeństwo Narodowe" 2011, nr 1, s. 15–28.
27. Odehnal B., *Gipfeltreffen mit Putins fünfter Kolonne* [online], http://www.tagesanzeiger.ch/ausland/europa/Gipfeltreffen-mit-Putins-fuenfter-Kolonne/story/30542701 [dostęp: 11 XII 2016].
28. Polyakova A., *Putinism and the European Far Right* [online], http://imrussia.org/en/analysis/world/2500-putinism-and-the-european-far-right [dostęp: 12 XII 2016].
29. Pomerantsev P., Weiss M., *The Menace of Unreality: How the Kremlin Weaponizes Information, Culture and Money*, London 2014, Institute of Modern Russia.
30. Posłuszna E., *Terroryzm w czasach globalizacji. Przyczynek do rozważań nad wojnami czwartej generacji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2016, nr 15, s. 174–187.
31. Potulski J., *Współczesne kierunki rosyjskiej myśli geopolitycznej: między nauką, ideologicznym dyskursem a praktyką*, Gdańsk 2010, Wydawnictwo Uniwersytetu Gdańskiego.
32. Rodkiewicz W, Rogoża J., *Potiomkinowski konserwatyzm. Ideologiczne narzędzie Kremla*, Warszawa 2015, Ośrodek Studiów Wschodnich.
33. Rogoża J., *Kreml „zagospodarowuje" europejską skrajną prawicę* [online], https://www.osw.waw.pl/pl/publikacje/analizy/2015-03-25/kreml-zagospodarowuje-europejska-skrajna-prawice [dostęp: 12 XII 2016].

34. Rossman V., *Moscow State University's Department of Sociology and the Climate of Opinion in Post–Soviet Russia*, w: *Eurasianism and the European Far Right: Reshaping the Europe – Russia Relationship*, M. Laruelle (red.), London 2015, Lexington Books, s. 55–77.
35. Rousset M., *La nouvelle Europe: Paris-Berlin-Moscou – Le continent paneuropéen face au choc des civilisations*, Paris 2009, Godefroy de Bouillon.
36. *Русская доктрина. Государственная идеология эпохи Путина*, А.Б. Кобяков, В.В. Аверьянов (red.), Москва 2016, Институт русской цивилизации.
37. *«Шалтай» слил письма коллег Малофеева и Дугина: Донбасс и евразийство* [online], http://medialeaks.ru/2711yt_dugin [dostęp: 11 XII 2016].
38. Shekhovtsov A., *French Eurasianists join (pro-) Russian Extremists in Eastern Ukraine* [online], http://euromaidanpress.com/2014/08/27/french-eurasianists-join-pro-russian-extremists-in-eastern-ukraine/ [dostęp: 12 XII 2016].
39. Shekhovtsov A., *Is Russia Insider sponsored by a Russian Oligarch with the Ties to the European Far Right?* „The Interpreter" [online] z 23 września 2015 r., http://www.interpretermag.com/is-russia-insider-sponsored-by-a-russian-oligarch-with-ties-to-the-european-far-right/ [dostęp: 11 XII 2016].
40. Shekhovtsov A., *Moskau und die Rechten. Wie radikale Gruppierungen Unterstützung von Moskau erhalten*, „Die Politische Meinung" 2016, nr 509, s. 99–103.
41. Shekhovtsov A., *Pro-Kremlin "Re-information" Efforts: Structural Relations between the Russian Media and the European Far Right* [online], http://www.integrityinitiative.net/articles/496 [dostęp: 11 XII 2016].
42. Shekhovtsov A., *Russian Fascist Aleksandr Dugin Gathering Intelligence on the French Military*, „The Interpreter" [online] z 28 września 2014 r., http://www.interpretermag.com/russian-fascist-aleksandr-dugin-gathering-intelligence-on-the-french-military/ [dostęp: 11 XII 2016].
43. Shekhovtsov A., *Russian Fascist Aleksandr Dugin's Dreams of Dictatorship in Russia* [online], http://anton-shekhovtsov.blogspot.com/2014/02/russian-fascist-aleksandr-dugin-is.html [dostęp: 11 XII 2016].
44. Shekhovtsov A., *Russian Politicians Building an International Extreme Right Alliance*, „The Interpreter" [online] z 15 września 2015 r., http://www.interpretermag.com/russian-politicians-building-an-international-extreme-right-alliance/ [dostęp: 12 XII 2016].
45. Shekhovtsov A., *The Far-Right "International Russian Conservative Forum" to Take Place in Russia*, „The Interpreter" [online] z 10 marca 2015 r., http://www.interpretermag.com/the-far-right-international-russian-conservative-forum-to-take-place-in-russia/ [dostęp: 12 XII 2016].
46. Sykulski L., *Integracja polityczna Eurazji we współczesnej rosyjskiej myśli geopolitycznej*, w: *Studia nad geopolityką XX wieku*, P. Eberhardt (red.), Warszawa 2013, PAN, s. 349–363.
47. Sykulski L., *Koncepcja Radykalnego Podmiotu i „Czwarta Teoria Polityczna" Aleksandra Dugina w kontekście bezpieczeństwa Polski i Unii Europejskiej*, „Przegląd Geopolityczny" 2014, nr 8, s. 229–242.
48. Thomas T.L., *The Russian Understanding of Information Operations and Information Warfare*, w: *Volume III of Information Age Anthology: The Information Age Military*, D.S. Alberts, D.S. Papp (red.), Washington 2001, CCRP, s. 777–815.

49. Umland A., *Aleksandr Dugin's Transformation from a Lunatic Fringe Figure into a Mainstream Political Publicist, 1980–1998: A Case Study in the Rise of Late and Post-Soviet Russian Fascism*, „Journal of Eurasian Studies" 2010, nr 1, s. 144–152.
50. Umland A., *Kulturhegemoniale Strategien der russischen extremen Rechten: Die Verbindung von faschistischer Ideologie und metapolitischer Taktik im „Neo-eurasimus" des Aleksandr Dugin*, „Österreichische Zeitschrift für Politikwissenschaft" 2004, nr 33, s. 437–454.
51. *Výroční zpráva Bezpečnostní informační služby za rok 2014* [online], https://www.bis.cz/pdf/2014-vz-cz.pdf [dostęp: 8 XII 2016].
52. Wojnowski M., *„Zarządzanie refleksyjne" jako paradygmat rosyjskich operacji informacyjno-psychologicznych w XXI w.,* „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 12, s. 11–36.
53. Wojnowski M., *Aleksandr Dugin a resorty siłowe Federacji Rosyjskiej. Przyczynek do badań nad wykorzystaniem geopolityki przez cywilne i wojskowe służby specjalne we współczesnej Rosji*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 11–38.
54. Аверьянов В.В. i in., *Другая холодная война. Стратегия для России*, „Изборский клуб" 2014, nr 10, s. 20–50.
55. Андреева О.С., *Неправительственные организации как инструмент глобальной политики*, „Власть" 2009, nr 4, s. 54–57.
56. Бовдунов А., *Цивилизационные разборки* [online], http://evrazia.org/article/230 [dostęp: 10 XII 2016].
57. Гавриш Г.Б., *Онтология неоевразийского политико-правового дискурса,* Ростов-на-Дону 2006, Ростовский юридический институт МВД России.
58. Гавриш Г.Б., *Трансформация механизмов обеспечения национальной безопасности в условиях постмодерна. Институциональные аспекты*, „Информационные войны" 2008, nr 2, s. 24–37.
59. Гавриш Г.Б., *Философия неоевразийства в контексте парадигм «пространства» и «времени»* [online], http://evraz-info.narod.ru/30.htm [dostęp: 10 XII 2016].
60. Домбровская И., *СИРИЗА, Дугин и Камменос: опасные связи или «полезные идиоты»?* [online], http://ru.rfi.fr/rossiya/20150308-opasnye-svyazi-grechesko-i-sirizy-s-moskvoi [dostęp: 11 XII 2016].
61. Дугин А.Г., *Геополитика постмодерна. Времена новых империй. Очерки геополитики XXI века*, Санкт-Петербург 2007, Амфора.
62. Дугин А.Г., Коровин В., Бовдунов А., *Сетевые войны (аналитический доклад)*, „Изборский клуб" 2013, nr 10, s. 38–68.
63. Дугин А.Г., *Логос и мифос. Социология глубин*, Москва 2010, Академический Проект, Трикста.
64. Дугин А.Г., *Принципы и стратегия грядущей войны* [online], http://katehon.com/ru/article/principy-i-strategiya-gryadushchey-voyny [dostęp: 2 XII 2016].
65. Дугин А.Г., *Русская война*, Москва 2015, ТД Алгоритм.
66. Дугин А.Г., *Сетецентричные войны*, „Информационные войны" 2008, nr 1, s. 10–17.
67. Дугин А.Г., *Стратегические выводы Прямой Линии Путина* [online], http://evrazia.org/article/2505 [dostęp: 2 XII 2016].
68. Дугин А.Г., *Теоретические основы сетевых войн*, „Информационные войны" 2008, nr 1, s. 2–10.

69. Дугин А.Г., *Философия глобализма – философия контрглобализма» (доклад на международной конференции «Глобализм и глобальная безопасность», г. Москва, декабрь 2000 г., Храм Христа Спасителя)*, w: *Основы евразийства*, А.Г. Дугин (red.), Москва 2002, Арктогея-центр, s. 548–557.
70. Дугин А.Г., *Четвёртая политическая теория. Россия и политические идеи XXI века*, Санкт-Петербург 2009, ТИД Амфора.
71. Зарифуллин П., *Сетевая война на Северном Кавказе*, „Информационные войны" 2008, nr 2, s. 37–42.
72. Зог О., *Инструменты Кремля: эксклюзивный список агентов российского влияния в европейских странах* [online], http://argumentua.com/stati/instrumenty-kremlya-eksklyuzivnyi-spisok-agentov-rossiiskogo-vliyaniya-v-evropeiskikh-stranakh [dostęp: 11 XII 2016].
73. Ипатов О.С., Кефели И.Ф., Левкин И.М., *Информационная геополитика на службе российского государства*, „Геополитика и безопасность" 2016, nr 2, s. 25–35.
74. Карпович О.Г., Манойло А.В., Филимонов Г.Ю., *Технологии «мягкой» силы на вооружении США: ответ России*, Москва 2015, ЮНИТИ-ДАНА.
75. Коновалов Д.А., Мельникова И.В., *Сравнительный анализ направлений современной российской консервативной общественно-политической мысли*, „Вестник Омского университета" 2013, nr 1, s. 181–188.
76. Коровин В.М., *Сетевая война Америки против России на примере Чечни*, „Информационные войны" 2008, nr 2, s. 42–47.
77. Коровин В.М., *Главная военная тайна США. Сетевые войны*, Москва 2009, Издательский дом Питер.
78. Коровин В.М., *Третья мировая сетевая война*, Санкт-Петербург 2014, Издательский дом Питер.
79. Косов Ю.В., Вовенда Ю.В., *Геополитические концепции информационного противоборства в российской общественной мысли*, „Управленческое консультирование" 2015, nr 10, s. 95–100.
80. Кунакова Л.Н., *Информационная война как объект научного анализа (понятие и основные характеристики информационной войны)*, „Альманах современной науки и образования" 2012, nr 6, s. 93–96.
81. Лауринавичюс М., *Россия при Путине. План Кремля для Европы* [online], http://ru.delfi.lt/v-fokuse/novosti/rossiya-pri-putine-plan-kremlya-dlya-evropy/ [dostęp: 11 XII 2016].
82. Лепский В.Е., Степанов А.М., *Особенности рефлексивных процессов в культовых организациях*, „Рефлексивные процессы и управление" 2002, nr 2, s. 59–73.
83. Манойло А.В., *Сепаратизм как вызов и угроза международной безопаности*, „Геополитический журнал" 2014, nr 7, s. 11–24.
84. Манойло А.В., *Ценностные основы управления межцивилизационными конфликтами: российская модель*, „Международные отношения" 2012, nr 1, s. 32–43.
85. Мартьянов Д.С., *Виртуальные ценности: структура, динамика, противоречия*, „Труды Санкт-Петербургского государственного института культуры и искусств" 2015, nr 206, s. 319–327.

86. Мелентьева Н.В., *Контргегемония по горизонтали и по вертикали (пролегомены к Евразийской версии)*, w: *Левиафан: Контргегемония и евроцентризм*, А.Г. Дугин (red.), Москва 2013, Евразийское Движение, s. 55–80.
87. Михаил Ефимович Фрадков [online], https://riss.ru/profile/fradkov/ [dostęp: 27 I 2017].
88. Наумов А.О., *Международные неправительственные организации и проблемы глобального управления*, „Государственное управление" 2013, nr 9, s. 49–76.
89. Подвинцев О.Б., *О моде на консерватизм в постсоветской России и разнообразии её природы*, „Вестник Пермского Университета" 2015, nr 2, s. 27–33.
90. Рустамова Ф., Цой И., Самуилкина А., *Как фонд Константина Малофеева помогает Новороссии* [online], http://www.rbc.ru/politics/08/09/2014/ [dostęp: 11 XII 2016].
91. Савин Л.В., *Горизонты войны*, w: *Геополитика. Информационно-аналитическое издание. Выпуск XXI: Война*, Л.В. Савин (red.), Москва 2013, Евразийское движение, s. 22–35.
92. Савин Л.В., *Сетецентричные войны – от концепции к спецоперациям*, w: *Геополитика. Информационно-аналитическое издание. Выпуск IV: Безопасность*, Л.В. Савин (red.), Москва 2010, Евразийское движение, s. 70–78.
93. Савин Л.В., *Новые способы ведения войны. Как Америка строит империю*, Санкт-Петербург 2016, Издательский дом Питер.
94. Савин Л.В., *От шерифа до террориста. Очерки о геополитике США*, Москва 2012, Евразийское движение.
95. Савин Л.В., *Сетецентричная и сетевая война. Введение в концепцию*, Москва 2011, Евразийское движение.
96. Савин Л.В., Федорченко С.Н., Шварц О.К., *Сетецентрические методы в государственном управлении*, Москва 2015, Сам полиграфист.
97. Сухович Е.В., *Социокультурный и онтологический уровни осмысления понятия «сеть»*, „Известия Волгоградского государственного педагогического университета" 2011, nr 9, s. 8–11.
98. Ткачёв И., Макаренко Г., Сухаревская А., *Наши в Европе. Откуда берутся союзники Кремля за рубежом*, „Ежедневная деловая газета РБК" 2015, nr 130, s. 1–4.
99. Умланд А., *Заблуждения западных апологетов Путина: пугало «русофобии» и внешняя критика нынешнего руководства Кремля*, „Форум новейшей восточноевропейской истории и культуры" 2015, nr 2, s. 261–267.
100. Яницкий О.Н., *Идеология и сеть*, „Власть" 2016, nr 1, s. 30–36.

Abstrakt

Artykuł dotyczy genezy, teorii oraz zastosowania rosyjskiej koncepcji wojny sieciowej. Ten termin został wprowadzony w Rosji przez Aleksandra Dugina. Według Dugina i jego współpracowników z ruchu eurazjańskiego rosyjska koncepcja wojny sieciowej stała się głównym środkiem do osiągania celów państwa w polityce międzynarodowej, regionalnej i wewnętrznej, a także do zyskiwania geopolitycznej przewagi, szczególnie w sferze informacyjnej. Stworzyli oni model „sieci eurazjańskiej", który jest odpowiedzią na „amerykańskie wyzwanie sieciocentryczne". Zdaniem geopolityka

„sieć eurazjańska" powinna się składać z grupy wysokich urzędników państwowych, najlepszych (zaangażowanych) kadr wywodzących się z rosyjskich służb specjalnych oraz rosyjskich i prorosyjskich intelektualistów, uczonych, politologów, patriotycznie zorientowanych dziennikarzy, artystów i działaczy kultury. Dugin zaproponował także stworzenie podstaw ideologicznych wojny sieciowej prowadzonej w celu uzyskania przewagi informacyjnej. Jego nowa ideologia, sformułowana w książce pt. *Czwarta Teoria Polityczna*, stanowi alternatywę dla amerykańskiej hegemonii i NATO.

Słowa kluczowe: wojna sieciowa, Aleksandr Dugin, ruch eurazjański, Czwarta Teoria Polityczna, geopolityka.

Abstract

The article concerns the origins, theory and application of the concept of the Russian netwar. This term was introduced in Russia by Aleksandr Dugin. According to Dugin and his contributors from Eurasian Movement, the Russian concept of netwar is the means the state uses to achieve its goals in international, regional and domestic politics and also to gain a geopolitical advantage, especially in information sphere. They created the "Eurasian" network model. It offers a symmetric response to the "net-centric challenge from the US". According to Dugin, the Eurasian network is conceived to consist of a special group of senior officials, the best "mission-oriented" staff from the Russian secret services, Russian and pro-Russian intellectuals, scientists, political scientists and the corps of patriotically-oriented journalists and culture activists. Dugin also offers ideological foundations for the netwar to gain informational advantage. The new ideology proposed by Dugin in his book *The Fourth Political Theory* is an alternative to American hegemony and NATO.

Keywords: netwar, Alexandr Dugin, Eurasian Movement, Fourth Political Theory, geopolitics.

Dariusz Gradzi

Bezpieczeństwo płatności elektronicznych jako element cyberbezpieczeństwa państwa – przegląd regulacji prawnych

Uwagi wstępne

Rynek płatności elektronicznych należy do tych segmentów gospodarki, które mają olbrzymi potencjał rozwojowy. Wraz ze wzrostem liczby i wartości transakcji rośnie zagrożenie związane z płatnościami dokonywanymi drogą elektroniczną[1]. Płatności elektroniczne dzieli się tradycyjnie na płatności internetowe[2] (dokonywane za pośrednictwem Internetu) oraz płatności mobilne[3]. Zarówno jedne, jak i drugie mogą być dokonywane przy użyciu karty płatniczej oraz poleceń przelewu (tradycyjny przelew bankowy lub tzw. pay-by-link[4] – PBL).

W obszarze płatności elektronicznych można zidentyfikować pięć głównych elementów szczególnie narażonych na zagrożenia. Są to:

1) systemy płatności[5], podmioty rozliczające transakcje płatnicze (np. Krajowa Izba Rozliczeniowa SA) oraz infrastruktura systemów kart płatniczych (w tym organizacji kartowych[6]),
2) informatyczne systemy bankowe,
3) infrastruktura podmiotów zaangażowanych w procesowanie transakcji płatniczych (w tym agentów rozliczeniowych),
4) infrastruktura akceptantów, tj. podmiotów będących odbiorcami płatności internetowej[7],

---

[1] A. Bury, *Karty płatnicze w Polsce*, Warszawa 2002, s. 183.

[2] B. Chinowski, *Elektroniczne metody płatności. Istota, rozwój, prognozy* [online], https://www.knf.gov.pl/Images/Elektroniczne%20metody%20platnosci_tcm75-36397.pdf, s. 5 [dostęp: 4 V 2016].

[3] Płatności dokonywane przy użyciu mobilnych urządzeń wyposażonych w system operacyjny, z multimedialnym interfejsem przy wykorzystaniu technologii radiowej, sieci telekomunikacyjnych bezprzewodowych (GSM, GPRS, UMTS, Wi-Fi, NFC, RFiD, Bluetooth), https://www.ecb.europa.eu/paym/cons/pdf/131120/recommendationsforthesecurityofmobilepaymentsdraftpc201311en.pdf [dostęp: 3 V 2016].

[4] Jest to jedna z metod płatności internetowych polegających na tym, że podczas zakupów online w trakcie płatności przez „bramkę płatniczą" klient otrzymuje specjalny link, który przekierowuje go do jego banku i po zalogowaniu pojawia się uzupełniony format przelewu z danymi odbiorcy (agenta rozliczeniowego) oraz kwotą. Natychmiast po autoryzacji przelewu odbiorca dostaje komunikat o płatności i może przystąpić do wykonania umowy, co znacznie przyspiesza transakcję online. Warunkiem skorzystania przez płatnika z tej usługi jest jej udostępnianie przez bank, w którym płatnik ma rachunek. Zob także: M. Grabowski, *Instrumenty płatnicze w prawie polskim* [online], https://depotuw.ceon.pl/bitstream/handle/item/327/Instrumenty%20Płatnicze%20w%20prawie%20polskim.pdf?sequence=1, s. 211 [dostęp: 12 V 2016].

[5] SORBNET2, TARGET2-NBP dla płatności wysokokwotowych, ELIXIR, EXPRESS ELIXIR, Krajowy System Rozliczeń, System płatności BlueCash, System Płatności Mobilnych BLIK, System Płatności Kartowych dla płatności detalicznych, http://www.nbp.pl/home.aspx?f=/systemplatniczy/nadzor_syst_platn/systemy_platnosci.html [dostęp: 2 V 2016].

[6] Art. 2 ust. 19b) *Ustawy z dnia 19 sierpnia 2011* r. *o usługach płatniczych* (Dz.U. z 2016 r. poz. 1572) definiuje organizację kartową jako podmiot określający zasady wydawania i akceptowania kart płatniczych, zawierający umowy z wydawcami (bankami) lub agentami rozliczeniowymi (będzie to np. VISA lub Mastercard).

[7] Art. 2 ust. 1b) ustawy o usługach płatniczych definiuje akceptanta jako odbiorcę innego niż konsument, na którego rzecz agent rozliczeniowy świadczy usługę płatniczą (w tym ujęciu będzie to np. sklep internetowy akceptujący zarówno płatności kartowe, jak i płatności za pośrednictwem tzw. pay-by-linków – przelewów

5) aplikacje i infrastruktura użytkowników końcowych, zarówno internetowych, jak i mobilnych (w tym urządzeń przenośnych oraz komputerów).

Część wymienionych elementów tworzy infrastrukturę krytyczną[8] i jest objęta Narodowym Programem Ochrony Infrastruktury Krytycznej[9], można je bowiem zaliczyć do systemów finansowych, których funkcjonowanie jest możliwe dzięki systemom łączności i teleinformatycznym. Tak zwana infrastruktura krytyczna obejmuje m.in. systemy bankowe i finansowe oraz telekomunikacyjne[10]. Na obszar płatności elektronicznych składają się zarówno systemy rzeczywiste (obiekty, serwery), jak i cybernetyczne, które umożliwiają świadczenie usług płatniczych w postaci płatności elektronicznych tylko w przypadku ich współistnienia i wzajemnej zależności. Z uwagi na specyfikę tych usług płatniczych (zdalny dostęp do infrastruktury informatycznej) oraz otwarty charakter systemów bankowych (do których wejście jest możliwe przy wykorzystaniu sieci publicznych) są one narażone na cyberprzestępczość.

Cyberprzestępczość sensu largo może być rozumiana jako (…) *posługiwanie się sieciami telekomunikacyjnymi do naruszania jakiegokolwiek dobra prawnego chronionego przez prawo karne*[11]. *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016*[12] definiuje cyberprzestępstwo jako (…) *czyn zabroniony popełniony w „cyberprzestrzeni"*. Cyberprzestrzeń jest rozumiana z kolei jako (…) *cyfrowa przestrzeń przetwarzania i wymiany informacji tworzona przez systemy i sieci teleinformatyczne wraz z powiązanymi pomiędzy nimi oraz relacjami z użytkownikami*. Użytkownikami – poza administracją rządową, organami władzy ustawodawczej i sądowniczej – są także osoby indywidulane (tj. klienci korzystający z płatności elektronicznych) oraz przedsiębiorcy (dostawcy usług płatniczych, np. banki)[13]. Statystyki dotyczące incydentów w cyberprzestrzeni koordynowanych przez Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT (ang. Computer Emergency Response Team)[14] pokazują wzrost liczby incydentów w stosunku do lat poprzednich. W 2014 r. zarejestrowano 12 017 przypadków, z czego 7498 zakwalifikowano jako incydent[15].

Wolumen elektronicznych transakcji płatniczych a skala zagrożenia

Na wykresach przedstawiono dynamikę wzrostu krajowych transakcji bezgotówkowych, dokonywanych zarówno kartami płatniczymi, jak i przy wykorzystaniu poleceń przelewu.

natychmiastowych, w których kwota transakcji płatniczej jest rozliczna przy udziale pośredniczącego agenta rozliczeniowego).

[8] W rozumieniu art. 3 pkt 2 ppkt b), c) i d) *Ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (tekst jednolity: Dz.U. z 2013 r. poz. 1166, ze zm).

[9] W rozumieniu art. 5b) ustawy o zarządzaniu kryzysowym.

[10] Por. art. 3 pkt 2 ustawy o zarządzaniu kryzysowym oraz R. Kośla, *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac* [online], http://www.cert.pl/PDF/Kosla_p.pdf [dostęp: 2 V 2016].

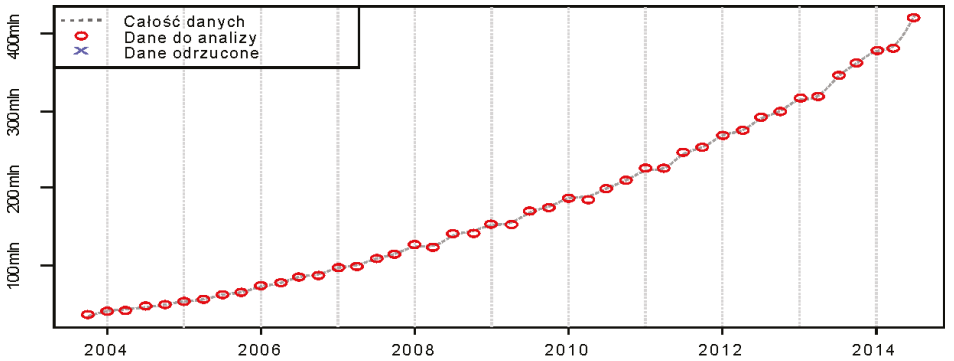
[11] M. Staszczyk, *Nieuprawnione transakcje bankowe jako przejaw cyberprzestępczości* [online], http://www.finanseiprawofinansowe.uni.lodz.pl/Publikacje/5/4_Staszczyk.pdf, s. 46 [dostęp: 12 V 2016].

[12] *Rządowy Program Ochrony Cyberprzestrzeni RP na lata 2011–2016* [online], https://bip.mswia.gov.pl/bip/programy/19057,Rzadowy-Program-Ochrony-Cyberprzestrzeni-RP-na-lata-2011-2016.html [dostęp: 2 V 2016].

[13] Tamże.

[14] http://www.cert.gov.pl/cer/o-nas/15,O-nas.html [dostęp: 7 V 2016].

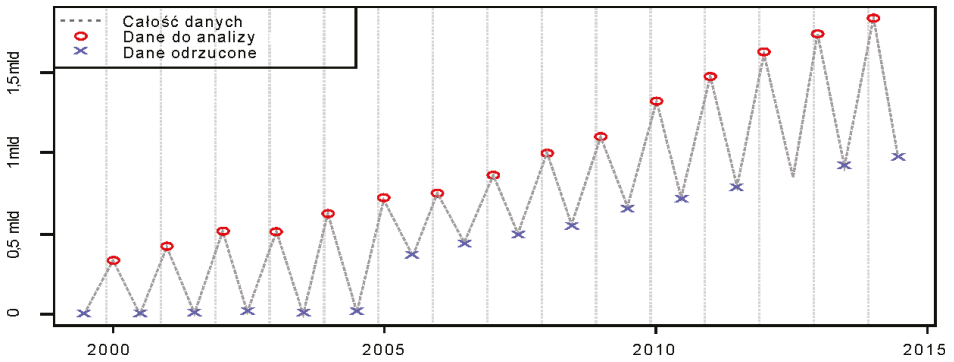
[15] *Raport o stanie bezpieczeństwa cyberprzestrzeni RP w 2014 roku*, http://www.cert.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/738,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2014-roku.html, s. 6, [dostęp: 2 V 2016].



Wykres 1. Liczba transakcji dokonanych kartami płatniczymi w latach 2004–2014.

Źródło: M. Kozakiewicz, M. Kwas, *Prognoza wybranych wskaźników rozwoju obrotu bezgotówkowego na lata 2014–2020* [online], http://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/prognoza2014-2020.pdf [dostęp: 2 V 2016].

Specjaliści zajmujący się tematyką płatności elektronicznych prognozują wzrost liczby transakcji z około 1,4 mld w 2013 r. (o łącznej wartości około 123 mld zł) do ok. 5,5 mld w 2020 r. (o łącznej wartości około 304 mld zł).



Wykres 2. Liczba złożonych poleceń przelewu w latach 2000–2015.

Źródło: M. Kozakiewicz, M. Kwas, *Prognoza wybranych wskaźników rozwoju obrotu bezgotówkowego na lata 2014–2020* [online], http://www.nbp.pl/systemplatniczy/obrot_bezgotowkowy/prognoza2014-2020.pdf [dostęp: 2 V 2016].

W przypadku poleceń przelewu prognozuje się, że ich liczba wzrośnie z około 1,0 mld w 2013 r. do około 2,7 mln w 2020 r.

Skala zagrożenia

W raporcie Europejskiego Banku Centralnego (ECB) za 2012 r.[16] wskazano, że całkowita wartość transakcji oszukańczych CNP (ang. *card not present* – transakcja dokonywana bez fizycznego przedstawienia karty[17], w środowisku internetowym) wyniosła 794 mln euro. Całkowita wartość oszukańczych transakcji kartowych – zarówno CNP, POS (ang. *points of sale* – transakcje u akceptantów z fizyczną prezentatą karty), jak i ATM (ang. *automated teller machine* – transakcje bankomatowe) w obszarze SEPA (ang. Single Euro Payment Area – Jednolity Obszar Płatności w Euro[18]) wyniosła 1,33 mld euro. Całkowita wartość transakcji oszukańczych CNP stanowiła zatem 60 proc. wszystkich oszustw kartowych.

Dało to asumpt do zintensyfikowania prac nad istniejącymi zagrożeniami. Równolegle do prowadzonych prac nad dyrektywą PSD II[19], która już obowiązuje i ma być wdrożona w państwach członkowskich do 13 stycznia 2018 r., Europejski Urząd Nadzoru Bankowego, Europejski Bank Centralny i polski regulator – Komisja Nadzoru Finansowego (KNF) – wydały swoje zalecenia odnośnie do podniesienia poziomu bezpieczeństwa płatności elektronicznych.

Do najważniejszych aktów prawnych dotyczących bezpieczeństwa płatności elektronicznych należą:

- dyrektywa w sprawie usług płatniczych (PSD I)[20],
- ustawa o usługach płatniczych wprowadzająca dyrektywę PSD I[21],
- dyrektywa w sprawie usług płatniczych (PSD II),
- wytyczne, zalecenia i rekomendacje opracowane i wydane przez Europejski Urząd Nadzoru Bankowego (ang. European Banking Authority – EBA), Europejski Bank Centralny oraz Komisję Nadzoru Finansowego.

Wszystkie trzy wymienione regulacje – wydane przez EBA, ECB i KNF – są bardzo zbliżone do siebie i podobnie skonstruowane redakcyjne, różnią się natomiast częściowo zakresem stosowania. Zdecydowanie najdalej idąca jest *Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe*[22] Komisji Nadzoru Finansowego, w której wyklucza się przekazywanie danych wrażliwych podmiotom trzecim – TPP (ang. *Third Party Providers*) oraz istotnie obostrza się otwieranie rachunków płatniczych „na przelew", o czym będzie mowa dalej.

Przed szczegółową analizą usług płatności elektronicznych konieczne jest zaprezentowanie siatki pojęciowej, która pozwoli na precyzyjne odniesienie się do procesu

[16] *Third Report on card fraud* [online], ECB (European Central Bank) z II 2014 r., https://www.ecb.europa.eu/pub/pdf/other/cardfraudreport201402en.pdf [dostęp: 7 V 2016].

[17] R. Kaszubski, Ł. Obzejta, *Karty płatnicze w Polsce*, Warszawa 2012, s. 22.

[18] http://www.sepapolska.pl/index.php/co-to-jest-sepa [dostęp: 6 V 2016].

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

[20] *Dyrektywa 2007/64/WE Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48/WE i uchylająca dyrektywę 97/5/WE* (Dz.Urz. UE L 319/1 z 5 XII 2007 r.).

[21] Dz.U. z 2016 r. poz. 1572.

[22] https://www.knf.gov.pl/Images/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf [dostęp: 8 V 2016].

dokonywania płatności elektronicznej i jej uczestników. Zgodnie z polską ustawą o usługach płatniczych:

- d o s t a w c a – to podmiot świadczący usługi płatnicze. W ustawie o usługach płatniczych zawarto wykaz dostawców, którymi mogą być m.in. banki krajowe, instytucje kredytowe, instytucje pieniądza elektronicznego, instytucje płatnicze, spółdzielcze kasy oszczędnościowo-kredytowe oraz biura usług płatniczych;
- a k c e p t a n t – to odbiorca inny niż konsument, dla którego agent rozliczeniowy świadczy usługę płatniczą (np. sklep stacjonarny lub internetowy). Jest to podmiot, który przyjmuje zapłatę w formie bezgotówkowej[23];
- u s ł u g a p ł a t n i c z a – to usługa, której istotą jest zmiana posiadania środków pieniężnych za pośrednictwem podmiotu trzeciego. Środki z rachunku w jednym banku zostają zapisane na rachunku użytkownika w innym banku. Ta usługa umożliwia zatem płatnikowi przekazanie środków pieniężnych odbiorcy. W ustawie o usługach płatniczych wprowadzono wykaz usług płatniczych. Do najbardziej typowych należą:
  - przyjmowanie wpłat gotówki,
  - dokonywanie wypłat gotówki,
  - prowadzenie rachunku płatniczego (warto odnotować, że podmiotem uprawnionym do prowadzenia rachunku płatniczego są nie tylko banki),
  - wykonywanie usług polecenia zapłaty,
  - wykonywanie usług polecenia przelewu (tradycyjny przelew bankowy),
  - wykonywanie transakcji płatniczych przy użyciu karty płatniczej lub podobnego instrumentu płatniczego,
  - wydawanie instrumentów płatniczych, np. kart płatniczych (ang. *issuing*),
  - wykonywanie transakcji płatniczych instrumentem płatniczym płatnika, zainicjowanych przez akceptanta lub za jego pośrednictwem, polegających na ich autoryzacji, przesyłaniu do wydawcy karty płatniczej lub systemów płatności zleceń płatniczych płatnika albo akceptanta mających na celu przekazanie akceptantowi należnych mu środków – (ang. *acquiring*)[24],
  - z wyjątkiem czynności rozrachunku transakcji w ramach systemu płatności w rozumieniu ustawy o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami[25]. Mowa tutaj o dokonywaniu płatności kartą płatniczą w sklepie (u tzw. akceptanta karty), który autoryzuje i rozlicza transakcję w ramach usług acquiringu świadczonych przez agentów rozliczeniowych. Agenci przekazują zlecenie płatnicze osoby dokonującej płatności do banku, który wydał kartę, i następnie – po otrzymaniu z tego banku środków pieniężnych – rozliczają się z akceptantem,
  - świadczenie przekazu pieniężnego (transfer środków pieniężnych przyjętych od płatnika do odbiorcy bez prowadzenia dla niego rachunku płatniczego – np. przyjmowanie opłat za rachunki o niskiej wartości w celu ich przekazania usługodawcom lub przyjmowanie wpłat, aby udostępnić je odbiorcy);

[23] M. Pacak, *Usługi płatnicze. Komentarz*, Warszawa 2014, s. 7.

[24] R. Kaszubski, Ł. Obzejta, *Karty płatnicze*…, s. 107.

[25] *Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami* (tekst jednolity: Dz.U. z 2016 r. poz. 1224).

- u ż y t k o w n i k – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, korzystająca z usług płatniczych jako płatnik lub odbiorca;
- p ł a t n i k – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, składająca zlecenie płatnicze prowadzące do obciążenia jej rachunku płatniczego lub dokonania wpłaty środków (podmiot dokonujący płatności);
- o d b i o r c a – to osoba fizyczna, prawna lub jednostka organizacyjna niebędąca osobą prawną, której ustawa przyznaje zdolność prawną, będąca odbiorcą środków pieniężnych stanowiących przedmiot transakcji płatniczej (podmiot otrzymujący płatność);
- zlecenie płatnicze – to oświadczenie płatnika lub odbiorcy skierowane do dostawcy zawierające polecenie wykonania transakcji płatniczej[26]. Inicjuje ono transakcję płatniczą. Do jego złożenia może być użyty instrument płatniczy. W zleceniu powinny być zawarte dane umożliwiające przeprowadzenie transakcji: dane płatnika i odbiorcy, kwota transakcji, unikatowy identyfikator odbiorcy, np. numer rachunku bankowego IBAN (ang. *International Bank Account Number*)[27];
- t r a n s a k c j a p ł a t n i c z a – to wpłata, transfer lub wypłata środków pieniężnych zainicjowane przez płatnika lub odbiorcę. Transakcja płatnicza może być:
  – zainicjowana przez płatnika, np. polecenie przelewu (tradycyjny przelew bankowy), które płatnik przesyła do swojego dostawcy usług płatniczych[28],
  – zainicjowana przez odbiorcę, jeśli płatnik uprzednio udzielił odbiorcy zgody na obciążenie rachunku płatnika w umownych terminach zapłaty z tytułu określonych zobowiązań. W tym wypadku to odbiorca inicjuje transakcję płatniczą bez udziału płatnika (np. polecenie zapłaty[29]);
- i n s t r u m e n t p ł a t n i c z y – to urządzenie lub procedury[30] wykorzystywane przez użytkownika do składania zleceń płatniczych uzgodnione przez użytkownika i dostawcę. W zakres jego desygnatów wchodzą:
  – przedmioty materialne, jak np. karty płatnicze,
  – zespoły procedur technicznych, jak np. interfejsy bankowości elektronicznej[31];
- k a r t a p ł a t n i c z a – to karta uprawniająca do wypłaty gotówki (bankomatowa) lub umożliwiająca złożenie zlecenia płatniczego za pośrednictwem akceptanta lub agenta rozliczeniowego;
- k a r t a d e b e t o w a – to karta płatnicza umożliwiająca wykonywanie transakcji płatniczych, z wyjątkiem transakcji wchodzących w skład środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu;
- k a r t a k r e d y t o w a – to karta płatnicza umożliwiająca wykonywanie transakcji płatniczych wchodzących w skład środków pieniężnych udostępnionych użytkownikowi z tytułu kredytu.

[26] M. Pacak, *Usługi płatnicze*..., s. 14.
[27] M. Grabowski, *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2012, s. 28.
[28] Tamże, s. 27.
[29] Art. 63d *Ustawy z dnia 29 sierpnia 1997 – Prawo bankowe* (tekst jednolity: Dz.U. z 2016 r. poz. 1988).
[30] M. Pacak, *Usługi płatnicze*…, s. 10.
[31] M. Grabowski, *Ustawa o usługach płatniczych*…, s. 19.

Pakiet regulacyjny

Szczegółowe omówienie zasygnalizowanych wcześniej aktów prawnych należy rozpocząć od pakietu regulacyjnego dotyczącego bezpieczeństwa płatności elektronicznych, na który składają się:

Zalecenia Europejskiego Banku Centralnego[32] (opracowane przez SecurePay – Europejskie Forum ds. Bezpieczeństwa Płatności Detalicznych – wspólną platformę współpracy dla EBA i ECB[33]). Zalecenia zostały opublikowane 31 marca 2013 r. z datą implementacji 1 lutego 2015 r. Komisja Nadzoru Finansowego w piśmie z 8 maja 2014 r. skierowanym do podmiotów nadzorowanych wskazała, że będzie uwzględniać przestrzeganie tych zaleceń przez dostawców w trakcie procesu nadzorczego. Oprócz wymienionych dostawców usług płatniczych zalecenia mają także zastosowanie do podmiotów zarządzających systemami płatności, tj. podmiotów odpowiedzialnych za całościowe funkcjonowanie systemu obsługującego dany instrument płatniczy (np. organizacje kartowe, Krajowa Izba Rozliczeniowa SA)[34].

6. **Wytyczne EBA**. Dokument został opublikowany 19 grudnia 2014 r. z datą stosowania od 1 sierpnia 2015 r.[35] EBA wydał 21 maja 2015 r. tzw. *compliance table*[36], w którym KNF oświadczył, że będzie się stosował do wytycznych w całości. Podobnie jak zalecenia ECB, wytyczne stosuje się także do systemów płatności[37].
7. **Rekomendacja Komisji Nadzoru Finansowego dotycząca bezpieczeństwa transakcji płatniczych w Internecie**. *Rekomendacja KNF*[38], której założenia zostały zaakceptowane 25 sierpnia 2015 r. na 272. posiedzeniu Komisji Nadzoru Finansowego, poprzedzona projektem skierowanym do konsultacji z podmiotami nadzorowanymi, została finalnie wydana 17 listopada 2015 r. Jest ona wzorowana na opublikowanych uprzednio wytycznych oraz zaleceniach EBA i ECB. Jej przedmiotem jest przede wszystkim zabezpieczenie elektronicznych kanałów komunikacji i zdalnego korzystania z usług płatniczych. *Rekomendacja KNF* jest skierowana do następujących dostawców:

[32] *Zalecenie Europejskiego Banku Centralnego z dnia 2 sierpnia 2016 r. w sprawie systemu zarządzania jakością danych na potrzeby statystyki inwestycji w papiery wartościowe (EBC/2016/24) (2016/C 297/01)* [online], https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf [dostęp: 2 V 2016].

[33] https://www.ecb.europa.eu/pub/pdf/other/mandateeuropeanforumsecurityretailpayments201410.en.pdf [dostęp: 2 V 2016].

[34] https://www.ecb.europa.eu/pub/pdf/other/recommendationssecurityinternetpaymentsoutcomeofpcfinalversionafterpc201301en.pdf, s. 1 [dostęp: 2 V 2016].

[35] Wytyczne zostały wydane na podstawie art. 16 ust. 3 *Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 1093/2010 z dnia 24 listopada 2010 r. w sprawie ustanowienia Europejskiego Urzędu Nadzoru (Europejskiego Urzędu Nadzoru Bankowego), zmiany decyzji nr 716/2009/WE oraz uchylenia decyzji Komisji 2009/78/WE* (Dz.Urz. UE L 331/12 z 15 XII 2010 r.).

[36] *Compliance Table – Guidelines* [online], https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+Compliance+Table-GL+security+of+internet+payments.pdf/34be3c3e-5521-4036-9805-3ee97162c4db [dostęp: 7 V 2016].

[37] https://www.eba.europa.eu/documents/10180/934179/EBA-GL-2014-12+%28Guidelines+on+the+security+of+internet+payments%29.pdf/f27bf266-580a-4ad0-aaec-59ce52286af0, s. 10 [dostęp: 2 V 2016].

[38] *Rekomendacja dotycząca bezpieczeństwa transakcji płatniczych wykonywanych w internecie przez banki, krajowe instytucje płatnicze, krajowe instytucje pieniądza elektronicznego i spółdzielcze kasy oszczędnościowo-kredytowe* [online], https://www.knf.gov.pl/Images/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf [dostęp: 21 I 2017].

– banków,
– krajowych instytucji płatniczych,
– krajowych instytucji pieniądza elektronicznego,
– spółdzielczych kas oszczędnościowo-kredytowych.

Rekomendacja KNF jest najniższym wspólnym mianownikiem w zakresie bezpieczeństwa, gdyż wprowadza minimalne wymogi, które dostawcy są zobowiązani stosować. Te wymogi nie zawierają szczegółowego opisu działań, a wyłącznie wyznaczają cele, pozostawiając dostawcom wybór środków do ich osiągnięcia. Komisja Nadzoru Finansowego już przed wydaniem *Rekomendacji KNF* dostrzegała ryzyko związane z płatnościami elektronicznymi i zarządzaniem tzw. credentialami (danymi do logowania). Z tego powodu zostały wydane:

- *Ostrzeżenie przed dopuszczeniem pośredników do rachunku bankowego w płatnościach internetowych*[39],
- komunikat – *Ryzyko związane z podawaniem innemu bankowi danych do logowania do rachunku bankowego*[40],
- poradnik na temat zasad bezpieczeństwa w bankowości elektronicznej[41],
- *Rekomendacja D dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach*[42],
- *Rekomendacja M dotycząca zarządzania ryzykiem operacyjnym w bankach*[43].

Rekomendacja KNF zawiera opis 14 szczegółowych zagadnień dotyczących następujących obszarów:

- zasad i organizacji procesu zarządzania i oceny ryzyka płatności internetowych,
- szczególnych środków kontroli i bezpieczeństwa w zakresie płatności internetowych,
- świadomości i edukowania klientów.

Rekomendacja, o której mowa, nie ma zastosowania do:

- płatności mobilnych innych niż przy użyciu przeglądarki internetowej (nie ma ona zastosowania np. do płatności dokonywanych przez odpowiednie aplikacje bankowe zainstalowane przez użytkownika na urządzeniach typu smartfon czy tablet),
- płatności zlecanych za pośrednictwem poczty tradycyjnej, polecenia telefonicznego, poczty głosowej lub technologii esemesowej,
- transakcji płatniczych dokonywanych przez przedsiębiorstwa za pośrednictwem dedykowanych sieci,
- usług innych niż dokonywanych w zakresie płatności internetowych (takich jak: elektroniczne usługi maklerskie, umowy zawierane online), świadczonych przez dostawców usług płatniczych za pośrednictwem ich stron internetowych.

[39] https://www.knf.gov.pl/Images/KNF_podawanie_danych_dostepu_do_rachunku_18_11_2013_tcm75-36300.pdf [dostęp: 6 V 2016]. Ostrzeżenie dotyczyło praktyki ujawniania podmiotowi trzeciemu (np. SOFDORT GmbH pośredniczącemu w inicjowaniu transakcji) danych niezbędnych do jej przeprowadzenia, który to podmiot sam automatycznie wypełniał formatkę przelewu.

[40] https://www.knf.gov.pl/o_nas/komunikaty/2014/ryzyko_zwiazane_z_podawaniem_innemu_bankowi_danych_do_logowania.html [dostęp: 7 V 2016].

[41] M. Górnisiewicz, R. Sobczyński, M. Struś, *Bezpieczeństwo finansowe w bankowości elektronicznej – przestępstwa finansowe związane z bankowością elektroniczną* [online], https://www.knf.gov.pl/Images/Bezp_finansowe_tcm75-39005.pdf [dostęp: 15 V 2016].

[42] https://www.knf.gov.pl/Images/Rekomendacja_D_8_01_13_uchwala_7_tcm75-33016.pdf [dostęp: 5 V 2016].

[43] https://www.knf.gov.pl/Images/Nowa_rekomendacja_M_projekt_tcm75-31515.pdf [dostęp: 5 V 2016].

Najistotniejszym wyłączeniem jest to odnoszące się do płatności mobilnych. Oznacza to, że *Rekomendacja KNF* nie dotyczy wszelkich płatności mobilnych, jeżeli są one dokonywane za pośrednictwem dedykowanych aplikacji (np. specjalnych, tworzonych przez dostawców aplikacji płatniczych w smartfonach, niebazujących na przeglądarce internetowej).

Omawiany dokument jest stosowany od 5 grudnia 2016 r., z wyjątkiem regulacji dotyczących rachunków płatniczych otwieranych „na przelew", wytycznych dotyczących właściwego i bezpiecznego używania spersonalizowanych danych uwierzytelniających i zakazu ich ujawniania, a także opisu obowiązków oraz zakresu odpowiedzialności dostawcy i klienta w zakresie korzystania z usług płatności elektronicznych.

Rekomendacja KNF, wprowadzając wymóg nieujawniania spersonalizowanych danych do logowania (login i hasło), ogranicza działalność podmiotów trzecich, tzw. świadczących usługi dostępu do rachunku płatniczego, obecnych na polskim rynku. Zaliczamy do nich: AIS (ang. *Account Information Service*) – usługę dostępu do informacji o rachunku płatniczym, która umożliwia zebranie w jednej aplikacji kont z różnych banków, porównywanie ich stanu, historii oraz prowadzenie statystyk wydatków; a także PIS (ang. *Payment Initiation Service*) – usługę inicjowania płatności przez podmiot trzeci (po przekazaniu przez klienta danych do logowania do konta bankowego podmiot trzeci wypełnia dane do przelewu i zleca go z konta bankowego jako klient).

Z uwagi na obszerność i wieloaspektowość zagadnień poruszonych w *Rekomendacji KNF* poniżej zostaną zaprezentowane tylko te, które mają największe znaczenie z punktu widzenia przedmiotu artykułu.

Polityka bezpieczeństwa

Każdy dostawca powinien wdrożyć i poddawać regularnej weryfikacji i aktualizacji formalny, odrębny dokument, w którym została określona polityka bezpieczeństwa w zakresie płatności elektronicznych. Wymagane jest również jej każdorazowe zatwierdzenie przez zarząd lub inny właściwy organ zarządzający.

Ocena ryzyka

Każdą usługę płatniczą oferowaną użytkownikowi należy szczegółowo ocenić pod kątem jej bezpieczeństwa i potencjalnego ryzyka, które jest z nią związane. Powinno się to odbywać zarówno na etapie projektowania i wdrażania usługi, jak i podczas jej użytkowania produkcyjnego. Na podstawie wyników oceny dostawcy ustalają, czy i jeżeli tak, to jakie zmiany są niezbędne do wprowadzenia do stosowanych obecnie środków bezpieczeństwa.

W ocenie ryzyka usługi płatniczej trzeba uwzględniać potrzebę ochrony i zabezpieczenia tzw. wrażliwych danych płatniczych. W *Rekomendacji KNF* w r a ż l i w e d a n e p ł a t n i c z e są zdefiniowane jako dane, których uzyskanie przez podmiot nieuprawniony może doprowadzić do dokonania nadużycia (mowa tutaj o danych: służących do zainicjowania transakcji płatniczej, danych wykorzystywanych do uwierzytelnienia – potwierdzenia – tożsamości klienta oraz wykorzystywanych do zamawiania przez klientów instrumentów płatniczych lub narzędzi uwierzytelniających)[44]. Są nimi przede wszystkim: loginy, hasła, numery PIN, numery

[44] https://www.knf.gov.pl/Images/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf, s. 6 [dostęp: 7 V 2016].

telefoniczne, adresy pocztowe, adresy e-mail, numery IBAN[45], numer PAN[46] karty płatniczej, kod CVV/CVC[47] karty, data ważności karty, numer karty[48]).

Incydenty

Dostawcy są zobowiązani do opracowania procedur dotyczących monitorowania incydentów bezpieczeństwa i postępowania w przypadku ich wystąpienia. Ta procedura ta ma przede wszystkim uwzględniać zgłaszanie incydentów kierownictwu (zarządowi) dostawcy oraz – w przypadku *poważnych incydentów bezpieczeństwa* – także właściwym organom, w tym Generalnemu Inspektorowi Informacji Finansowej, Generalnemu Inspektorowi Ochrony Danych Osobowych, Komisji Nadzoru Finansowego oraz Narodowemu Bankowi Polskiemu. Przez poważny incydent bezpieczeństwa płatności rozumie się w *Rekomendacji KNF* incydent, który ma (lub może mieć) istotny wpływ na bezpieczeństwo, integralność lub ciągłość działania systemów dostawcy. Przy tej ocenie należy uwzględnić m.in. liczbę klientów potencjalnie poszkodowanych z powodu wystąpienia incydentu oraz zagrożoną kwotę transakcji[49]. Dostawcy są zobowiązani do opracowania dodatkowej procedury współpracy z właściwymi organami ścigania.

Agenci rozliczeniowi powinni umownie zobowiązać akceptantów, na których rzecz świadczą usługi, do współpracy w zakresie poważnych incydentów bezpieczeństwa. W przypadku gdy dany akceptant nie współpracuje lub narusza zasady współpracy, na agencie rozliczeniowym spoczywa obowiązek wyegzekwowania zobowiązań wynikających ze współpracy lub rozwiązania umowy z takim akceptantem.

Przeciwdziałanie ryzyku

Omawiana *Rekomendacja KNF* wymaga od dostawców wdrożenia środków bezpieczeństwa zgodnych z opracowaną polityką bezpieczeństwa. Przy projektowaniu produktów płatniczych dostawcy powinni odpowiednio dzielić środowiska na rozwojowe, testowe i produkcyjne. Zostali też zobowiązani do wdrożenia zasady minimalnych uprawnień przy zarządzaniu dostępem.

W tym dokumencie nakazano wdrożenie procesów monitorowania, śledzenia i ograniczania dostępu do wrażliwych danych płatniczych oraz krytycznych zasobów logicznych i fizycznych (bazy danych, sieci, systemy).

Wymaga się, aby środki bezpieczeństwa były poddawane okresowym audytom przeprowadzanym przez niezależnych ekspertów. Z grona ekspertów zostały wyłączone podmioty zaangażowane w rozwój, wdrażanie i zarządzanie usługami płatności internetowych.

---

[45] IBAN (ang. *International Bank Account Number*) – międzynarodowy standard numeracji kont bankowych. Został on utworzony przez Europejski Komitet Standardów Bankowych do wspomożenia obsługi płatności w Unii Europejskiej, za: http://www.najlepszekonto.pl/numer-konta-bankowego-iban [dostęp: 14 II 2017] – przyp. red.

[46] Ang. *Primary Account Number*.

[47] CVV – Card Verification Value (w organizacji VISA), CVC – Card Verification Code (w organizacji MasterCard), zob. R. Kaszubski, Ł. Obzejta, *Karty płatnicze*…, s. 17.

[48] J.M. Nieto, *European Banking Authority Guidelines on the Security of Internet Payments* [online], http://www.slideshare.net/jmnietomoreno/european-banking-authority-guidelines-on-the-security-of-internet-payments [dostęp: 28 IV 2016].

[49] https://www.knf.gov.pl/Images/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf, s. 6 [dostęp: 7 V 2016].

W każdej umowie outsourcingowej[50] w zadaniach dotyczących bezpieczeństwa należy uwzględniać wymogi wprowadzone *Rekomendacją KNF*.

Największe ryzyko związane z przetwarzaniem danych klientów występuje po stronie akceptantów, z których wielu nie ma odpowiedniej infrastruktury i możliwości finansowych na jej opracowanie i wdrożenie, co prowadzi do kradzieży tożsamości lub nieuprawnionego dostępu do danych płatniczych. Z tego powodu agenci rozliczeniowi zostali zobowiązani do aktualizowania umów z akceptantami pod kątem zastosowania przez nich środków bezpieczeństwa w zgodzie z *Rekomendacją KNF*. W przypadku gdy akceptant nie stosuje się do tych wymogów, agent powinien rozwiązać z nim umowę, co w praktyce oznacza jej wypowiedzenie przez agenta.

Śledzenie transakcji

Każdą transakcję płatniczą należy szczegółowo zarejestrować przez nadanie jej numeru porządkowego, znacznika czasowego[51], odnotowanie danych transakcyjnych, ich zmian i ingerencji w te dane. *Rekomendacja KNF* wprowadza wymóg, aby dostawcy prowadzili dzienniki zdarzeń umożliwiające śledzenie wprowadzania nowych danych transakcyjnych oraz ich modyfikowania i usuwania.

Identyfikacja klienta

Dostawcy powinni identyfikować klienta zgodnie z właściwymi przepisami ustawy o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu[52] przed uzyskaniem dostępu do danej usługi płatniczej. Jak się wydaje, chodzi tutaj zarówno o samą procedurę identyfikacji, jak i o zweryfikowanie informacji podanych przez klienta zgodnie z postanowieniami wspomnianej ustawy[53]. *Rekomendacja KNF* nakłada na banki wymóg – stosowany od 1 lipca 2016 r. – aby po zawarciu umowy o prowadzenie rachunku płatniczego, do którego otwarcia wykorzystano przelew z innego banku jako potwierdzenie tożsamości klienta, nie było możliwe otwarcie przelewem weryfikacyjnym z tego rachunku kolejnego rachunku płatniczego (konta bankowego)[54]. Warto odnotować, że w *Rekomendacji KNF* doszło do zmiany w stosunku do projektu, w którym przy otwieraniu rachunku „na przelew" wymagano każdorazowo osobistego potwierdzenia tożsamości klienta. Ma to stanowić kompromis między ergonomią produktów bankowych z jednej strony a walką z nadużyciami przy zakładaniu rachunków bankowych „na przelew". Tym samym dopuszczono możliwość otwarcia rachunku płatniczego na podstawie tzw. przelewu weryfikacyjnego z innego banku, przy założeniu, że ten bank przy tradycyjnym otwieraniu konta dopełnił wszelkich wymogów w zakresie identyfikacji i weryfikacji klienta.

[50] Outsourcing (skrót z ang. *outside-resource-using*) – wydzielenie ze struktury organizacyjnej przedsiębiorstwa niektórych funkcji i przekazanie ich do wykonania innym podmiotom, za: https://pl.wikipedia.org/wiki/Outsourcing. Wśród głównych założeń umowy zawieranej w outsourcingu pomiędzy zleceniodawcą a wyspecjalizowaną firmą usługową wyróżnia się obustronne zrozumienie zasad i warunków współpracy oraz wskazanie konsekwencji niedostosowania się stron do przyjętych uzgodnień, za: https://mfiles.pl/pl/index.php/Umowa_outsourcingowa (przyp. red.).

[51] Znacznik czasu (stempel czasu, ang. *time stamp*) – dane ułatwiające określenie momentu, w którym zaszło określone zdarzenie, za: https://pl.wikipedia.org/wiki/Znacznik_czasu (przyp. red.).

[52] Art. 8b, 9 i 9a *Ustawy z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (tekst jednolity: Dz.U. z 2016 r. poz. 299).

[53] Tamże.

[54] https://www.knf.gov.pl/Images/REKOMENDACJA_dot_bezpieczenstwa_transakcji_platniczych_tcm75-43526.pdf, s. 16 [dostęp: 7 V 2016].

Zgodnie z *Rekomendacją KNF* dostawcy mają obowiązek informowania klientów o właściwym i bezpiecznym używaniu spersonalizowanych danych uwierzytelniających (haśle, loginie, kodzie SMS), bezpiecznym używaniu sprzętu i oprogramowania, sposobie postępowania na wypadek kradzieży lub utraty danych uwierzytelniających, procedurze postępowania w przypadku wykrycia nadużyć lub ich podejrzenia. Dodatkowo dostawca ma mieć możliwość zablokowania określonej transakcji lub instrumentu płatniczego ze względów bezpieczeństwa.

Silne uwierzytelnienie klienta (ang. „strong customer authentication")

Jest to niewątpliwie najważniejsze zalecenie *Rekomendacji KNF* skierowane do dostawców. Jego podstawą było założenie, aby uwierzytelnienie użytkownika przy dokonywaniu transakcji było co najmniej dwuelementowe, dzięki czemu można zmniejszyć liczbę transakcji oszukańczych. Silne uwierzytelnienie klienta jest jednym z najważniejszych elementów zawartych w dyrektywie PSD II. Polega ono na tym, że dostawca (np. bank), chcąc uwierzytelnić klienta, ma obowiązek zastosować co najmniej dwa z trzech wymienionych elementów weryfikujących:

1) wiedzę klienta (hasło, kod PIN) – coś, o czym wie tylko użytkownik,
2) posiadanie (własność klienta, np. telefon komórkowy) – coś, co użytkownik ma,
3) cechy klienta (cecha biometryczna) – coś, czym użytkownik jest.

Te elementy muszą być niezależne od siebie w ten sposób, że ujawnienie jednego z nich nie naraża innego elementu na zidentyfikowanie. Jeden z nich (z wyjątkiem cechy klienta) musi być niemożliwy do ponownego użycia oraz niemożliwy do nieautoryzowanego pozyskania przez Internet.

Zgodnie z *Rekomendacją KNF* nr 7 silne uwierzytelnienie klienta należy stosować w przypadku inicjowania płatności w środowisku internetowym lub uzyskiwania dostępu przez klienta do tzw. wrażliwych danych płatniczych bądź ich modyfikacji (np. powiadomienie banku o numerze telefonu, na który jest wysyłany SMS w celu zautoryzowania transakcji). Jako dobrą praktykę dostawców w *Rekomendacji KNF* przewidziano możliwość powiązania autoryzacji z określoną kwotą lub odbiorcą płatności (rachunek bankowy lub jego fragment), co oznacza dodanie odpowiednich informacji w SMS-ie autoryzacyjnym. Należy zauważyć, że banki będą dążyły do alternatywnych metod autoryzacji ze względu na koszty. Jak się bowiem szacuje, roczny koszt wysyłania kodów autoryzacyjnych SMS-em to wydatek 60–70 mln zł[55].

Silne uwierzytelnienie klienta może nie być stosowane przez dostawców w przypadkach:

- płatności na rzecz tzw. zaufanych odbiorców, zdefiniowanych z nazwy i numeru rachunku bankowego przez użytkownika na tzw. białych listach,
- transakcji między dwoma rachunkami płatniczymi tego samego klienta, prowadzonymi przez tego samego dostawcę,
- innych przelewów w ramach jednego dostawcy, uzasadnionych analizą ryzyka transakcji płatniczej,
- płatności o niskiej wartości, zgodnie z postanowieniami ustawy o usługach płatniczych, tj. płatności dokonywanych przy użyciu instrumentów płatniczych na

[55] *Bezpieczeństwo bankowości elektronicznej. Narzędzia identyfikacji, uwierzytelniania i autoryzacji w nowej rzeczywistości. Raport specjalny 01/2016 kwiecień* [online], http://www.obserwatorium.biz/images/posts/raports/5_PL.pdf, s. 1 [dostęp: 21 I 2017].

kwotę nieprzekraczającą równowartości 30 euro w walucie polskiej, albo które mają ustalony limit wydatków w wysokości nieprzekraczającej równowartości 150 euro w walucie polskiej, lub też służą do przechowywania środków pieniężnych w kwocie nieprzekraczającej w żadnym momencie równowartości 150 euro w walucie polskiej[56].

W *Rekomendacji KNF* przewidziano silne uwierzytelnianie klienta także w przypadku transakcji kartami płatniczymi. Musi je umożliwiać wydawca karty, tj. najczęściej bank, przez przystosowanie do tego każdej karty. W praktyce oznacza to, że niewystarczające jest autoryzowanie[57] transakcji płatniczej samym numerem karty, datą ważności i kodem CVV/CVC[58]. Dodatkowo musi być użyty drugi element w postaci np. kodu SMS.

W dyrektywie PSD II silne uwierzytelnienie klienta jest unormowane w artykule 97. Ma ono następować w przypadkach:

- uzyskiwania dostępu do rachunku płatniczego w trybie online,
- inicjowania płatności elektronicznej,
- przeprowadzania czynności za pomocą kanału zdalnego, co może wiązać się z ryzykiem oszustwa płatniczego lub innych nadużyć.

W przypadku inicjowania elektronicznych zdalnych transakcji płatniczych dostawcy mają stosować silne uwierzytelnienie klienta z elementem, który dynamicznie łączy konkretną transakcję z określoną kwotą i określonym odbiorcą. To oznacza uwierzytelnienie np. za pośrednictwem kodu SMS, który obligatoryjnie będzie musiał zawierać kwotę oraz wskazywać odbiorcę zlecenia płatniczego. Europejski Bank Centralny w dokumencie konsultacyjnym z 8 grudnia 2015 r., sporządzonym w celu opracowania tzw. regulacyjnego standardu technicznego[59] w zakresie wymogów „silnego uwierzytelnienia klienta", wskazał, że wartość użyta przy „dynamicznym łączeniu" transakcji może być wykorzystana tylko do uwierzytelnienia konkretnej transakcji i żadnej innej, nie może też być ponownie użyta w przypadku jej ujawnienia[60].

Narzędzia uwierzytelniające

Rekomendacja KNF obliguje dostawców do tego, aby wnioskowanie przez klientów o narzędzia uwierzytelniające i (lub) oprogramowanie oraz dostarczanie klientom narzędzi służących do uwierzytelniania oraz oprogramowania odbywało się w sposób bezpieczny. To oznacza, że tego typu procesy powinny się odbywać w zaufanym środowisku informatycznym. Dostawca jest zobowiązany do stworzenia procedury dostarczania spersonalizowanych danych uwierzytelniających oraz oprogramowania (powinno być ono m.in. podpisane cyfrowo przez dostawcę).

---

[56] Art. 19 *Ustawy z dnia 19 sierpnia 2011 r. o usługach płatniczych* (tekst jednolity: Dz.U. z 2016 r. poz. 1572).

[57] R. Kaszubski, Ł. Obzejta, *Karty płatnicze*…, s. 165.

[58] https://www.knf.gov.pl/Images/14_06_2013_karty%20zblizeniowe_tcm75-34934.pdf, s. 11 [dostęp: 12 V 2016].

[59] Więcej informacji i status prawny RTS (regulacyjnych standardów technicznych) znajduje się w piśmie KNF z 22 V 2014 r., https://www.knf.gov.pl/Images/Pismo_UKNF_do_bankow_dot_%20aktow_wykonawczych_i_wytycznych_do_CRD_IV_CRR_tcm75-38013.pdf [dostęp: 6 V 2016].

[60] https://www.eba.europa.eu/documents/10180/1303936/EBA-DP-2015-03+(RTS+on+SCA+and+CSC+under+PSD2).pdf, s. 13 [dostęp: 2 V 2016].

Logowanie, sesje płatnicze

W tym zakresie dostawcy już wcześniej wprowadzili odpowiednie standardy. Zostały one powtórzone w *Rekomendacji KNF* i uzupełnione przez zapisanie:

- ograniczania liczby prób logowania lub uwierzytelniania,
- zasad wygaszania sesji płatniczych,
- okresu ważności haseł ograniczonego do niezbędnego minimum,
- określenia maksymalnej liczby nieudanych prób logowania lub uwierzytelniania, po których ma nastąpić blokada dostępu,
- automatycznego zamykania nieaktywnych usług płatności internetowych po upływie określonego czasu.

Monitorowanie transakcji

Każdą transakcję płatniczą należy monitorować pod kątem potencjalnego nadużycia. Z tego powodu dostawcy są zobowiązani stosować mechanizmy mające na celu zapobieganie nielegalnym (oszukańczym) transakcjom, wykrywać je oraz blokować ich wykonanie. Te mechanizmy powinny być oparte na określonych regułach, takich jak czarne listy naruszonych lub skradzionych danych kart płatniczych. Dodatkowo należy monitorować nietypowe zachowania klientów lub urządzeń podczas sesji płatniczych (np. zmianę adresu IP czy zakresu adresów IP) lub nietypowe kategorie akceptantów. Agenci rozliczeniowi są zobowiązani do posiadania odpowiednich mechanizmów zapobiegających nadużyciom ze strony akceptantów.

Ochrona wrażliwych danych płatniczych

W *Rekomendacji KNF* zobowiązano dostawców usług płatniczych do ochrony i zabezpieczenia tzw. wrażliwych danych płatniczych, o których była już mowa wcześniej, przed kradzieżą i nieautoryzowanym dostępem podczas ich przechowywania, przetwarzania i przesyłania. Wprowadzono także zasadę nieprzechowywania przez akceptantów jakichkolwiek danych wrażliwych, z wyjątkiem sytuacji, w której są one immanentnie związane z daną usługą płatniczą.

Edukowanie klientów

Komisja Nadzoru Finansowego za pośrednictwem *Rekomendacji*... kładzie nacisk na uświadamianie klientów, jakie ryzyko jest związane z korzystaniem z płatności elektronicznych i jak bezpiecznie przeprowadzać transakcje w środowisku internetowym. Najważniejszym wymaganiem nałożonym na dostawców jest umożliwienie takiej komunikacji z klientem, aby mógł on zweryfikować autentyczność otrzymanych wiadomości. W tym celu dostawcy powinni wdrożyć co najmniej jeden kanał komunikacyjny oraz poinformować klientów, że wiadomości przekazywane im za pośrednictwem innego kanału (np. e-maila) będą niewiarygodne.

Dodatkowo dostawcy są zobowiązani do wdrożenia programów edukacyjnych dla klientów na temat bezpiecznego korzystania z płatności elektronicznych oraz zapoznania ich z:

- procedurami zgłaszania transakcji podejrzanych lub oszukańczych,

- sposobem powiadamiania klienta przez dostawcę o transakcjach podejrzanych lub oszukańczych.

Istotnym zaleceniem jest to, aby akceptanci jasno oddzielali proces dokonywania płatności elektronicznej przez „bramę płatniczą" od dokonywania zakupów online. Ma to na celu klarowne oddzielenie komunikacji z dostawcą usług płatniczych od komunikacji z akceptantem (np. sklepem).

Limity dla transakcji płatniczych

Dostawcy mają obowiązek ustalenia limitu transakcyjnego dla płatności internetowych przed rozpoczęciem świadczenia usług w postaci np. maksymalnej wartości indywidualnej transakcji płatniczej lub maksymalnej łącznej wartości transakcji w określonym czasie[61]. Dobrą praktyką dostawców ma być także powiadamianie SMS-em lub telefonicznie o transakcjach podejrzanych lub wysokiego ryzyka. Ponadto dostawcy powinni – w ramach dobrych praktyk – umożliwić użytkownikom dalsze indywidualne określenie swoich zachowań i nawyków płatniczych przez możliwość zezwolenia przez użytkownika na inicjowanie płatności tylko z określonych krajów (płatności z innych krajów mają być blokowane) czy definiowania białych i czarnych list odbiorców płatności (podmiotów, do których mogą lub nie mogą być dokonywane płatności internetowe z danego rachunku płatniczego).

Status inicjacji i realizacji płatności

Dostawcy usług płatniczych są zobowiązani do potwierdzania klientom zainicjowania płatności internetowej oraz dostarczania im informacji mających na celu zorientowanie się, czy transakcja została zainicjowania i wykonana prawidłowo. Powinni także umożliwiać klientom w niemal rzeczywistym czasie weryfikację statusu wykonania transakcji oraz salda rachunku w dowolnym momencie oraz w bezpiecznym i zaufanym środowisku.

Podsumowanie

Cyberprzestępczość z uwagi na jej rozmiar już dawno straciła wymiar wyłącznie prawnokarny, a zyskała nowy – gospodarczy i społeczny[62]. Coraz powszechniejsze jest wykorzystywanie nowych metod płatności elektronicznych (w tym przelewów pay-by-link) lub rachunków bankowych otwieranych „na przelew" do popełniania przestępstw[63]. Celem podmiotów oferujących usługi w zakresie płatności elektronicznych jest przyspieszenie i uproszczenie procesu zapłaty. W przypadku transakcji kartowych lub przelewów pay-by-link standardowe środki prawne[64], które mają przeciwdziałać

[61] Uwidacznia się tutaj potencjalny konflikt *Rekomendacji KNF* z zasadą swobody dysponowania środkami zgromadzonymi na rachunku przez posiadacza – art. 50 *Ustawy z dnia 29 sierpnia 1997 r. – Prawo bankowe* (tekst jednolity: Dz.U. z 2016 r. poz. 1988).

[62] A. Kańciak, *Problematyka cyberprzestępczości w Unii Europejskiej*, „Przegląd Bezpieczeństwa Wewnętrznego" 2013, nr 8; także: [online] http://www.abw.gov.pl/pl/pbw/publikacje/przeglad-bezpieczenstw-9/931,Przeglad-Bezpieczenstwa-Wewnetrznego-nr-8-5-2013.html [dostęp: 28 IV 2016].

[63] http://lublin.wyborcza.pl/lublin/1,48724,17474196,Ukradli_z_konta_60_tys__zl__Czy_bank_zareagowal_zbyt.html [dostęp: 6 V 2016].

[64] Art. 106a ustawy prawo bankowe – blokada środków na rachunku oraz art. 18 *Ustawy z dnia*

transakcjom oszukańczym, są bardzo często zawodne, ponieważ niezwykle trudno jest zidentyfikować i „uchwycić" na czas daną transakcję. Z tego powodu istnieje potrzeba właściwego uregulowania bezpieczeństwa płatności na etapie organizacji infrastruktury i procedur. Prawidłowe funkcjonowanie płatności elektronicznych oraz zaufanie użytkowników tego wymiaru cyberprzestrzeni, a także reputacja instytucji finansowych, są warunkiem koniecznym ich rozwoju.

Regulacje wydane przez ECB, EBA i KNF należy odebrać pozytywnie jako próbę podniesienia poziomu bezpieczeństwa, zanim dyrektywa PSD II i wprowadzony przez nią wymóg „silnego uwierzytelnienia klienta" zostaną zaimplementowane do krajowego porządku prawnego. Statystyki Narodowego Banku Polskiego za drugą połowę 2015 r.[65] pokazują, że banki odnotowały w tym czasie 38 976 przypadków oszustw kartowych na kwotę 18,6 mln zł, co obrazuje tendencję spadkową w stosunku do pierwszej połowy tego samego roku. Niemniej jednak należy zauważyć, że aż 55 proc. wszystkich oszustw kartowych dotyczy przestępstw dokonywanych w Internecie (CNP) i że w ich przypadku tendencja jest wzrostowa. Cyberprzestępczość na rynku płatności elektronicznych jest i nadal będzie stałym elementem przestępczości związanej z obrotem gospodarczym[66].

Bibliografia:

1. Bury A., *Karty płatnicze w Polsce*, Warszawa 2002, CeDeWu.
2. *Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) 1093/2010 oraz uchylająca dyrektywę 2007/64/WE* (Dz.Urz. UE L 337/35 z 23 XII 2015 r.).
3. *Dyrektywa Parlamentu Europejskiego i Rady z dnia 13 listopada 2007 r. w sprawie usług płatniczych w ramach rynku wewnętrznego zmieniająca dyrektywy 97/7/WE, 2002/65/WE, 2005/60/WE i 2006/48 WE i uchylająca dyrektywę 97/5/WE* (Dz.Urz. UE L 319/1 z 5 XII 2007 r.)
4. Grabowski M., *Ustawa o usługach płatniczych. Komentarz*, Warszawa 2012, C.H. Beck.
5. Kaszubski R., Obzejta Ł., *Karty płatnicze w Polsce*, Warszawa 2012, Wolters Kluwer.
6. Pacak M., *Usługi płatnicze. Komentarz*, Warszawa 2014, LexisNexis.
7. *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym* (tekst jednolity: Dz.U. z 2013 r. poz. 1166, ze zm.).
8. *Ustawa z dnia 19 sierpnia 2011 r. o usługach płatniczych* (Dz.U. z 2016 r. poz. 1572).
9. *Ustawa z dnia 24 sierpnia 2001 r. o ostateczności rozrachunku w systemach płatności i systemach rozrachunku papierów wartościowych oraz zasadach nadzoru nad tymi systemami* (tekst jednolity: Dz.U. z 2016 r. poz. 122).

16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu (tekst jednolity: Dz.U. z 2016 r. poz. 299) – wstrzymanie transakcji, blokada rachunku.

[65] http://www.nbp.pl/systemplatniczy/ocena/ocena2015_2.pdf, s. 88-91 [dostęp: 12 V 2016], http://www.cashless.pl/temat-dnia/1275-uspokajajace-statystyki-nbp-liczba-fraudow-przy-uzyciu-kart-i-przelewow-mocno-spadla [dostęp: 12 V 2016].

[66] M. Staszczyk, *Nieuprawnione transakcje bankowe…* [dostęp: 12 V 2016].

10. *Ustawa z dnia 29 sierpnia 1997 r. – Prawo bankowe* (tekst jednolity: Dz.U. z 2016 r. poz. 1988).
11. *Ustawa z dnia 16 listopada 2000 r. o przeciwdziałaniu praniu pieniędzy oraz finansowaniu terroryzmu* (tekst jednolity: Dz.U. z 2016 r. poz. 299).

Abstrakt

Rynek płatności elektronicznych należy do tych segmentów gospodarki, które mają olbrzymi potencjał rozwojowy. Wraz ze wzrostem liczby i wartości transakcji rośnie zagrożenie związane z procesowaniem płatności dokonywanych elektronicznie. Coraz powszechniejsze jest wykorzystywanie nowych metod płatności elektronicznych (w tym przelewów pay-by-link) i rachunków bankowych otwieranych „na przelew" do popełniania przestępstw. Regulacje wydane przez Europejski Bank Centralny, EBA i Komisję Nadzoru Finansowego należy odebrać pozytywnie jako próbę podniesienia poziomu bezpieczeństwa. Prawidłowość dokonywania płatności elektronicznych oraz zaufanie użytkowników do tego typu usług stanowią warunek niezbędny dla rozwoju cyberprzestrzeni.

Słowa kluczowe: cyberprzestępczość, Komisja Nadzoru Finansowego, elektroniczne transakcje płatnicze, płatności mobilne, płatności internetowe.

Abstract

The market of electronic payments is one of those segments of the economy, which are endowed with huge growth potential. With the increasing volume of the transactions the risk related with processing electronic payments grows. Increasingly common is the use of new electronic payment methods (including pay-by-link transfers) or bank accounts which are opened "via the Internet" („on transfer") to commit crimes. The regulations issued by the European Central Bank, the European Banking Authority and the Financial Supervisory Authority should be assessed positively, as an attempt to raise the level of payment's security. Proper making of electronic payments and reliance of the users of these kinds of services are a prerequisite for the development of cyberspace.

Keywords: cybercrime, Financial Supervision Authority, electronic payments transactions, mobile payments, Internet payments.

Waldemar Walczak

Działania analityczno-informacyjne identyfikujące mechanizmy korupcyjne w procesach zarządzania

Wprowadzenie

Często się akcentuje, że korupcja wywołuje poważne konsekwencje dla funkcjonowania państwa, gospodarki i społeczeństwa. Opinie na temat mechanizmów korupcyjnych i skali korupcji w Polsce w dużym stopniu opierają się na subiektywnej percepcji tego zjawiska. Są także kształtowane na podstawie doniesień medialnych. Wyrażane poglądy zależą od tego, jakie dokładnie czyny i wzorce zachowań są utożsamiane z praktykami korupcyjnymi występującymi w procesach zarządzania.

Celem niniejszego artykułu jest przedstawienie rozważań i analiz przybliżających do lepszego poznania i zrozumienia mechanizmów korupcyjnych, powszechnie występujących w procesach zarządzania. Na wstępie scharakteryzowano różne sposoby definiowania omawianego pojęcia, co umożliwia szersze, a zarazem bardziej szczegółowe spojrzenie na konkretne działania określane mianem korupcji. W dalszej części pracy rozpatrywane problemy naświetlono z perspektywy podważenia zaufania do państwa i jego organów. Następnie wnikliwie omówiono cele i znaczenie realizowanych czynności o charakterze analityczno-informacyjnym oraz zaprezentowano metodykę postępowania, która umożliwia wszechstronne zidentyfikowanie i dokładniejsze zrozumienie charakteru badanych zdarzeń i procesów.

Rozumienie pojęcia k o r u p c j a – uwagi definicyjne

Korupcja jest wieloaspektowym zjawiskiem społecznym, które może być rozpatrywane i analizowane na wielu płaszczyznach[1]. Dociekania badawcze na temat tego zjawiska mogą dotyczyć zarówno rozumienia jego istoty, źródeł (przyczyn) występowania oraz uwarunkowań rozwoju[2], jak również jego konsekwencji[3]. W literaturze akcentuje się specyfikę i złożoność omawianego pojęcia z uwagi na to, że korupcja przybiera różne formy (oblicza), a wraz z rozwojem społeczeństwa pojawia się w nowych odsłonach. Podkreśla się przy tym, że występuje w wielu różnych konfiguracjach i układach, przy jednoczesnym udziale nierzadko większej liczby zaangażowanych w nią osób[4]. W świetle badań opinii publicznej korupcja jest postrzegana w kategorii jednego z najważniejszych problemów społecznych w Polsce[5], wzbudzającego powszechne zainteresowanie

[1] Zob. P. Wiatrowski, *Prawne, ekonomiczne i socjologiczne aspekty korupcji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2008, nr 776, s. 97–111; M. Brol, *Ekonomiczne, instytucjonalne i kulturowe uwarunkowania korupcji*, Monografie i Opracowania Uniwersytetu Ekonomicznego we Wrocławiu, Wrocław 2015.

[2] J. Matejuk, *Korupcja – istota, źródła, zakres i zagrożenia*, „Przegląd Organizacji" 2004, nr 5, s. 7–10.

[3] R. Bochan, *Ekonomiczno-społeczna analiza przyczyn i skutków występowania mechanizmów korupcyjnych w gospodarce*, „Studia Ekonomiczne Regionu Łódzkiego" 2013, nr 9, s. 105–128.

[4] J. Filek, *Polski trójkąt korupcyjny*, „Annales: etyka w życiu gospodarczym" 2006, tom 9, nr 1, s. 158.

[5] A. Robak, M. Czaja, *Korupcja – zarys istoty zjawiska*, w: *Postawy wobec korupcji w samorządzie terytorialnym. Raport z badań w województwie śląskim*, A. Turska-Kawa, M. Czaja (red.), Katowice 2015, s. 9.

i szeroki odźwięk w mediach. Pojawiają się też inne określenia tego zjawiska: *plaga społeczna XXI wieku*[6], *choroba społeczna niszcząca tkankę miękką społeczeństwa obywatelskiego (zaufanie, poczucie wpływu)*[7] oraz zaburzająca prawidłowe funkcjonowanie państwa, instytucji publicznych i gospodarki.

Ryszard Szyc proponuje, aby k o r u p c j ę rozumieć w ujęciu szerokim jako (…) *wszelkie wykorzystywanie władzy publicznej dla celów prywatnych*[8]. Autor dodatkowo uzupełnia swoje rozważania o cenną refleksję: *O tym, że każda władza korumpuje, wiadomo nie od dziś, a w związku z tym, że władza jest od zawsze, możemy przyjąć za pewnik, że i korupcja także istnieje od zawsze*[9]. Idąc tym tokiem rozumowania, należy zauważyć, że występowanie tzw. władzy stanowi aksjomat i wyróżnik funkcjonowania każdej organizacji (zarówno w sektorze publicznym, jak i prywatnym). Pod pojęciem w ł a d z a rozumie się naczelne kierownictwo, które ma stosowne uprawnienia i kompetencje, m.in. w zakresie zaciągania zobowiązań finansowych, podejmowania decyzji wywołujących określone skutki prawne, a także zajmowania się sprawami majątkowymi.

Według Centralnego Biura Antykorupcyjnego, pojęcie k o r u p c j i występuje w dwóch aspektach: w ujęciu ogólnym i prawnym. Wyjaśniono przy tym, że rozróżnia się korupcję w szerszym kontekście społeczno-ekonomicznym oraz w węższym, tj. na użytek prawa karnego materialnego. Wytłumaczenie dla tak dokonanej typizacji (klasyfikacji) zawiera się w zdaniu: *Podział taki stosuje się, ponieważ prawo karne wymaga precyzyjnego, jednoznacznego języka, zaś dla celów np. prewencyjnych wystarczające jest używanie szerokiego pojęcia*[10]. Dodatkowo podkreślono, że korupcja rozumiana w znaczeniu ogólnym (…) *obejmuje również te zachowania, które nie są spenalizowane, a ich popełnianie co najwyższej narusza zasady etyki, moralności, kultury, np. nepotyzm czy kumoterstwo*[11], które określa się mianem *niekaralnych form korupcji*[12]. W związku z powyższym w pełni zasadne i adekwatne będzie posługiwanie się określeniem l e g a l n a k o r u p c j a w odniesieniu do wszystkich działań, czynów i zachowań korupcyjnych, których popełnianie nie wiąże się z ponoszeniem odpowiedzialności karnej.

Według CBA n e p o t y z m oznacza nadużywanie zajmowanego stanowiska przez protegowanie krewnych. Zaznaczono przy tym, że (…) *podstawowym wyznacznikiem nepotyzmu jest tak zwana bezpośrednia podległość służbowa*[13]. Z takiego sformułowania jasno wynika, że brak występowania bezpośredniej zależności służbowej będzie oznaczać, że nie mamy do czynienia z nepotyzmem. W praktyce takie działania najczęściej polegają na lokowaniu krewnych w tej samej instytucji publicznej, ale w departamentach, biurach, komórkach organizacyjnych, którymi kierują inne, zaprzyjaźnione osoby. Kumoterstwo tym różni się od nepotyzmu, że faworyzowanie osób, które otrzymują lukratywne stanowiska, nie wynika z pokrewieństwa, ale z powiązań towarzyskich[14]. W praktyce zarządzania kumoterstwo jest synonimem wzajemnego poplecznictwa i pro-

[6] B. Hołyst, *Korupcja jako plaga społeczna XXI wieku*, „Przegląd Antykorupcyjny" 2011, nr 1, s. 24.

[7] A. Turska-Kawa, *Psychologiczne determinanty korupcji politycznej*, w: *Postawy wobec korupcji w samorządzie terytorialnym*…, s. 31.

[8] R. Szyc, *Miejsce organów kontroli w walce z korupcją – identyfikacja i eliminacja mechanizmów korupcjogennych*, „Kontrola Państwowa" 2015, nr 6, s. 37.

[9] Tamże, s. 37.

[10] *Poradnik antykorupcyjny dla przedsiębiorców. Przedsiębiorca w środowisku zagrożeń korupcyjnych*, Warszawa 2011, s. 12.

[11] Tamże, s. 12.

[12] Tamże, s. 30.

[13] *Poradnik antykorupcyjny dla przedsiębiorców...*, s. 30.

[14] Tamże, s. 30.

tekcjonizmu opartego na kolesiostwie. Najczęściej takie zjawiska znajdują swoje odzwierciedlenie w procesach akceleracji ścieżek kariery oraz zapewniania lukratywnych posad gronu wybrańców, co w rezultacie prowadzi do wytworzenia się zorganizowanych koterii zawłaszczających instytucje sektora finansów publicznych. Elementem, który wyróżnia współdziałającą grupę osób należących do wytworzonej kamaryli jest dbanie o realizację i ochronę partykularnych, prywatnych interesów. Koneksje, znajomości i rozległe powiązania (zarówno towarzyskie, jak i partyjno-biznesowe) stanowią fundament i spoiwo istniejących układów.

W najnowszym opracowaniu CBA z 2016 r. zawarto następującą definicję: (…) *korupcja jest – ogólnie rzecz ujmując – nadużywaniem stanowiska lub funkcji dla osiągnięcia prywatnych korzyści*[15]. Niestety, jest to sformułowanie, które cechuje niedookreśloność i niejasność tekstu, co bezpośrednio przekłada się na swobodę interpretacyjną. Aby w praktyce eliminować konkretne zachowania korupcyjne i przeciwdziałać ich rozprzestrzenianiu się, na wstępie należy je scharakteryzować w sposób zrozumiały, precyzyjny i jednoznaczny. Pierwsza niejasność dotyczy tego, w jakim ujęciu należy interpretować zwrot *nadużywanie stanowiska* i pełnionej funkcji, druga zaś – wykazu podmiotów, pojedynczych osób lub szerszej grupy wybrańców, które zyskują możliwość *osiągnięcia prywatnych korzyści* w wyniku określonych decyzji (podejmowanych działań). Na tym tle rodzi się pytanie: Czy sformułowania zawarte w cytowanej definicji należy interpretować wyłącznie w kontekście znaczeniowym czynu zabronionego, popełnianego przez funkcjonariusza publicznego, co zostało zdefiniowane w art. 231 kk? Czy może chodzi o *instrumentalne wykorzystywanie* władzy także przez pozostałych decydentów – ewidentnie naruszające zasady równości[16] i sprawiedliwości społecznej[17] – chociażby w ramach prawnie przysługujących uprawnień (z tytułu zajmowanego stanowiska, pełnionej funkcji) dla zapewnienia korzyści osobistych i majątkowych wybranym, faworyzowanym beneficjentom? A być może takie przedsięwzięcia stanowią wyłącznie naruszenie określonych standardów, norm etyczno-moralnych, a zatem nie są przejawem działania na szkodę interesu publicznego i nie można ich w ten sposób postrzegać?

Przy uwzględnieniu sformułowań użytych w analizowanej definicji trzeba uznać, że termin k o r u p c j a swoim zakresem pojęciowym obejmuje wszystkie czyny związane z nadużywaniem stanowiska w celu zapewnienia prywatnych korzyści (osobistych i majątkowych) zarówno bezpośrednio decydentowi, jak i osobom (podmiotom) trzecim. Co więcej, nie można zawężać znamion korupcji wyłącznie do podejmowania czynności sprzecznych z prawem. Wytłumaczenie wzmacniające zasadność wyrażonej konstatacji odnajdujemy w stanowisku wyrażonym przez CBA: (…) *można rozpatrywać to zjawisko na dwóch płaszczyznach: prawnej, pojmowanej jako działanie naruszające przepisy prawa, oraz etycznej, rozumianej jako nieuczciwe zachowanie*[18]. W uzupełnieniu warto jednak dodać, że zakres penalizacji zachowań korupcyjnych wy-

[15] *Korupcja polityczna. Wskazówki dla przedstawicieli organów władzy wybieranych w wyborach powszechnych*, Centralne Biuro Antykorupcyjne, Warszawa 2016, s. 7.

[16] Art. 32 ust. 1: *Wszyscy są wobec prawa równi. Wszyscy mają prawo do równego traktowania przez władze publiczne*, ust. 2: *Nikt nie może być dyskryminowany w życiu politycznym, społecznym lub gospodarczym z jakiejkolwiek przyczyny*. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. z 1997 r. Nr 78 poz. 483, ze zm.).

[17] Art. 2 *Konstytucji RP*: *Rzeczpospolita Polska jest demokratycznym państwem prawnym, urzeczywistniającym zasady sprawiedliwości społecznej*.

[18] *Korupcja polityczna. Wskazówki dla przedstawicieli organów władzy...*, s. 7.

stępujących w rzeczywistości społeczno-gospodarczej zależy od definicji prawnej korupcji, jaka została zawarta w *Ustawie z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*[19].

Radosław Bochan trafnie i słusznie zauważa, że (…) *mechanizmy korupcyjne najczęściej usytuowane są w obszarze wzajemnych interakcji pomiędzy środowiskiem urzędniczym lub politycznym a podmiotami gospodarczymi, których działanie lub zysk zależne są od decyzji funkcjonariuszy publicznych lub osób pełniących funkcje publiczne*[20]. Nie oznacza to jednak, że korupcja występuje tylko w sferze działalności instytucji państwowych i odnosi się wyłącznie do funkcjonowania aparatu administracji publicznej[21]. Praktyki korupcyjne znajdują swoje odzwierciedlenie w procesach zarządczych związanych z bieżącą działalnością wszystkich typów organizacji. Niemniej tylko w kontekście paradygmatów zarządzania w strukturach administracji publicznej te zjawiska są ujmowane w kategorii patologii[22]. Podobne zdarzenia występujące w prywatnym biznesie są określane mianem zdolności przedsiębiorczego działania, kreatywności oraz umiejętności kształtowania korzystnych relacji biznesowych. Krzysztof Nowakowski jest zdania, że uniwersalne atrybuty korupcji obowiązują także w obrębie podmiotów prywatnych oraz w relacjach między nimi[23]. Jest to realistyczne i rozsądne postrzeganie procesów gospodarczych, które mają swoje potwierdzenie w rzeczywiści organizacyjnej, chociaż nie dla wszystkich są one łatwe do zauważenia.

Korupcja jako czynnik podważający zaufanie do państwa i jego organów

Brunon Hołyst zaznacza, że korupcja nie jest nowym zjawiskiem, istniała zawsze (…) *ale obecnie objęła już wszystkie działy służby publicznej, stała się też elementem polityki handlowej, a więc nowym rodzajem przestępczości gospodarczej*[24]. Zdaniem Pawła Falenty korupcja prowadzi do (...) *marnotrawienia środków publicznych*, a także (…) *narusza fundament systemu wolnorynkowego – zasadę uczciwej konkurencji*. W wymiarze społecznym jest podstawowym czynnikiem odpowiadającym za (…) *spadek szacunku społeczeństwa do legalnej władzy*[25]. Dodatkowo podkreśla się, że zachowania korupcyjne podważają zaufanie obywateli do norm i wartości społecznych, jakie powinny obowiązywać w państwie prawa, a także przyjętych rozwiązań instytucjonalnych[26]. Stanowią również poważne zagrożenie dla gospodarki[27] oraz prawidłowego funkcjonowania systemu demokratycznego[28], zwłaszcza z uwagi na powszechnie obo-

[19] Definicje prawne czynów, które w rozumieniu ustawy są korupcją, zostały wyszczególnione w art. 1 ust. 3a *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U. z 2006 r. Nr 104 poz. 708, ze zm.).

[20] R. Bochan, *Ekonomiczno-społeczna analiza przyczyn i skutków występowania mechanizmów korupcyjnych*..., s. 107.

[21] D. Fleszer, *Z problematyki korupcji w administracji publicznej*, w: *Jak możliwy jest dialog*?, A. Kamińska, E. Kraus, K. Ślęczka (red.), Sosnowiec 2014, s. 285.

[22] Tamże.

[23] K. Nowakowski, *Nowe zjawisko korupcji komercyjnej*, „Współczesna Ekonomia" 2010, nr 2, s. 112.

[24] B. Hołyst, *Korupcja jako plaga społeczna XXI wieku*…, s. 27.

[25] P. Falenta, *Przestępstwo korupcji – uwarunkowania karnoprawne i społeczne*, „Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu" 2016, nr 1, s. 159–160.

[26] B. Hołyst, *Korupcja jako plaga społeczna XXI wieku*…, s. 34.

[27] Wiatrowski P., *Korupcja i jej zapobieganie. Wręczenie kontrolne czy kontrolowane (uwagi de lege ferenda)*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2005, nr 690, s. 100.

[28] R. Dyoniziak, *Korupcja jako wyzwanie dla demokracji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2008, nr 763, s. 5–11.

wiązujący, chociaż rzadko przywoływany, przepis Konstytucji Rzeczpospolitej Polskiej – zgodnie z art. 1: *Rzeczpospolita Polska jest dobrem wspólnym wszystkich obywateli*[29]. A zatem z prawnego punktu widzenia zarówno majątek narodowy, jak i instytucje publiczne nie stanowią indywidualnego dobra, a tym bardziej prywatnej własności wąskiej grupy elit politycznych oraz wpływowych grup interesu.

Aleksander Cywiński przedstawia interesujące spostrzeżenia na temat istoty i wagi procesu budowy zaufania między państwem polskim a obywatelami w kontekście używanych określeń, jakie występują w obowiązujących ustawach. Autor podaje m.in. następujące przykłady przepisów prawa zawierających w swej treści słowo „zaufanie": (…) *organy administracji publicznej prowadzą postępowanie w sposób budzący zaufanie jego uczestników do władzy publicznej* (art. 8 kpa); *Urzędnik państwowy obowiązany jest w szczególności* (…) *strzec autorytetu Rzeczypospolitej Polskiej oraz dążyć do pogłębiania zaufania obywateli do organów państwa* (art. 17 ust. 2 pkt 2 ustawy o pracownikach urzędów państwowych)[30]; *Sędzia powinien* (...) *unikać wszystkiego, co mogłoby przynieść ujmę godności urzędu lub osłabić zaufanie do jego bezstronności* (art. 34 § 2 ustawy o Sądzie Najwyższym)[31]. Poczynione uwagi mają istotne walory utylitarne, umożliwiają bowiem porównanie wzorców zachowań nakazywanych przez polskie prawo z realiami codziennej praktyki zarządzania.

Wartościowym uzupełnieniem dla prowadzonych rozważań jest stanowisko Krajowej Rady Sądownictwa z 15 września 2016 r., w którym zawarto m.in. następującą argumentację: *Możliwość podejmowania przez Prezydenta arbitralnej decyzji o niepowołaniu sędziów byłaby niezgodna z art. 60 w zw. z art. 32 ust. 1 oraz w zw. z art. 2 Konstytucji, które gwarantują każdemu obywatelowi prawo dostępu do służby publicznej na jednakowych i równych zasadach*[32]. W odniesieniu do takich instytucji, jak m.in.: Biuro Trybunału Konstytucyjnego, Biuro Rzecznika Praw Obywatelskich, Kancelaria Sejmu, Kancelaria Senatu bądź Kancelaria Prezydenta RP polskie prawo nie gwarantuje równych praw obywatelom, którzy byliby zainteresowani podjęciem pracy na urzędniczych stanowiskach we wspomnianych instytucjach publicznych. O możliwości otrzymania zatrudnienia w tych podmiotach przesądza tylko i wyłącznie arbitralna decyzja osoby mającej stosowne uprawnienia decyzyjne do występowania w imieniu pracodawcy. Wypada żałować, że niewiele osób zwraca na to uwagę, w debacie publicznej zaś te sprawy pozostają całkowicie przemilczane. Należy z całą mocą podkreślić, że do wymienionych organizacji sektora finansów publicznych – zgodnie z obowiązującym prawem – nie stosuje się zasady podawania do publicznej wiadomości informacji o naborze na wolne stanowiska urzędnicze, o tzw. postępowaniach otwartych i konkurencyjnych. W teorii (bo z pewnością nie w praktyce) mają one stwarzać pozorne szanse na równe traktowanie w procesach rekrutacji do etatowej pracy, która w powszechnej opinii jest postrzegana w kategorii „służby publicznej". Te refleksje nie dają się podważyć, gdyż takie są fakty.

---

[29] *Konstytucja Rzeczypospolitej Polskiej*…

[30] A. Cywiński, *O zaufaniu – perspektywa prawna i ekonomiczna*, w: *Zaufanie w szkole w społeczeństwie sieciowym*, M. Czerepaniak-Walczak, E. Perzycka (red.), Szczecin 2013, s. 22.

[31] Tamże, s. 23.

[32] Zob. *Stanowisko Krajowej Rady Sądownictwa z dnia 15 września 2016 r. w sprawie odmowy powołania przez Prezydenta Rzeczypospolitej Polskiej kandydatów przedstawionych przez Krajową Radę Sądownictwa z wnioskiem o powołanie na stanowiska sędziowskie* [online], http://www.krs.pl/pl/aktualnosci/d,2016,9/4351,stanowisko-krajowej-rady-sadownictwa-z-dnia-15-wrzesnia-2016-r-w-sprawie-odmowy-powolania-przez-prezydenta-rzeczypospolitej-polskiej-kandydatow-przedstawionych-przez-krajowa-rade-sadownictwa-z-wnioskiem-o-powolanie-na-stanowiska-sedziowskie [dostęp: 20 IX 2016].

Przy prezentacji analiz na temat roli zaufania warto odwołać się do kolejnych fragmentów stanowiska KRS, w których m.in. stwierdzono, że brak uzasadnienia decyzji o odmowie powołania na stanowisko sędziego (…) *narusza transparentność procesu nominacyjnego* oraz (…) *może podważać zaufanie obywateli do wymiaru sprawiedliwości*[33]. Z uwzględnieniem przesłanek zawartych w art. 32 Konstytucji RP w zw. z art. 1 i art. 2 można wnioskować, że każda arbitralna i uznaniowa decyzja podejmowana przez jakikolwiek organ władzy publicznej może być postrzegana i oceniana przez pryzmat budowy zaufania do państwa, przestrzegania zasad sprawiedliwości społecznej i równego traktowania wszystkich obywateli.

Wśród głównych czynników, które w największym stopniu oddziałują na poziom zaufania obywateli do państwa, wymienia się przestrzeganie prawa i zasad etyki. Bardzo rzeczowa i logiczna argumentacja wzmacniająca słuszność tej tezy zawiera się w następującym zdaniu: (…) *spadek zaufania społecznego jest bowiem z reguły skutkiem naruszenia prawa i ignorowania wartości etycznych, takich jak uczciwość, równość i sprawiedliwość przez polityków oraz funkcjonariuszy publicznych*[34]. Wymienione trzy fundamentalne i niekwestionowane wartości etyczno-moralne, które niestety w ostatnich latach uległy znaczącej erozji, w praktyce są głównym pryzmatem oceny poczynań każdej władzy przez obywateli. Ponadto przestrzeganie określonych wzorców postępowania w codziennej rzeczywistości determinuje wykreowany wizerunek, a przede wszystkim wiarygodność władzy, w oczach opinii publicznej. Budowa zaufania do władzy jest procesem bardzo złożonym. Oczywiście ludzie kształtują swój światopogląd w głównej mierze na podstawie informacji i doniesień medialnych, które następnie są poddawane poszerzającej interpretacji przez zapraszanych do dyskusji polityków, ekspertów i publicystów. Niezależnie od wpływu tych czynników, zaufanie do władzy powstaje w umysłach ludzi na skutek zdolności autonomicznego myślenia, które w gruncie rzeczy sprowadza się do analizy porównawczej w zakresie zgodności deklarowanych postaw, wartości i norm etycznych z konkretnymi przykładami postępowania, faktów oraz zdarzeń, które występują w codziennej praktyce zarządzania[35]. Zasady bezstronności, uczciwości, równego traktowania czy zakazu dyskryminacji, popularyzowane w teoriach naukowych, pozostają w relacji dychotomicznej do rzeczywistych motywów oraz prawdziwych przesłanek dla podejmowanych decyzji zarządczych, zarówno w sprawach kadrowych, jak i w procesach dotyczących czynności prawnych wywołujących określone skutki finansowe.

W nawiązaniu do prowadzonych rozważań cenne uwagi prezentuje Robert Lizak: (…) *nieuczciwe postępowanie organów władzy publicznej i ich przedstawicieli stanowi poważne zagrożenie dla ładu instytucjonalnego państwa, obniża zdolność państwa do organizowania życia zbiorowego społeczeństwa, a wręcz niszczy państwo*[36]. Co więcej, to właśnie termin k o r u p c j a jest używany w kontekście określonych wzorców postępowania. *Korupcja jest niczym innym jak nieuczciwym zachowaniem*[37]. Zasadniczy problem polega jednak na tym, że słowo „uczciwość" w odniesieniu do konkretnych działań czy podejmowanych decyzji może być postrzegane oraz interpretowane różnie,

[33] Tamże.

[34] *Korupcja polityczna. Wskazówki dla przedstawicieli organów władzy*..., s. 14.

[35] W. Walczak, *Kontrola zakazu łączenia stanowisk w radach nadzorczych a budowanie zaufania do państwa*, „Kontrola Państwowa" 2014, nr 1, s. 69.

[36] R. Lizak, *Rola Centralnego Biura Antykorupcyjnego jako komórki compliance państwa*, „Przegląd Antykorupcyjny" 2015, nr 1, s. 44.

[37] Tamże, s. 43.

w zależności od tego, kto wyraża swoje sądy wartościujące, a także z uwagi na to, jakie przyjmuje kryterium oceny (standardy, normy zachowań). Nie ulega wątpliwości, że w praktyce zarządzania liczy się tylko taka ocena, która ma moc wiążącą. Pozostałe poglądy, stanowiska lub wyrażane opinie mogą co najwyżej być głosem w dyskusji na dany temat, który pozostaje bez znaczenia i nie ma wpływu na dalszy przebieg wydarzeń.

W literaturze przedmiotu akcentuje się, że główną potrzebą (przesłanką) uzasadniającą powołanie CBA było (…) *poczucie zagrożenia korupcją w życiu publicznym*[38]. W ocenie przedstawiciela tej instytucji do głównych zadań Biura (…) *należy sprawdzanie działań urzędniczych według spełniania kryteriów legalności i etyczności*[39]. Z takiego stwierdzenia wynika, że w ramach prowadzonych czynności kontrolnych powinny być brane pod uwagę łącznie te dwie przesłanki. Powinno się je stosować jako podstawowe kryteria oceny badanych zdarzeń, decyzji związanych z wydatkowaniem środków finansowych oraz pozostałych procesów zarządczych, szczególnie dotyczących gospodarowania powierzonym mieniem. Do prawidłowego i wnikliwego przeprowadzenia czynności sprawdzających jest jednak niezbędne znaczne poszerzenie perspektywy badawczej, co oznacza potrzebę uwzględnienia również celowości, zasadności przeznaczania określonych kwot pieniędzy na konkretne przedsięwzięcia, rzetelności prowadzonego postępowania, korzyści z zawieranych transakcji handlowych uzyskanych przez obie strony oraz rozpoznania rzeczywistych motywów przesądzających o tym, że to akurat dany podmiot uzyskał lukratywne zlecenie, umowę o współpracę itp. Ponadto prawidłowego zidentyfikowania wymaga charakter powiązań i zależności, które nakładają się na komplementarną sieć przepływów strumieni finansowych na konta wybranych beneficjentów.

Rozpoznawanie mechanizmów korupcyjnych w procesach zarządzania

B. Hołyst uważa, że (…) *wykrycie korupcji jest niezwykle trudne ze względu na ścisłe powiązania osób ją uprawiających, ich konspiracyjne metody działania oraz maskowanie technik manipulacyjnych*[40]. Dodaje przy tym, że (…) *ciemna strona tej przestępczości jest zatem na pewno bardzo duża*[41], a (…) *za sprawą wszechogarniającej korupcji straty w obrocie gospodarczym są wielokrotnie większe niż te, które powoduje przestępczość pospolita*[42]. W nawiązaniu do powyższych refleksji po pierwsze nie można się zgodzić z tym, że korupcja obejmuje swoim zakresem wyłącznie działania o charakterze stricte przestępczym, co zostało wykazane na podstawie wcześniejszych analiz. Po drugie, trzeba podzielić opinię autora na temat porażającej skali praktyk korupcyjnych, jednak z zastrzeżeniem, że ta uwaga dotyczy tzw. korupcji legalnej, która jest łatwa do zidentyfikowania. To nepotyzm i kumoterstwo są uznawane za główne przejawy korupcji, która z powodu poplecznictwa stanowi poważne zagrożenie gospodarki z racji uzyskiwania rozległych wpływów, pozycji w państwie i instytucjach publicznych[43]. Co ważne, osoby zaangażowane w ten proceder nie zostają pociągnięte do odpowiedzialności za swoje działania, gdyż są one podejmowane zgodnie z prawem – w ramach przyznanych kompetencji decyzyjnych i uprawnień.

[38] K. Dojwa, P. Turczyński, *Centralne Biuro Antykorupcyjne: od potrzeby społecznej do grupy dyspozycyjnej*, „Acta Universitatis Wratlislaviensis" 2008, nr 3079, Socjologia XLIV, s. 157.

[39] R. Lizak, *Rola Centralnego Biura Antykorupcyjnego*..., s. 41.

[40] B. Hołyst, *Korupcja jako plaga społeczna XXI wieku*…, s. 27.

[41] Tamże.

[42] Tamże, s. 28.

[43] P. Laskowski, *Korupcja władz lokalnych*, „Zeszyty Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu" 2005, nr 1, s. 71.

Maciej Ciesielski prawidłowo diagnozuje, że istota nowoczesnych form korupcji sprowadza się do (…) *relacji (powiązań), które mają przeważnie charakter nieformalny, zakulisowy, oraz ogniskują się wokół wpływu, którego efektem jest realizacja partykularnych celów (osobistych, biznesowych)*[44]. Krzysztof Nowakowski w sposób przemyślany, bardzo celnie określa te relacje mianem „klientelizmu", które nawiązuje do więzi społecznych znanych z epoki feudalnej[45]. Niestety, poglądy na temat klientelizmu jako elementu związanego ze sprawowaniem władzy nie straciły na aktualności, a wręcz przeciwnie – tożsame zjawiska powszechnie występują w czasach dzisiejszych. Podobnie jak w przeszłości, tak i obecnie można bez większego wysiłku intelektualnego rozpoznać (…) *pajęczyny oparte na układach zawodowo-towarzystkich notabli*, którzy z racji zajmowanych stanowisk i pełnionych funkcji górują nad innymi mieszkańcami, (…) *tworząc nieformalne konstelacje społeczne. Wymiana informacji zapewnia im skuteczność działania, a wzajemność świadczeń – awans społeczny i materialny*[46]. System, w którym awans jednostki zależy od protekcji możnego i wpływowego patrona, nie jest wyłącznie domeną epoki feudalnej, gdyż powyższe reguły obowiązują również w demokratycznym państwie prawa, w realiach gospodarki opartej na wiedzy. Piotr Solarz opisuje te zjawiska w następujący sposób: (…) *klientelizm polega na tym, iż partia staje się kolektywnym patronem, wokół którego powstaje sieć powiązań kolektywistycznych oparta na wykorzystaniu możliwości, jakie płyną z faktu kontroli aparatu państwowego*[47]. Są to niezwykle zasadne opinie i ze wszech miar cenne diagnozy.

W praktyce zarządzania mamy do czynienia z potężnym (…) *zjawiskiem kolonizacji machiny państwowej i* wysuwaniem (…) *na eksponowane stanowiska członków czy też zaufanych partii*[48]. Przede wszystkim chodzi o przejęcie przez wąskie grono protegowanych beneficjentów pełnej władzy i kontroli nad majątkiem i finansami, jakie są w dyspozycji organizacji zaliczanych do sektora finansów publicznych i nadzorowanych podmiotów. Należy w tym miejscu podkreślić, że skala całkowitego zawłaszczenia państwa szczególnie w ciągu ostatnich ośmiu lat jest dla wielu niezorientowanych osób wręcz niewyobrażalna. Nie wszyscy bowiem potrafią szybko oraz prawidłowo zidentyfikować charakter powiązań ludzi nominowanych do obejmowania prestiżowych stanowisk, gdyż wokół każdej partii jest także tworzona wielowymiarowa sieć kontaktów i zależności personalnych o charakterze niejawnym. W tej nieformalnej strukturze ważną rolę odgrywają osoby niekojarzone wprost z działalnością polityczną, jaką relacjonują media. Te osoby nie są członkami partii, pozostają w cieniu bieżących rozgrywek politycznych, na co dzień zajmują się prywatnym biznesem, pracują w strukturach wymiaru sprawiedliwości i prokuratury, organach kontroli, w sektorze bankowym, na wyższych uczelniach, na eksponowanych stanowiskach w administracji publicznej, w mediach, w służbach specjalnych, kierują działalnością fundacji i stowarzyszeń. Wyróżniają się tym, że po zmianie ekipy rządowej ich kontakty zostają zagospodarowane w celu ukształtowania kolejnej, nowej struktury powiązań instytucjonalno-towarzysko-

[44] M. Ciesielski, *Zjawiska korupcyjne jako podstawowa kategoria zagrożeń bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP – perspektywa Służby Kontrwywiadu Wojskowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 213.

[45] K. Nowakowski, *Klientelizm jako forma korupcji*, „Ruch Prawniczy, Ekonomiczny i Socjologiczny" 2007, nr 1, s. 213.

[46] Tamże, s. 220.

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

[48] Tamże.

-biznesowych, a także ukierunkowania przepływów finansowych między konkretnymi podmiotami dzięki podejmowaniu legalnych przedsięwzięć gospodarczych. Jest to możliwe z uwagi na posiadaną władzę i zdobyte uprawnienia decyzyjne (z racji zajmowanych stanowisk, pełnionych funkcji), które można skutecznie wykorzystać dla realizacji partykularnych interesów. W rezultacie powstają redystrybucyjne klany, których spoiwem funkcjonowania jest dążenie do maksymalizacji korzyści finansowych i osobistych dla swoich członków. Oficjalna argumentacja trafiająca do opinii publicznej będzie zawsze uzasadniała potrzebę podejmowania określonych działań w imię dobra wspólnego – dbania o interes publiczny. Nie zmienia to jednak tego, że zjawisko zawłaszczania państwa[49] traktowane jako przejaw korupcji[50] jest immanentną cechą każdej ekipy rządzącej naszym krajem. Zmieniają się ludzie u sterów władzy, ale metodyka postępowania od lat pozostaje ta sama. Jedyne różnice polegają na odmiennej percepcji i selektywnym nagłaśnianiu określonych zdarzeń przez niektóre media, co w żadnym wypadku nie może być traktowane jako usprawiedliwienie tego, że poprzednicy postępowali podobnie.

W rozszyfrowywaniu praktyk korupcyjnych powszechnie występujących w procesach zarządzania główną rolę odgrywają właściwie realizowane czynności o charakterze analityczno-informacyjnym. Rezultatem wykonywanej pracy analitycznej jest wygenerowanie wartościowej wiedzy, która powstaje dzięki prawidłowo przeprowadzonej analizie rozległej wiązki informacji mających ścisły związek z rozpatrywanym zagadnieniem. Pozyskiwane informacje, aby mogły zostać uznane za użyteczne, powinny spełniać klika podstawowych warunków. Przede wszystkim muszą być istotne z punktu widzenia realizowanych czynności sprawdzających, a także aktualne, wiarygodne i potwierdzone. Co więcej, muszą trafić do osoby, która będzie w stanie dokonać ich odpowiedniej interpretacji. Sekwencja procesów myślowych ukierunkowanych na zrozumienie zdobytych danych wymaga umiejętnego łączenia faktów w aspekcie przyczynowo-skutkowym oraz chronologicznym, zauważania koincydencji określonych zdarzeń, identyfikacji zależności, które występują między pozyskanymi informacjami, a także skoncentrowania uwagi na występujących implikacjach, następstwach. Ta najważniejsza faza działań analitycznych ma zasadnicze znaczenie dla kolejnych czynności rozpoznawczych, przesądza bowiem o charakterze poznania badanego fragmentu rzeczywistości organizacyjnej i rzutuje na kompleksowość, szczegółowość i wnikliwość prowadzonych działań.

Jak wspominano wcześniej, najłatwiejszymi do ujawnienia, powszechnie stosowanymi praktykami korupcyjnymi są nepotyzm i kumoterstwo. Ich skala jest porażająca, ponieważ nikt spoza układu, kto nie ma koneksji i poparcia wpływowego patrona, nie ma nawet najmniejszej szansy na objęcie intratnego (eksponowanego) stanowiska. To również dotyczy szeregowych pracowników zatrudnianych w instytucjach publicznych. System działa w sposób bezwzględny, co oznacza, że praca i kariera są zarezerwowane tylko „dla swoich" – dla pozostałych osób stanowiska są niedostępne. Tam, gdzie przepisy prawa wymagają podawania do publicznej wiadomości informacji na temat tzw. postępowań otwartych i konkurencyjnych, każde ujawniane ogłoszenie stanowi jedynie legitymizację uprzednio poczynionych nieformalnych ustaleń, kto ma otrzymać daną posadę. To oznacza, że wszystko jest z góry przesądzone i odbywa się według

[49] Ł. Afeltowicz, *Zawłaszczone państwa, sieci społeczne i wyobraźnia socjologiczna: krytyczna analiza koncepcji state capture*, „Studia Socjologiczne" 2010, nr 1, s. 69–105.

[50] W. Jasiński, *Rządowy program przeciwdziałania korupcji – kształtowanie polityki antykorupcyjnej w latach 2014–2019*, „Kontrola Państwowa" 2014, nr 5, s. 99.

misternie wyreżyserowanego scenariusza wydarzeń, począwszy od określenia wymagań formalnych zawartych w ogłoszeniu, przez dobór składu komisji konkursowej, a na wytycznych, kto ma wygrać konkurs, kończąc. Innymi słowy, potencjalny kandydat bez protekcji i rekomendacji nie ma najmniejszych szans na skuteczne konkurowanie, gdyż wszystko zostało już wcześniej rozstrzygnięte. Oczywiście mogą się zdarzyć incydentalne przypadki (kiedy przygotowana „ustawka" nie powiedzie się za pierwszym razem), które pozna opinia publiczna, jak chociażby sprawa zaangażowania aktualnie urzędującego prezesa Najwyższej Izby Kontroli w kontekście przeprowadzanych konkursów na stanowiska dyrektorów delegatur NIK.

Niestety, opisywana metodyka postępowania nie kończy się na sprawach kadrowych, lecz ma swoje rozwinięcie i kontynuację w innych procesach zarządczych. Mechanizmy korupcyjne powszechnie występują (co absolutnie nie oznacza, że są najczęściej ujawniane), zwłaszcza w sytuacjach dotyczących:

- celowego ustawiania (profilowania) wymagań formalnych zawartych w Specyfikacji Istotnych Warunków Zamówienia (SIWZ) dla prowadzonych postępowań przetargowych pod konkretnego protegowanego beneficjenta – świadome, zamierzone stawianie w uprzywilejowanej pozycji określonego podmiotu i skuteczne zablokowanie, wyeliminowanie potencjalnej konkurencji z możliwości ubiegania się o zamówienie,
- podejmowania wysoce stronniczych, arbitralnych i uznaniowych decyzji, w wyniku czego faworyzowane osoby lub podmioty (firmy prywatne, a także organizacje pozarządowe) otrzymują wiele intratnych zleceń, a także podpisuje się odpowiednie kontrakty, umowy o współpracy i dokonuje się zakupów określonych towarów i usług.

Identyfikacja korupcji we wspomnianych procesach zarządczych wymaga żmudnych i szczegółowych prac analitycznych, które swoim zakresem muszą obejmować samą rozpracowywaną organizację, charakter jej relacji z innymi podmiotami oraz osobami pełniącymi ważne funkcje publiczne, a także ocenę istotnych zdarzeń z przeszłości, które pomagają we właściwy sposób zrozumieć teraźniejszość.

Przy badaniu postępowań przetargowych prowadzonych przez daną jednostkę organizacyjną należy zwrócić szczególną uwagę na wcześniejsze rozstrzygnięcia. W tym celu warto znaleźć odpowiedzi na następujące pytania: Kto zarządzał instytucją w danym okresie? Z kim był powiązany? Dzięki komu uzyskał stanowisko? Jakie firmy wygrywały przetargi? Kto przygotowywał warunki SIWZ? Kto zasiadał w komisji przetargowej? Jakie były podpisywane aneksy do zawartych umów i na jaką kwotę? Kto przygotowywał i akceptował owe dokumenty? Takie kompleksowe i szczegółowe podejście jest bezwarunkowo konieczne, jeśli ktoś chce naprawdę dogłębnie poznać, a przede wszystkim zrozumieć, rzeczywiste motywy i mechanizmy podejmowanych działań. W przeciwnym wypadku można mówić co najwyżej o powierzchownych działaniach sprawdzających przeprowadzonych w celach statystycznych. Analiza samych oświadczeń majątkowych jest niewystarczająca, gdyż trzeba zidentyfikować również aktywność biznesową grona najbliższej rodziny i znajomych (tj. sieć kontaktów) w celu ustalenia przedsięwzięć, w które angażowali się w przeszłości, i którymi zajmują się obecnie. Bardzo pomocne w tych dociekaniach są nie tylko powszechnie dostępne bazy danych Krajowego Rejestru Sądowego[51] lub Centralnej Ewidencji i Informacji o Dzia-

[51] Zob. https://ems.ms.gov.pl/krs/wyszukiwaniepodmiotu.

łalności Gospodarczej[52], lecz także aplikacje, które umożliwiają szybkie wykrycie wcześniejszych i aktualnych powiązań, np. KtoKogo.pl[53] lub portal prześwietl.pl[54]. Komplementarne czynności muszą dotyczyć sprawdzenia operatywności określonych osób w sferze politycznej, a także ich kontaktów – zażyłych znajomości z wysoko postawionymi przedstawicielami władzy, zajmujących w przeszłości lub aktualnie ważne stanowiska, na których przysługują rozległe uprawnienia decyzyjne. Równoległe rozpoznawanie tych dwóch obszarów aktywności jest w pełni uzasadnione i logiczne.

Wykonywanie pracy analitycznej w głównej mierze sprowadza się do stawiania właściwych pytań i myślenia lateralnego w poszukiwaniu adekwatnych odpowiedzi. Myślenie lateralne wymusza potrzebę holistycznego postrzegania badanego zjawiska, a także wymaga zdolności patrzenia na rozpatrywaną sprawę z wielu perspektyw i dostrzegania tego, co jest ważne. Podczas analizy podmiotu, który uzyskał lukratywne zamówienie (np. wielomilionowy kontrakt) w kręgu zainteresowań powinny znajdować się następujące informacje: W którym roku i przez kogo podmiot został utworzony? Gdzie jest jego główna siedziba i miejsce prowadzenia działalności? Jaka jest struktura właścicielska i zaangażowanie kapitałowe? Czy podmiot posiada inne spółki zależne? Kto wcześniej zasiadał, a kto obecnie zasiada we władzach podmiotu? W jaki sposób zostały dobrane osoby, którym przyznano uprawnienia decyzyjne w zakresie zarządzania bieżącą działalnością? Kto miał bezpośredni wpływ na te procesy kadrowe? Kto stanowi najważniejszą grupę klientów danego podmiotu? Jakie biznesowe aktywności stanowią główne źródła przychodów? Kto jest kooperantem (partnerem) danego podmiotu? Jaka jest grupa podwykonawców? Jakie relacje i powiązania występują między władzami danego podmiotu a jego najważniejszymi klientami? W jakie przedsięwzięcia biznesowe finansowane ze środków publicznych podmiot był uprzednio zaangażowany (jaki ośrodek władzy publicznej przekazywał środki finansowe, czyja decyzja o tym przesądziła, na jaką kwotę opiewała wartość wykonanych czy też zleconych prac, usług lub zakupów)? W jakich projektach współfinansowanych ze środków UE badany podmiot uczestniczył (wartość projektu, jaka instytucja publiczna przekazywała środki finansowe, kto dokonywał oceny składanego wniosku, kto podpisywał umowę o dofinansowanie)? Jakie organizacje z sektora pozarządowego otrzymywały wsparcie (w jakiej wysokości) od badanego podmiotu? Kto był beneficjentem sponsoringu? Warto również rozpoznać i sprawdzić kumulowanie stanowisk (łączenie funkcji) przez osoby zasiadające aktualnie i w przeszłości we władzach danego podmiotu, a także ich najbliższych współpracowników, z uwzględnieniem wcześniejszej aktywności m.in. w strukturach administracji państwowej i w prywatnym biznesie. Wówczas zyskamy pełniejszy, bardziej klarowny obraz badanej rzeczywistości społeczno-gospodarczej.

Do newralgicznych obszarów, w których znajdują odzwierciedlenie praktyki korupcyjne w procesach zarządczych, najczęściej zaliczają się uznaniowe decyzje dotyczące zakupu określonych towarów i sprzętu (np. sprawy związane z informatyzacją), umowy cywilno-prawne z podmiotami zewnętrznymi obejmujące swoim zakresem usługi doradcze, szkoleniowe, doradztwo prawne, doradztwo biznesowe, marketing i reklama, public relation, sponsoring, ubezpieczenia majątkowe itp. Przy badaniu treści i zakresu prac objętych tymi umowami koniecznie trzeba dokonać wnikliwej i wszechstronnej analizy umożliwiającej uzyskanie odpowiedzi na pytanie: Jakie rzeczywiste czynniki

[52] Zob. https://prod.ceidg.gov.pl/ceidg/ceidg.public.ui/search.aspx.
[53] Zob. http://www.kto-kogo.pl/.
[54] Zob. https://przeswietl.pl/.

przesądziły o wyborze danego, konkretnego podmiotu, zasadności i cenie realizowanych prac? Należy także poddać drobiazgowej kontroli dokumentację wykonawczą i rozliczeniową. W przypadku umów dotyczących usług o charakterze niematerialnym stanowią one najwygodniejszą formę tzw. legitymizacji prawnej wyprowadzania środków finansowych danego pomiotu, gdyż w niektórych przypadkach trudno jednoznacznie wykazać, że wartość zawieranych umów jest celowo zawyżona, przez co mogło dojść do niekorzystnego rozporządzania powierzonym mieniem bądź działania na szkodę danego podmiotu. Dlatego przy badaniu umów dotyczących usług niematerialnych warto zwrócić uwagę na zasadność zlecania określonych prac firmom zewnętrznym, jeśli charakter tych prac pokrywa się z zakresem obowiązków i zadań realizowanych przez macierzyste komórki organizacyjne danego podmiotu. Należy także skoncentrować się na porównaniu wymiernych rezultatów, które są pochodną zawieranych umów (korzyści uzyskane przez dany podmiot) z wymiernymi korzyściami finansowymi, jakie czerpały osoby (firmy) zewnętrzne wykonujące otrzymane zlecenia. Taka komparatywna analiza jest bardzo pożądana, jeśli chcemy dokonać bezstronnej i obiektywnej oceny zleceń z punktu widzenia zasadności zawierania określonych umów, tj. z uwzględnieniem przesłanek celowości, rzetelności i gospodarności. Nie liczy się to, co zostało zapisane w umowie, lecz konkretne, wymierne rezultaty, które mają swoje potwierdzenie w rzeczywistości. Tłumaczenie, że cena była wysoka, gdyż firma poniosła wysiłek na rzecz realizowanego zlecenia, jest całkowicie niewystarczające. Znaczenie mają faktycznie wykonane działania, a nie te zadeklarowane w umowie. Ponadto trzeba ustalić, kto bezpośrednio był odpowiedzialny w firmie za rozliczenie zleconych prac (które dokumenty potwierdzają ich należyte wykonanie), a także kto przygotowywał i podpisywał stosowne dokumenty księgowe, na których podstawie dokonano zapłaty.

Przy uwzględnieniu tego, że decyzja o wyborze konkretnych zleceniobiorców mogła mieć charakter uznaniowy i wysoce stronniczy należy porównać ceny świadczonych usług, które obowiązują na rynku, chociażby przeglądając oferty innych firm dostępne w Internecie. Jeśli wartość, na jaką opiewa zawarta umowa, w rażący sposób odbiega od stawek przyjętych przez konkurentów, to istnieje uzasadnione podejrzenie, że mamy do czynienia z niegospodarnością i brakiem zachowania należytej staranności w procesach zarządzania powierzonym mieniem. W takiej sytuacji można dodatkowo zwrócić się z konkretnym zapytaniem ofertowym (zawierającym tożsamy zakres prac i zadań do realizacji, jakie zostały zawarte w danej umowie) do kilkudziesięciu wybranych podmiotów funkcjonujących na rynku, aby przekonać się, czy wyeliminowanie potencjalnej konkurencji i arbitralny wybór faworyzowanego podmiotu można faktycznie uznać za świadomą niegospodarność – celowe nadużycie władzy dla zapewnienia prywatnych korzyści osobie trzeciej traktowanej w uprzywilejowany sposób – co de facto jest ewidentnym przejawem korupcji. Każdy zleceniodawca, podejmując uznaniową decyzję o przekazaniu środków finansowych w ramach zlecenia dla firmy zewnętrznej, musi godzić się z tym, że oznacza to nie tylko nierówne traktowanie, lecz także skuteczne wyeliminowanie innych podmiotów na rzecz faworyzowanego beneficjenta.

Z punktu widzenia obowiązującego prawa owe czyny będą różnie interpretowane w zależności od tego, kto jest decydentem. Inną odpowiedzialność będzie po-

nosić osoba o statusie funkcjonariusza publicznego[55], a zupełnie inną menedżerowie[56] np. spółek kapitałowych prawa handlowego z udziałem państwowych osób prawnych. W prywatnym biznesie omawiane praktyki w ogóle nie będą postrzegane w kategorii korupcji, ponieważ prawne tłumaczenie będzie odwoływało się do swobody prowadzenia działalności gospodarczej i możliwości podejmowania dowolnych decyzji finansowych bez potrzeby ich jakiegokolwiek uzasadniania.

Aby wyjaśnić celowość zawierania umów o zawyżonych kosztach, warto zwrócić uwagę na charakter zaufania, jaki łączy decydenta (patrona) z klientem (wykonawcą usługi). Ich ustalenia poczynione na temat kwoty nadwyżki możliwej do podziału i wspólnie uzgodnionej nie są dokonywane w formie pisemnej pod rygorem nieważności, jako swoisty załącznik do umowy, lecz są omawiane w formie ustnej jako ściśle strzeżona tajemnica obu stron. Decydent, dając zlecenie na zawyżoną kwotę, nie czyni tego bezinteresownie – wie, że może liczyć na „niewymuszone, dobrowolne odwzajemnienie" ze strony klienta. Aby uniknąć podejrzenia o przekazywanie nienależnych korzyści majątkowych, wystarczy, że sam klient lub zaufany pośrednik zawrze umowę np. na doradztwo w formie ustnej z innym prywatnym podmiotem wskazanym przez decydenta bądź da zlecenie na określone prace albo zapewni miejsce w radzie nadzorczej bądź inne stanowisko osobie poleconej, i w ten sposób skutecznie odwdzięczy się za przychylność (przysługę). Może również wpłacić określoną kwotę przewidzianą przepisami prawa na konto wskazanej partii albo w przyszłości wesprzeć fundusz wyborczy decydenta. Klient może również stać się mecenasem wskazanej fundacji, w której jest zatrudniona osoba powiązana z decydentem itp. Aktualnie to właśnie m.in. takie nowoczesne formy (oparte na złożonych powiązaniach personalnych) przybierają mechanizmy korupcyjne powszechnie występujące w praktyce zarządzania. Oficjalne statystyki dotyczące przestępczości korupcyjnej prezentowane w cyklicznych publikacjach CBA pt. „Mapa Korupcji" odnośnie do wykrytych spraw, (…) *w najlepszym przypadku, stanowią one przede wszystkim informację o efektywności działania organów państwa odpowiedzialnych za zwalczanie korupcji, a nie ilustrację skali występowania tego zjawiska w Polsce*[57].

Podsumowanie

Waldemar Kryspin Jaruszewski słusznie uważa, że (…) *kumulacja korupcji jest zjawiskiem wysoce niebezpiecznym dla rozwoju społeczno-gospodarczego państwa*, a jej powszechne występowanie prowadzi w rezultacie do (…) *zwiększającej się liczby nieformalnych sieci społecznych działających na podstawie reguł pokrewieństwa i norm wzajemności, które stanowią bazę układów klientelistycznych*[58]. Są to cenne przemyślenia i uwagi, które niezwykle trafnie odzwierciedlają współczesne realia społeczno-gospodarcze w Polsce. Trzeba jednak dodać, że zawężanie zjawiska korupcji wyłącznie do czynów przestępczych jest całkowicie niezasadne.

[55] W. Walczak, *Odpowiedzialność funkcjonariusza publicznego za podejmowane decyzje zarządcze będące nadużyciem władzy*, „Wiedza Prawnicza" 2013, nr 6, s. 72–92.

[56] W. Walczak, *Odpowiedzialność menedżerów z tytułu zajmowania się sprawami majątkowymi podmiotów gospodarczych*, „Wiedza Prawnicza" 2014, nr 1, s. 76–96.

[57] P. Koryś, C. Trutkowski, *Nie jest tak dobrze czy nie jest tak źle? Zmiany poziomu percepcji korupcji w Polsce w świetle badań społecznych*, „Zarządzanie Publiczne" 2014, nr 2, s. 68.

[58] W.K. Jaruszewski, *Wpływ kapitału intelektualnego i korupcji na stan bezpieczeństwa*, „Studia Gdańskie. Wizje i rzeczywistość" 2015, t. 12, s. 327–328.

Działania analityczno-informacyjne koncentrują się przede wszystkim na prognozowaniu, poprawnej analizie i właściwie przeprowadzonej identyfikacji najważniejszych zagrożeń korupcyjnych godzących w interesy ekonomiczne państwa, a także formułowaniu wyprzedzających informacji o nieprawidłowościach. Powszechną akceptację zyskują poglądy, że bezpieczeństwo państwa należy postrzegać w dwóch zasadniczych wymiarach – w pierwszym, tradycyjnym ujęciu kojarzy się ono z aspektem militarnym, rozumianym jako zapewnienie ochrony suwerennego państwa przed zagrożeniami zewnętrznymi, w drugim zaś odnosi się do zagadnień społecznych i ekonomicznych[59]. Aktualnie podkreśla się, że to właśnie bezpieczeństwo ekonomiczne jest najważniejsze, ponieważ (…) *stanowi płaszczyznę rywalizacji i konkurencji między krajami*, a ponadto umożliwia (…) *niezakłócone i prawidłowe funkcjonowanie gospodarek narodowych*[60]. Należy zgodzić się z opinią naczelnego organu kontroli państwowej, że czynniki takie jak: (…) *dowolność i uznaniowość w podejmowaniu decyzji, nadmierne korzystanie z usług zewnętrznych i pośrednictwa, słabość nadzoru i kontroli wewnętrznej, konflikt interesów, lekceważenie dokumentacji i sprawozdawczości* są zaliczane do (...) *podstawowych mechanizmów korupcjogennych*[61]. Problem polega jednak na tym, że nie wystarczy podać do publicznej wiadomości czynników, które sprzyjają korupcji, lecz przede wszystkim należy skutecznie zwalczać i eliminować korupcyjne patologie z codziennej praktyki zarządzania.

Robert Grochowski uważa, że (…) *działalność służb specjalnych jest elementem tworzenia zaufania społecznego i politycznego między władzami politycznymi a obywatelami*[62]. Z badania przeprowadzonego przez CBOS w 2015 r. wynika, że 35 proc. ankietowanych pozytywnie ocenia działalność CBA. Można to oczywiście zinterpretować tak, że ponad jedna trzecia respondentów wyraża korzystną (pochlebną) opinię[63], albo nieco inaczej: 75 proc. udzielonych odpowiedzi nie potwierdza pozytywnej oceny działalności urzędu do spraw walki z korupcją[64]. Wydaje się, że jeden z ważniejszych elementów rzutujących na poziom zaufania ma związek z tym, że o wielu bulwersujących nieprawidłowościach opinia publiczna najpierw dowiaduje się z mediów, które ujawniają patologie korupcyjne, a dopiero wielokrotne nagłośnienie sprawy skutkuje zainteresowaniem ze strony CBA. Radosław Bochan zaznacza, że m.in. (…) *tworzenie dokumentacji przetargowej, której wymagania spełnia jedna firma, czy „poprawianie" ofert po otwarciu przetargu jest podstawą do zainteresowania się sprawą przez wyspecjalizowane w tym zakresie służby*[65]. Podobnie powinno być m.in. w odniesieniu do procesów związanych

[59] J. Bil, *Wpływ zachowań korupcyjnych na bezpieczeństwo Polski*, „Przegląd Strategiczny" 2013, nr 1, s. 217.

[60] G. Waszkiewicz, *Ryzyko polityczne wskaźnikiem bezpieczeństwa narodowego państwa*, „Studia Bezpieczeństwa Narodowego" 2015, nr 8, s. 190–191.

[61] Z. Dobrowolski, *Przeciwdziałanie patologiom organizacyjnym. Rola naczelnego organu kontroli państwowej w zwalczaniu korupcji*, „Przedsiębiorczość i Zarządzanie" 2014, t. 15, z. 5, cz. II, s. 120.

[62] R. Grochowski, *Rola służb specjalnych w demokratycznym państwie prawa*, „Środkowoeuropejskie Studia Polityczne" 2013, nr 4, s. 196.

[63] Zob. Informator Centralnego Biura Antykorupcyjnego, Warszawa 2015, s. 3.

[64] Ustawodawca, określając zasadność i sens powołania CBA, uznał, że jest to (…) *służba specjalna do spraw zwalczania korupcji w życiu publicznym i gospodarczym, w szczególności w instytucjach państwowych i samorządowych, a także do zwalczania działalności godzącej w interesy ekonomiczne państwa* (art. 1 ust. 1). Definicje prawne czynów, które w rozumieniu ustawy są korupcją, zostały natomiast wyszczególnione w art. 1 ust. 3a. CBA zajmuje się zwalczaniem praktyk korupcyjnych w życiu publicznym i gospodarczym, które wskazuje ustawodawca, mając na uwadze szeroki zakres realizowanych zadań wymienionych w art. 2 ustawy. Zob. *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U. z 2006 r. Nr 104 poz. 708, ze zm.).

[65] R. Bochan, *Ekonomiczno-społeczna analiza przyczyn i skutków występowania mechanizmów korupcyj-*

z przyznawaniem korzystnych wielomilionowych kontraktów oraz uprzywilejowanym traktowaniem wybranych podmiotów gospodarczych czy też konfliktem interesów.

Druga kwestia może dotyczyć przesłanek, na które zwraca uwagę Paweł Pochodyła. Chodzi mianowicie o postrzeganie roli CBA w kontekście założeń programowych, jakie legły u podstaw powołania urzędu do zwalczania korupcji: pilnowanie zaprowadzonego wcześniej „porządku" i w razie potrzeby interweniowanie, gdyby „układ" zaczął się odradzać – innymi słowy, (…) *aby w miejsce „starych układów" nie powstawały nowe*[66]. W praktyce zarządzania występują ponadto inne patologie, które mogą stanowić dopełnienie opisywanych praktyk korupcyjnych, m.in.: wystawianie fikcyjnych faktur, oszustwa podatkowe (np. wyłudzenia podatku VAT), a także poświadczanie nieprawdy w dokumentach.

Bibliografia:

1. Afeltowicz Ł., *Zawłaszczone państwa, sieci społeczne i wyobraźnia socjologiczna: krytyczna analiza koncepcji state capture*, „Studia Socjologiczne" 2010, nr 1, s. 69–105.
2. Bil J., *Wpływ zachowań korupcyjnych na bezpieczeństwo Polski*, „Przegląd Strategiczny" 2013, nr 1, s. 217–227.
3. Bochan R., *Ekonomiczno-społeczna analiza przyczyn i skutków występowania mechanizmów korupcyjnych w gospodarce*, „Studia Ekonomiczne Regionu Łódzkiego" 2013, nr 9, s. 105–128.
4. Brol M., *Ekonomiczne, instytucjonalne i kulturowe uwarunkowania korupcji*, Monografie i Opracowania nr 257, Wrocław 2015, Wydawnictwo Uniwersytetu Ekonomicznego we Wrocławiu.
5. Ciesielski M., *Zjawiska korupcyjne jako podstawowa kategoria zagrożeń bezpieczeństwa i zdolności bojowej Sił Zbrojnych RP – perspektywa Służby Kontrwywiadu Wojskowego*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 209–218.
6. Cywiński A., *O zaufaniu – perspektywa prawna i ekonomiczna*, w: *Zaufanie w szkole w społeczeństwie sieciowym*, M. Czerepaniak-Walczak, E. Perzycka (red.), Szczecin 2013, Zapol Dmochowski, Sobczyk Sp.j., s. 21–28.
7. Dobrowolski Z., *Przeciwdziałanie patologiom organizacyjnym. Rola naczelnego organu kontroli państwowej w zwalczaniu korupcji*, „Przedsiębiorczość i Zarządzanie" 2014, t. 15, z. 5, cz. II, s. 113–127.
8. Dojwa K., Turczyński P., *Centralne Biuro Antykorupcyjne: od potrzeby społecznej do grupy dyspozycyjnej*, „Acta Universitatis Wratlislaviensis" 2008, nr 3079, Socjologia XLIV, s. 157–175.
9. Dyoniziak R., *Korupcja jako wyzwanie dla demokracji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2008, nr 763, s. 5–11.
10. Falenta P., *Przestępstwo korupcji – uwarunkowania karnoprawne i społeczne*, „Prace Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu" 2016, nr 1, s. 147–163.
11. Filek J., *Polski trójkąt korupcyjny*, „Annales: etyka w życiu gospodarczym" 2006, tom 9, nr 1, s. 157–171.

nych w gospodarce, „Studia Ekonomiczne Regionu Łódzkiego" 2013, nr 9, s. 109.

[66] P. Pochodyła, *Pozycja ustrojowa Centralnego Biura Antykorupcyjnego w systemie organów państwowych*, „Zeszyty Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie" 2011, nr 1, s. 221.

12. Fleszer D., *Z problematyki korupcji w administracji publicznej*, w: *Jak możliwy jest dialog*?, A. Kamińska, E. Kraus, K. Ślęczka (red.), Sosnowiec 2014, Oficyna Wydawnicza Humanistas, s. 285–296.
13. Grochowski R., *Rola służb specjalnych w demokratycznym państwie prawa*, „Środkowoeuropejskie Studia Polityczne" 2013, nr 4, s. 195–207.
14. Hołyst B., *Korupcja jako plaga społeczna XXI wieku*, „Przegląd Antykorupcyjny" 2011, nr 1, s. 24–41.
15. Informator Centralnego Biura Antykorupcyjnego, Warszawa 2015.
16. Jaruszewski W.K., *Wpływ kapitału intelektualnego i korupcji na stan bezpieczeństwa*, „Studia Gdańskie. Wizje i rzeczywistość" 2015, t. 12, s. 305–330.
17. Jasiński W., *Rządowy Program Przeciwdziałania Korupcji – kształtowanie polityki antykorupcyjnej w latach 2014–2019*, „Kontrola Państwowa" 2014, nr 5, s. 95–113.
18. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. z 1997 r. Nr 78 poz. 483, ze zm.).
19. *Korupcja polityczna. Wskazówki dla przedstawicieli organów władzy wybieranych w wyborach powszechnych*, Warszawa 2016, Centralne Biuro Antykorupcyjne.
20. Koryś P., Trutkowski C., *Nie jest tak dobrze czy nie jest tak źle? Zmiany poziomu percepcji korupcji w Polsce w świetle badań społecznych*, „Zarządzanie Publiczne" 2014, nr 2, s. 63–83.
21. Laskowski P., *Korupcja władz lokalnych*, „Zeszyty Naukowe Wyższej Szkoły Zarządzania i Przedsiębiorczości w Wałbrzychu" 2005, nr 1, s. 70–77.
22. Lizak R., *Rola Centralnego Biura Antykorupcyjnego jako komórki compliance państwa*, „Przegląd Antykorupcyjny" 2015, nr 1, s. 39–46.
23. Matejuk J., *Korupcja – istota, źródła, zakres i zagrożenia*, „Przegląd Organizacji" 2004, nr 5, s. 7–10.
24. Nowakowski K., *Nowe zjawisko korupcji komercyjnej*, „Współczesna Ekonomia" 2010, nr 2, s. 111–128.
25. Pochodyła P., *Pozycja ustrojowa Centralnego Biura Antykorupcyjnego w systemie organów państwowych*, „Zeszyty Naukowe Wyższej Szkoły Ekonomii i Innowacji w Lublinie" 2011, nr 1, s. 221–240.
26. *Poradnik antykorupcyjny dla przedsiębiorców. Przedsiębiorca w środowisku zagrożeń korupcyjnych*, Warszawa 2011, Centralne Biuro Antykorupcyjne.
27. Robak A., Czaja M., *Korupcja – zarys istoty zjawiska*, w: *Postawy wobec korupcji w samorządzie terytorialnym. Raport z badań w województwie śląskim*, A. Turska-Kawa, M. Czaja (red.), Katowice 2015, Fundacja Akademicka IPSO ORDO, s. 9–18.
28. Solarz P., *Ekonomiczne i kulturowo-polityczne przyczyny korupcji w Polsce po akcesji do Unii Europejskiej*, „Kwartalnik Naukowy Uczelni Vistula" 2013, nr 4, s. 5–14.
29. *Stanowisko Krajowej Rady Sądownictwa z dnia 15 września 2016 r. w sprawie odmowy powołania przez Prezydenta Rzeczypospolitej Polskiej kandydatów przedstawionych przez Krajową Radę Sądownictwa z wnioskiem o powołanie na stanowiska sędziowskie.*
30. Szyc R., *Miejsce organów kontroli w walce z korupcją – identyfikacja i eliminacja mechanizmów korupcjogennych*, „Kontrola Państwowa" 2015, nr 6, s. 37–53.
31. Turska-Kawa A., *Psychologiczne determinanty korupcji politycznej*, w: *Postawy wobec korupcji w samorządzie terytorialnym. Raport z badań w województwie śląskim*, A. Turska-Kawa, M. Czaja (red.), Fundacja Akademicka IPSO ORDO, Katowice 2015, s. 31–46.

32. *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U. z 2006 r. Nr 104 poz. 708, ze zm.).
33. Walczak W., *Kontrola zakazu łączenia stanowisk w radach nadzorczych a budowanie zaufania do państwa*, „Kontrola Państwowa" 2014, nr 1, s. 66–83.
34. Walczak W., *Odpowiedzialność funkcjonariusza publicznego za podejmowane decyzje zarządcze będące nadużyciem władzy*, „Wiedza Prawnicza" 2013, nr 6, s. 72–92.
35. Walczak W., *Odpowiedzialność menedżerów z tytułu zajmowania się sprawami majątkowymi podmiotów gospodarczych*, „Wiedza Prawnicza" 2014, nr 1, s. 76–96.
36. Waszkiewicz G., *Ryzyko polityczne wskaźnikiem bezpieczeństwa narodowego państwa*, „Studia Bezpieczeństwa Narodowego" 2015, nr 8, s. 189–202.
37. Wiatrowski P., *Prawne, ekonomiczne i socjologiczne aspekty korupcji*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2008, nr 776, s. 97–111.
38. Wiatrowski P., *Korupcja i jej zapobieganie. Wręczenie kontrolne czy kontrolowane (uwagi de lege ferenda)*, „Zeszyty Naukowe Uniwersytetu Ekonomicznego w Krakowie" 2005, nr 690, s. 95–112.

Abstrakt

W artykule przestawiono kompleksowe rozważania i analizy przybliżające do lepszego poznania i zrozumienia mechanizmów korupcyjnych, jakie powszechnie występują w procesach zarządzania. Na wstępie scharakteryzowano różne ujęcia definicyjne omawianego zjawiska, akcentując jednocześnie, że wzorce zachowań określane mianem k o r u p c j a nie zawężają się wyłącznie do czynów zabronionych przez prawo. W dalszej części pracy zwrócono uwagę na postrzeganie omawianych problemów z perspektywy podważania zaufania do państwa i jego organów. Podkreślono przy tym, że każda arbitralna i uznaniowa decyzja podejmowana przez organy władzy publicznej może być oceniana z punktu widzenia przestrzegania zasad sprawiedliwości społecznej i równego traktowania. Następnie wnikliwie omówiono cele i znaczenie realizowanych czynności o charakterze analityczno-informacyjnym, które służą rozpoznawaniu praktyk korupcyjnych. Dodatkowo zaprezentowano metodykę postępowania, która umożliwia wszechstronne zdiagnozowanie oraz właściwe zrozumienie istoty, a także złożoności badanych zdarzeń i procesów.

Słowa kluczowe: korupcja, działania analityczno-informacyjne, Centralne Biuro Antykorupcyjne, zaufanie publiczne, bezpieczeństwo ekonomiczne państwa.

Abstract

The article presents comprehensive deliberations and analyses bringing closer view to better cognition and understanding of the corruption mechanisms which constitute general practices appearing in management processes. Firstly, different definitional approaches to the discussed phenomenon are characterized, stressing simultaneously that patterns of behaviours described as c o r r u p t i o n are not narrowing exclusively to actions forbidden by the law. Hereinafter the attention is paid to perceiving analyzed

problems from the perspective of undermining trust to the state and its organs. It was emphasized that each arbitrary and discretionary decision made by public authorities could be assessed from the point of view respecting adherence to the principles of the social justice and the fair treatment. Next, the aims and significance of carried out analytical-information activities which are devoted to recognizing and identifying corruption practice are thoroughly discussed which are devoted to recognizing and identifying corruption practice. Finally, the article presents methods of proceedings which enable versatile diagnosis and appropriate understanding the essence as well as the complexities of examined phenomena and processes.

Keywords: corruption, analytical-information activities, Central Anticorruption Bureau, public trust, economic security of the state.

Tomasz Safjański

Zintegrowane zwalczanie przestępczości zorganizowanej w regionie Morza Bałtyckiego (BALTCOM) – geneza, główne aspekty działania oraz perspektywy rozwoju

Podejście państw nadbałtyckich do problemu walki z przestępczością jest wypadkową współpracy politycznej w regionie. Zasadnicze decyzje dotyczące form, okresu i kierunków regionalnej polityki zwalczania przestępczości transgranicznej są podejmowane podczas cyklicznych spotkań Rady Państw Morza Bałtyckiego (dalej RPMB), w której zasiadają szefowie rządów państw nadbałtyckich. Pierwsze ze spotkań Rady odbyło się 3–4 maja 1996 r. w Visby (Szwecja), drugie 22–23 stycznia 1998 r. w Rydze, trzecie 12–13 kwietnia 2000 r. w Kolding (Dania), a czwarte 10 czerwca 2002 r. w Sankt Petersburgu. Aktualnie spotkania premierów RPMB odbywają się co dwa lata, przemiennie z sesjami ministrów spraw zagranicznych, i kończą okres prezydencji danego państwa nadbałtyckiego. W spotkaniach RMPB biorą udział przedstawiciele prezydencji Rady Unii Europejskiej oraz Komisji Europejskiej.

Początek współpracy w zakresie przeciwdziałania przestępczości w regionie dało ustanowienie w 1993 r. Konferencji Morza Bałtyckiego ds. Zwalczania Przestępczości Międzynarodowej (The Baltic Sea Conference on Combating International Crime), w której ramach odbywały się coroczne spotkania na szczeblu politycznym. Podczas tych spotkań w ramach grup roboczych przygotowywano propozycje wspólnych działań oraz opracowywano potrzebne materiały. Ze względu na brak bezpośredniej współpracy operacyjnej organów ścigania kooperacja oparta na formule konferencji nie miała istotnego znaczenia w zwalczaniu przestępczości międzynarodowej, a jedynie wymiar symboliczny[1].

W maju 1996 r. na szczycie RPMB w Visby uzgodniono powołanie specjalnej grupy międzyrządowej mającej na celu wypracowanie rozwiązań umożliwiających zespołowe prowadzenie bezpośrednich działań operacyjnych. Pierwsze spotkanie przedstawicieli szefów rządów odbyło się 16 czerwca 1996 r. w Sztokholmie. Zainicjowano na nim działalność Grupy Zadaniowej ds. Zwalczania Przestępczości Zorganizowanej w Regionie Morza Bałtyckiego (The Task Force on Organised Crime in the Baltic Sea Region, dalej: Grupa Zadaniowa). Do Grupy, o której mowa, należy 11 państw basenu Morza Bałtyckiego: Niemcy, Norwegia, Islandia, Szwecja, Finlandia, Rosja, Dania, Polska, Litwa, Estonia i Łotwa. Wymienione państwa są reprezentowane przez przedstawicieli szefów rządów. Status obserwatora w Grupie otrzymały Komisja Europejska, Europol, Frontex, Interpol i Światowa Organizacja Celna.

W 1998 r. na kolejnym szczycie RPMB w Rydze postanowiono o utworzeniu w ramach Grupy Zadaniowej Komitetu Operacyjnego (The Operative Committee).

Główne cele zintegrowanego zwalczania przestępczości w regionie Morza Bałtyckiego obejmują:

1) usprawnianie i zacieśnianie współpracy między krajowymi organami ścigania państw regionu, w tym między: siłami policyjnymi, służbami celnymi, formacjami ochrony granic oraz służbami migracyjnymi,

[1] *Searching and finding solutions – a booklet about the Task-Force on Organized Crime in the Baltic Sea Region*, Sztokholm 2000, s. 4.

2) skoncentrowanie działań na zwalczaniu wybranych form przestępczości zorganizowanej, m.in.: produkcji i obrotu narkotykami, nielegalnej migracji, handlu ludźmi, przemytu towarów, obrotu skradzionymi pojazdami, handlu bronią i materiałami radioaktywnymi, fałszowania pieniędzy oraz prania brudnych pieniędzy,
3) pogłębianie oraz wzmacnianie współpracy policyjnej w regionie wynikającej ze zobowiązań Unii Europejskiej, układu z Schengen, umów i porozumień międzynarodowych, szczególnie w zakresie transgranicznej wymiany informacji oraz działalności oficerów łącznikowych,
4) utrzymywanie wysokiego poziomu etyki zawodowej w organach ścigania i wymiaru sprawiedliwości.

Każdy z obszarów współpracy jest stale nadzorowany przez konkretne państwo lub państwa. Poniżej zaprezentowano zakres odpowiedzialności poszczególnych krajów:

- Polska: badania dotyczące korupcji oraz wspólne[2] działania operacyjne w zakresie zwalczania produkcji i obrotu narkotykami,
- Szwecja: badania dotyczące handlu kobietami,
- Niemcy: wspólne działania operacyjne w zakresie zwalczania nielegalnej migracji,
- Rosja: problematyka zwrotu skradzionych pojazdów,
- Łotwa: wspólne działania operacyjne w zakresie zwalczania przestępczości celnej,
- Finlandia: wspólne działania operacyjne w zakresie zwalczania procederu prania brudnych pieniędzy,
- Norwegia: wspólne działania operacyjne w zakresie zwalczania obrotu skradzionymi pojazdami,
- Litwa: problematyka ochrony świadka oraz wspólne działania operacyjne w zakresie zwalczania przestępczości celnej.

Istnieją również obszary podlegające nadzorowi rotacyjnemu, do których należą badania przestępczości celnej oraz współpraca prokuratorska.

Do regionalnego systemu zwalczania przestępczości BALTCOM należą:

- Grupa Zadaniowa,
- Komitet Operacyjny,
- grupy eksperckie,
- system komunikacji BALTCOM,
- punkty kontaktowe BALTCOM,
- sekretariat.

Strukturę organizacyjną regionalnego systemu zwalczania przestępczości BALTCOM przedstawiono na schemacie.

[2] Tu i w kolejnych podpunktach chodzi o działania wykonywane wspólnie z innymi państwami nadbałtyckimi – przyp. red.

Schemat. Struktura organizacyjna regionalnego systemu zwalczania przestępczości BALTCOM.

Źródło: Opracowanie własne.

W przedstawionej strukturze Grupa Zadaniowa odgrywa nadrzędną rolę. Z formalno-prawnego punktu widzenia jest specjalnym ciałem międzyrządowym powołanym w celu poszukiwania rozwiązań oraz inicjowania wspólnych przedsięwzięć o charakterze strategicznym. Grupa Zadaniowa nie jest stałym organem, ale siecią współpracy konkretnych osób reprezentujących 11 państw regionu Morza Bałtyckiego. Z reguły w jej skład wchodzą przedstawiciele szefów rządów państw regionu w randze sekretarzy stanu, wywodzący się z ministerstw spraw wewnętrznych lub ministerstw sprawiedliwości. Podstawą prawną podejmowanych działań są – w zależności od charakteru przedsięwzięcia oraz państw biorących w nim aktywny udział – konwencje międzynarodowe Organizacji Narodów Zjednoczonych, Rady Europy, Unii Europejskiej czy bilateralne porozumienia i umowy.

Spotkania Grupy Zadaniowej odbywają się od dwóch do trzech razy w roku. Jej działalność podlega ocenie i nadzorowi szefów rządów państw nadbałtyckich. Co dwa lata Grupa składa RPMB raporty ze swojej działalności.

Wspieraniem Grupy Zadaniowej w realizacji jej zadań zajmuje się sekretariat. Działa on w państwie sprawującym prezydencję.

Pracami Grupy Zadaniowej kieruje państwo sprawujące prezydencję. Ma ona charakter rotacyjny, a okres jej sprawowania wynosi dwa lata. O tym, które państwo będzie sprawować prezydencję, decyduje Grupa Zadaniowa. Jako pierwsza Grupie przewodniczyła Szwecja (1996–2001), następnie były to: Dania (2001–2004), Polska (2004–2005), Finlandia (2005–2006), Estonia (2007–2010), Litwa (2011–2012), Norwegia (2013–2014) i Rosja (2015–2016).

Państwo sprawujące prezydencję ma za zadanie regularnie informować o pracach Grupy Zadaniowej następujące organy: Stały Komitet ds. Współpracy Operacyjnej (Standing Committee on Internal Security, COSI), Multidyscyplinarną Grupę ds. Przestępczości Zorganizowanej Rady Unii Europejskiej (Multi-Disciplinary Group on Organised Crime, MDG), Zarząd Europolu oraz Radę Państw Morza Bałtyckiego. Najczęściej właśnie w państwie sprawującym prezydencję odbywają się spotkania Grupy.

Grupa Zadaniowa koncentruje swoją działalność na przestępstwach objętych zakresem przedmiotowym działania Europolu. Tak określony mandat został przyznany Grupie przez szefów rządów państw członkowskich Rady Państw Morza Bałtyckiego, którzy mają kompetencje do jego rozszerzenia i przedłużenia.

W wymiarze operacyjnym Grupa Zadaniowa zatwierdza propozycje wspólnych kierunków działania proponowanych przez Komitet Operacyjny i przesyła propozycje do właściwych ministrów bądź innych organów decyzyjnych.

Za realizację form i metod współpracy policyjnej odpowiada Komitet Operacyjny (The Operative Committee – OPC), który wypracowuje rozwiązania umożliwiające zespołowe prowadzenie bezpośrednich działań operacyjnych. Spotkania tego komitetu odbywają się częściej niż posiedzenia Grupy Zadaniowej (około pięciu razy w roku). W jego skład wchodzą delegowani funkcjonariusze organów ścigania (policji, służb celnych i służb ochrony granic). Komitet Operacyjny odgrywa główną rolę w ocenianiu zagrożeń państw regionu Morza Bałtyckiego związanych z przestępczością zorganizowaną, ułatwia wymianę doświadczeń i najlepszych praktyk, przedkłada propozycje politycznych i legislacyjnych rozwiązań w tym zakresie, a także zajmuje się kwestiami finansowymi związanymi z działalnością Grupy Zadaniowej. Do jego zadań należy również koordynacja współpracy w obszarach o szczególnym znaczeniu (korupcja, szkolenia, administracja podatkowa). Funkcją Komitetu jest implementacja zintensyfikowanej wymiany informacji oraz konkretnych działań operacyjnych.

Komitet Operacyjny działa w ścisłej współpracy z punktami kontaktowymi (ang. *focal points*) wyznaczonymi przez państwa członkowskie. Każde państwo ma obowiązek stworzenia takiego punktu, gdyż stanowi on krajowe centrum współpracy regionalnej. Punkty kontaktowe BALTCOM mają charakter stały i są czynne całodobowo. W strukturze polskiej Policji funkcję tego typu punktu pełni Biuro Międzynarodowej Współpracy Policji KGP.

Pod bezpośrednim nadzorem Komitetu Operacyjnego działają grupy eksperckie. W ich skład wchodzą specjaliści z konkretnych dziedzin zwalczania przestępczości i są one forami wymiany informacji oraz planowania wspólnych przedsięwzięć policyjnych. Pierwsze tego typu grupy utworzono w 1998 r. Obecnie jest ich osiem: ds. handlu narkotykami, ds. handlu kobietami i dziećmi, ds. nielegalnej migracji, ds. nielegalnego handlu wysoko opodatkowanymi dobrami, ds. kradzieży własności intelektualnej, ds. kradzieży pojazdów, ds. handlu bronią oraz ds. przestępczości środowiskowej. W wymiarze praktycznym grupy eksperckie odpowiadają za planowanie oraz przeprowadzanie operacji policyjnych. Spotkania w ramach tego typu grup odbywają się w zależności od potrzeb. Pod ich nadzorem przeprowadzono wiele krótko- bądź długoterminowych operacji i projektów zakończonych sukcesami.

Jako przykład działalności grupy eksperckiej można przedstawić Grupę Ekspertów ds. Zwalczania Handlu Kobietami i Dziećmi (Grupa THB) zajmującą się koordynacją wspólnych operacji z tego zakresu państw nadbałtyckich. Jest ona jedną z pięciu stałych grup roboczych Komitetu Operacyjnego, a inicjatywę jej utworzenia wysunęła w 2003 r.

Szwecja. Pierwotnym celem Grupy THB było przeciwdziałanie handlowi kobietami z obwodów Murmańskiego i Archangielskiego, które trafiały do domów publicznych w Szwecji, Finlandii i Norwegii. Materiały informacyjne Grupy THB są wykorzystywane w pracach Grupy Roboczej Przeciwko Handlowi Ludźmi Rady Państw Morza Bałtyckiego[3].

Do podstawowych form i metod współpracy policyjnej BALTCOM ukierunkowanych na zwalczanie handlu ludźmi należy zaliczyć:

- połączone operacje i wspólne przedsięwzięcia operacyjne,
- wymianę informacji kryminalnych,
- badania i analizy,
- szkolenia specjalistyczne.

Istotą połączonych operacji policyjnych jest wykonywanie w tym samym czasie skoordynowanych czynności wykrywczo-kontrolnych przez właściwe organy wszystkich państw regionu. Operacje policyjne są prowadzone w celu: zatrzymywania osób zaangażowanych w handel ludźmi, zabezpieczania przedmiotów związanych z działalnością przestępczą, zbierania informacji o zwalczanym zagrożeniu (np. o przebiegu szlaków przerzutowych nielegalnych imigrantów czy bieżącym modus operandi) oraz identyfikowania ofiar procederu (głównie kobiet i dzieci). Z punktu widzenia zasięgu geograficznego prowadzonych działań wyróżnia się operacje o ograniczonym zasięgu (z zaangażowaniem minimum dwóch państw) oraz operacje regionalne (uczestniczą w nich wszystkie państwa nadbałtyckie).

Przykładami dotychczas przeprowadzonych operacji policyjnych o charakterze połączonym są m.in.:

1) „Speed I" (maj 1997), „Speed II" (listopad 1997), „Bus stop" (czerwiec 1998), „General aviation" (październik 1998), „Channel" (czerwiec 1999), „Ro-Ro x 3" (wrzesień 1999), „Early Bird" (wrzesień 1999), w zakresie zwalczania produkcji i obrotu narkotykami,
2) „Goldfinger" (styczeń 1999 – styczeń 2000), w zakresie zwalczania procederu prania brudnych pieniędzy,
3) „Baltic Guard I" (maj–czerwiec 1997), „Baltic Guard II" (sierpień–wrzesień 1997), „Baltic Guard 98" (maj 1998), „Emigrant" (październik 1998), „Vivian" (maj 1999), „Greenway 99" (czerwiec 1999), „OAK" (wrzesień 1999), w zakresie zwalczania nielegalnej migracji,
4) „Escort" (styczeń–luty 1999), w zakresie zwalczania przemytu,
5) „Baltic Sea Task-Force vehicle control I" (kwiecień–czerwiec 1997), „Baltic Sea Task-Force vehicle control II" (październik 1997), Projekt Kaliningradzki (czerwiec 1998), „Storskog" (sierpień 1998), „Nordic Routes I" (sierpień 1998), „Nordic Routes II" (luty–marzec 1999), „Nordic Routes III" (wrzesień 1999), w zakresie zwalczania obrotu skradzionymi pojazdami.

Na czas prowadzenia połączonych operacji policyjnych są tworzone specjalne punkty kontaktowe (wspominane *focal points*), których zadaniem jest wspomaganie prowadzonych działań.

Państwa nadbałtyckie mają specjalny system wymiany informacji kryminalnych, w którego skład wchodzi sieć łączności (*The Baltic Sea Encrypted Network*) oraz sieć

[3] Zob. Z. Lasocik, E. Rekosz-Cebula, Ł. Wieczorek, *Handel ludźmi do pracy przymusowej: mechanizmy powstawania i efektywne zapobieganie. Raport z realizacji Projektu ADSTRINGO – Przeciwdziałanie handlowi ludźmi do pracy przymusowej poprzez usprawnienie współpracy, diagnozę problemów i wzmocnienie systemowego podejścia w Polsce i Federacji Rosyjskiej*, Warszawa–Sztokholm 2014.

punktów kontaktowych. Sieć łączności została utworzona w 1997 r. na podstawie systemu X-400 użytkowanego w ramach INTERPOL-u. W celu utworzenia jednolitych standardów łączności opracowano specjalny podręcznik (*The Task-Force Contact Manual*).

Wymiana informacji w ramach Grupy Zadaniowej dotyczy przede wszystkim zagadnień operacyjnych związanych z przedmiotem działania grup eksperckich oraz prowadzonymi operacjami połączonymi (zarówno informacje *ex-ante*, jak i *ex-post*). Są to dane dotyczące m.in.:

- osób zatrzymanych lub aresztowanych podczas wspólnych działań,
- szlaków przemytu narkotyków,
- przejęć narkotyków – głównie środków uzyskiwanych z konopi siewnej i indyjskiej (marihuany i haszyszu), kokainy, heroiny, amfetaminy, ecstasy i LSD,
- nazwisk, adresów, numerów telefonów oraz powiązań między osobami zamieszanymi w handel narkotykami,
- tras przerzutu kobiet i dzieci (ofiar handlu ludźmi),
- tras nielegalnych migrantów,
- identyfikowania kanałów i szlaków przemytu kradzionych samochodów oraz dóbr wysoko opodatkowanych (papierosów, alkoholu).

W ramach BALTCOM prowadzi się również projekty analityczne związane z wymianą danych wywiadowczych. Przykładowo w odniesieniu do handlu ludźmi są to:

- projekt „Reveal" dotyczący wymiany informacji o zorganizowanych grupach przestępczych zaangażowanych w handel ludźmi,
- projekt „Minors" zogniskowany na wymianie informacji dotyczących osób nieletnich narodowości chińskiej, które mogą być ofiarami procederu[4].

Współpraca sądowa jest skupiona wokół problemu ochrony świadka, kooperacji prokuratorskiej oraz monitorowania stanu ratyfikacji konwencji i innych aktów prawa międzynarodowego z zakresu zwalczania przestępczości.

W ramach sytemu BALTCOM dużą wagę przywiązuje się do stworzenia jednolitych standardów działania. W tym celu stworzono specjalne podręczniki: dotyczący utrzymywania wzajemnej łączności (*Task-Force Contact Manual*), prowadzenia operacji przesyłki kontrolowanej (*Baltic Sea Manual on Controlled Deliveries*) oraz zwalczania procederu prania brudnych pieniędzy (*Baltic Sea Manual on Money Laundering and Asset Tracing*).

W zakresie zwalczania przestępczości transgranicznej Grupa Zadaniowa prowadzi szeroką współpracę z innymi podmiotami. Wśród nich można wyróżnić dwie główne grupy: państwa trzecie oraz instytucje. Państwa trzecie to kraje, które nie są państwami członkowskimi Grupy Zadaniowej, np. Holandia (w zakresie zwalczania produkcji narkotyków syntetycznych), Wielka Brytania (w zakresie zwalczania przemytu papierosów) oraz USA (w zakresie zwalczania handlu ludźmi). Grupa rozwija także współpracę z krajami Europy Wschodniej, takimi jak Białoruś czy Ukraina.

Grupa Zadaniowa była w ostatnich dwóch dekadach narzędziem często wykorzystywanym przez państwa regionu do umacniania zdolności zapobiegania i zwalczania przestępczości zorganizowanej. Przegląd współpracy policyjnej podejmowanej w regionie Morza Bałtyckiego na przełomie XX i XXI wieków wskazuje na bogate doświadczenia w realizacji wielu inicjatyw kontrprzestępczych. Z całą pewnością sprzyjała im stabilizacja polityczna i ekonomiczna stosunków międzypaństwowych w regionie Morza Bałtyckiego.

[4] *Action Plan on Trafficking in Human Beings*, Rada Unii Europejskiej, 6282/1/07 REV 1, Bruksela 2007, s. 17.

Obecnie zasadnicze pytanie brzmi: Czy wobec efektywnej współpracy policyjnej w ramach Europolu jest jeszcze przestrzeń dla dalszego rozwoju Grupy Zadaniowej?

Grupa Zadaniowa powstała w zupełnie innym środowisku międzynarodowym niż to, jakie jest dzisiaj, a warunki dwustronnej i wielostronnej współpracy państw regionu Morza Bałtyckiego znacznie różniły się od obecnych. Kiedy rozpoczynała ona swoją działalność, państwa prowadzące współpracę miały odmienne uregulowania prawne, stosowały inne metody i przechodziły różne szkolenia w zakresie przeciwdziałania przestępczości zorganizowanej oraz walki z nią. Uzasadnieniem działania Grupy były potrzeba przełamywania przeszkód utrudniających współpracę (np. ograniczone kanały i środki wymiany informacji) oraz budowanie zaufania w bezpośrednich stosunkach i kontaktach pomiędzy funkcjonariuszami służb policyjnych państw do niedawna oddzielonych żelazną kurtyną.

Obecnie region Morza Bałtyckiego jest prawie w całości częścią Unii Europejskiej lub obszaru Schengen, oferujących wiele kanałów i środków wymiany informacji. To powoduje naturalne przesuwanie sfery współpracy policyjnej większości państw nadbałtyckich na platformę Europolu.

Zasadniczym problemem dla współpracy kontrprzestępczej w regionie Morza Bałtyckiego staje się postawa polityczna Rosji, nabierająca wyraźne oznaki konfrontacyjne. Wzrost napięć w relacjach międzypaństwowych oraz ostre konflikty międzynarodowe zawsze negatywnie odbijają się na współpracy policyjnej między skonfliktowanymi państwami. Z tego powodu w ostatnim okresie poziom koordynacji wspólnych działań policyjnych w formule BALTCOM wyraźnie osłabł. Współpraca policyjna państw w regionie Morza Bałtyckiego pełni obecnie rolę subsydiarną wobec współdziałania w ramach Europolu oraz czynności podejmowanych na podstawie zawartych umów bilateralnych.

Niezależnie od tej oceny formuła współdziałania BALTCOM ma znaczenie dla zwalczania przestępczości o charakterze przemytniczym, gdyż mimo przyjętych reżimów prawnych wymiana towarowa między Obwodem Kaliningradzkim a centralną częścią Rosji zawsze będzie generować zagrożenie, że część wymienianych towarów zostanie przemycona do państw UE.

Wobec narastającej presji w związku z falą migracji do państw UE należy spodziewać się zwiększenia roli BALTCOM-u w zwalczaniu nielegalnej migracji i handlu ludźmi. Nielegalny przerzut ludzi będzie przez najbliższe lata czynnikiem o dużej sile oddziaływania na stan bezpieczeństwa w całej Europie. Należy również zakładać wzrost presji migracyjnej na państwa regionu Morza Bałtyckiego, w tym również z kierunku wschodniego.

Bibliografia:

1. *Action Plan on Trafficking in Human Beings*, Rada Unii Europejskiej, 6282/1/07 REV 1, Bruksela 2007.
2. Bielecki Z., Zwalczanie przestępczości narkotykowej w regionie państw Morza Bałtyckiego, „Policja" 2004, nr 1–2, s. 90–94.
3. Lasocik Z., Rekosz-Cebula E., Wieczorek Ł., *Handel ludźmi do pracy przymusowej: mechanizmy powstawania i efektywne zapobieganie. Raport z realizacji Projektu ADSTRINGO – Przeciwdziałanie handlowi ludźmi do pracy przymusowej poprzez usprawnienie współpracy, diagnozę problemów i wzmocnienie systemowego podej ścia w Polsce i Federacji Rosyjskiej*, Warszawa–Sztokholm 2014, bw.

4. *Searching and finding solutions – a booklet about the Task-Force on Organized Crime in the Baltic Sea Region*, The Secretariat of the Task-Force on Organized Crime in the Baltic Sea Region, Sztokholm 2000, bw.

Abstrakt

Artykuł przedstawia genezę, główne aspekty działania oraz perspektywy rozwoju współpracy w ramach formuły BALTCOM, której celem jest zwalczanie przestępczości transgranicznej w regionie Morza Bałtyckiego. W 2016 r. przypada 20. rocznica nawiązania operacyjnej współpracy w zakresie zwalczania przestępczości zorganizowanej przez państwa tego regionu. Problematyka omawiana w artykule jest bardzo skomplikowana z powodu specyfiki działań kontrprzestępczych prowadzonych w ramach BALTCOM-u oraz jego umiejscowienia w systemie współpracy międzynarodowej. W artykule zwrócono uwagę na korzyści wynikające z metod i form międzynarodowego współdziałania Polski w BALTCOM.

Słowa kluczowe: BALTCOM, współpraca międzynarodowa, operacje połączone, wymiana informacji, zagrożenia transgraniczne.

Abstract

The article presents the origins, the main aspects of activity and development prospects of the cooperation in the framework of BALTCOM, which is aimed at combating cross-border crime in the Baltic Sea Region. In 2016 it is the 20th anniversary of the establishment of operational cooperation in combating organized crime in the Baltic Sea Region. The presented issue is extremely complex due to the specific nature of the activities carried out on BALTCOM platform and its unique position in the international system of cooperation. Article draws the attention to possible benefits for Poland from such form of international cooperation in combating organized crime as BALTCOM.

Keywords: BALTCOM, international cooperation, joint operations, criminal intelligence, transborder threats.

Marek Świerczek

Wojna hybrydowa jako strategia polityczna. Próba analizy historycznej na przykładzie działań ZSRS wobec II RP

Wstęp

Podczas analizy działań współczesnych rosyjskich służb specjalnych należy zdać sobie sprawę z tego, że ich modus operandi został wypracowany na początku lat 20. XX w. To właśnie wtedy rewolucyjne pomysły twórców kontrwywiadu ofensywnego i szeroko zaprojektowanych operacji dezinformacyjnych[1] zetknęły się z osiągnięciami carskiej Ochrany[2], której funkcjonariusze w dużym stopniu zasilili nie tylko kształtujący się wywiad Armii Czerwonej, lecz także WCzeKa oraz późniejsze GPU i OGPU. Z tego powodu wszelkie próby zrozumienia działalności współczesnego wywiadu rosyjskiego, zarówno na płaszczyźnie stricte operacyjnej, jak i rozumianej jako jeden z elementów polityki zagranicznej Rosji, wymagają perspektywy historycznej. Tylko takie spojrzenie pozwala poznać stosowane w przeszłości operacyjne instrumentarium i wyciągnąć wnioski na podstawie celów osiąganych za jego pomocą.

Jedną z metod obecnie wykorzystywanych w rosyjskiej polityce jest tzw. wojna hybrydowa. Są to kompleksowe działania, których założenia teoretyczne zostały wypracowane na początku lat 20. XX w. przez Razwiedupr RKKA[3] w celu destabilizacji Rzeczpospolitej Polskiej za pomocą metod dywersyjno-terrorystycznych[4].

Geneza

Bitwa warszawska zablokowała szybką ekspansję bolszewizmu na zachód Europy, ale problemami Sowdepii[5], które w rzeczywistości zahamowały eksport rewolucji, były

[1] Twórcą nowych rozwiązań operacyjnych na poziomie taktycznym i strategicznym był Artur Artuzow, który zaplanował, a następnie zrealizował największe i najciekawsze operacje sowieckiego kontrwywiadu, tj. Syndykat 2 i Trust. Artuzow (ur. 16 II 1891 r. w Ustinowie, zm. 21 VIII 1937 r. w Moskwie) wywodził się ze zruszczonej rodziny szwajcarskiej (prawdziwe nazwisko Frautschi). W czasie studiów politechnicznych w Petersburgu zetknął się ze studenckim ruchem socjalistycznym. Podczas rewolucji październikowej wstąpił do RKP(b) i z ramienia partii w 1919 r. rozpoczął służbę w WCZeKa. Rok później został zastępcą naczelnika Osobogo Otdieła, a wkrótce potem – naczelnikiem KRO GPU (Wydziału Kontrwywiadowczego). W latach 1931–1935 był naczelnikiem INO GPU (wywiadu), łącząc tę funkcję z funkcją najpierw zastępcy naczelnika Razwiedupra (RU) RKKA (wywiadu Armii Czerwonej), a od 1937 r. – naczelnika RU RKKA. W 1937 r. został aresztowany przez NKWD i rozstrzelany. Za: http://svr.gov.ru/history/ar.htm [dostęp: 28 VIII 2015].

[2] WCzeKa przejęła nie tylko archiwa i metody pracy, lecz także pracowników Ochrany. W Ludowym Komisariacie Spraw Wewnętrznych 48,3% pracowników wywodziło się ze struktur carskich, w samej zaś CzeKa – 16,1%. Zob. R. Pipes, *Rosja bolszewików*, Warszawa 2005, s. 449.

[3] Ros. Разведывательное Управление Рабоче-Крестьянской Красной Армии, Zarząd Wywiadowczy Sztabu Robotniczo-Chłopskiej Armii Czerwonej. Taka nazwa funkcjonowała od 4 kwietnia 1921 r., wcześniej był to Registrupr – poprzednik dzisiejszego wywiadu wojskowego FR – GRU.

[4] Podobne założenia tego typu operacji specjalnych wypracował oficer wojsk białych płk Jewgienij Messner, którego prace na temat *mjatieżnoj wojny* (wojny buntowniczej) na pewno były znane GPU i RKKA – por. wywiad z Adamem Rotfeldem, *Putin walczy o duszę Rosji*, „Gazeta Wyborcza" z 26 marca 2014.

[5] Określenie Rosji Sowieckiej używane w Oddziale II SG WP, skrót od rosyjskiej nazwy *Совет Депутатов.*

nie porażka armii Michaiła Tuchaczewskiego, lecz kryzys gospodarczy i wewnętrzna sytuacja Rosji Sowieckiej. Dobrą ilustracją tej tezy było wystąpienie Lenina w czasie X Zjazdu RKP(b):

> Na froncie ekonomicznym, przy próbie przejścia do komunizmu, ponieśliśmy wiosną 1921 roku większą klęskę, niż którakolwiek z klęsk, jakie ponieśliśmy w walce z Kołczakiem, Denikinem czy Piłsudskim[6].

Po 30 miesiącach od wprowadzenia komunizmu wojennego[7], na początku 1921 r., stało się jasne, że sytuacja gospodarcza w ZSRS jest krytyczna. Nacjonalizacja środków produkcji, zniesienie prywatnego handlu, likwidacja pieniądza, objęcie gospodarki narodowej planem oraz wprowadzenie pracy przymusowej spowodowały chaos i załamanie gospodarcze[8].

W latach 1920–1921 produkcja przemysłowa w stosunku do roku 1913 spadła o 82 proc. (w przemyśle metalurgicznym, istotnym podczas wojny, produkcja wynosiła 6 proc. stanu z 1914 r.)[9], wydajność pracy – o 74 proc., a produkcja zbóż – o 40 proc. Drastycznie zmniejszyła się populacja miejska, zwłaszcza w północnej Rosji, którą południe kraju zaopatrywało w żywność. Liczba mieszkańców Piotrogrodu spadła o 70 proc., a Moskwy – o 50 proc.[10] Liczebność nierolniczej siły roboczej zmniejszyła się z 3,6 mln osób w 1917 r. do 1,5 mln. Towarzyszył temu spadek o 1/3 płacy realnej robotników przemysłowych. Bolszewikom – w dużym stopniu z powodu ideologicznego zaślepienia – udało się całkowicie zrujnować piątą co do wielkości (w 1914 r.) gospodarkę świata[11].

Konfiskaty ziarna wprowadzone przez komunizm wojenny odbywały się według absurdalnej zasady zakładającej, że im więcej zboża chłop wyprodukował, tym więcej mu go odbierano, nie zezwalając na sprzedaż nadwyżek. Chłopom nie opłacało się zatem zbierać więcej ponad to, co było im potrzebne do wyżywienia rodzin i obsiania pól. To z kolei doprowadziło do wzrostu rekwizycji, podczas których nawet ziarno siewne padało ofiarą, a w konsekwencji – do głodu[12]. Ten zaś skłonił zwykle bierną

---

[6] R. Pipes, *Rosja bolszewików*, Warszawa 2013, s. 373.

[7] Komunizm wojenny wynikał z ideologicznego zaślepienia bolszewików (których jednym z głównych przedstawicieli był Lew Trocki) zakładających, że siłą roboczą Rosji Sowieckiej powinno się zarządzać jak armią, czyli stosując wszystkie elementy dyscypliny wojskowej, z pominięciem jakichkolwiek bodźców ekonomicznych – por. opis pozycji Trockiego w: *Материалы к изучению истории СССР (1921–1941 гг.)*, Москва 1989 – fragmenty bez paginacji na stronie: http://www.hrono.ru/sobyt/1900sob/1921_10sezd.php [dostęp: 16 II 2015]: „Именно на принудительном общественно-обязательном труде и стоит все социалистическое строительство. Социалистическое общество строится на основах коллективного принуждения класса, на труде общеобязательным... В военной области имеется соответствующий аппарат, который пускается в действие для принуждения солдат к исполнению своих обязанностей. Это должно быть в том или другом виде и в области трудовой... Рабочая масса... должна быть перебрасываема, назначаема, командуема точно так же, как солдаты. Это есть основа милитаризации труда... после того, как мы преодолеем первую нищету, мы сможем перескакивать целый ряд ступеней в своем развитии".

[8] R. Pipes, *Rosja bolszewików*…, s. 373.

[9] L. Nikulin, *Miortwaja zyb'* [online], bez paginacji, http://royallib.ru/book/nikulin_lev/mertvaya_zib.html [dostęp: 21 XI 2013].

[10] R. Pipes, *Rosja bolszewików*…, s. 374–375; por. D. Koenker, W.G. Rosenberg, R.G. Suny, *Party, State, and Society in the Russian Civil War*, Bloomington 1989, s. 58–61.

[11] Por.: R. Pipes, *Rosja bolszewików*…, s. 374–375.

[12] Już w styczniu 1921 r. ponad 50% chłopskich rodzin na Tambowszczynie głodowała. Por. wystąpienie Lenina w czasie X Zjazdu RKP(b): „Но эти обстоятельства привели нас к тому, что крестьянское хозяйство после продолжавшейся так долго войны так ослабело, что неурожай оказался и на почве понижения засева, и ухудшения средств производства, и понижения урожайности, и недостатка рабочей силы,

i obojętną na politykę ludność wiejską do buntu. Skala wzburzenia była ogromna. Należy przy tym pamiętać, że choć bolszewicy kontrolowali miasta, to jednak 80 proc. populacji Rosji zamieszkiwało na wsiach[13]. Według danych CzeKi w 1921 r. doszło do 118 lokalnych powstań (należy przypuszczać, że ta statystyka z powodów propagandowo-ideologicznych była zaniżona)[14]. Zgrupowania chłopskie liczyły nawet do 50 tys. powstańców, były zorganizowane na wzór Armii Czerwonej i kontrolowały potężne terytorium[15]. W walkach ze zbuntowanymi chłopami (które na Zachodzie nazwano „ruchem zielonych", widząc w nim ideologiczną opozycję wobec czerwonego reżimu) Armia Czerwona straciła 237 908 żołnierzy[16].

Jednocześnie problemy z aprowizacją (a także zapewnieniem dostaw oleju i węgla, co w rosyjskim klimacie prowadziło do poważnych problemów ludności miejskiej zmuszonej do rozbierania pustych domów na opał) sprowokowały strajki w przemyśle i niemal całkowitą utratę poparcia społecznego[17]. W lutym 1921 r. wybuchł bunt marynarzy w Kronsztadzie, do którego doszło po decyzji z 22 stycznia 1921 r. o zmniejszeniu o 1/3 racji żywnościowych. Zbuntowana załoga z Kronsztadu została spacyfikowana w marcu 1921 r. przez Lwa Trockiego, który jednak wykorzystał do tego nie Armię Czerwoną (gdyż przestał jej ufać[18]), ale specjalne jednostki, zwane *czast'jami osobowo naznaczenia*, utworzone w 1919 r. w celu tłumienia rozruchów. Bunt kronsztadzki, choć krwawo stłumiony, był sygnałem dla bolszewików mówiącym o możliwej utracie poparcia także wśród żołnierzy, to natomiast mogło oznaczać koniec reżimu opartego na aparacie przymusu, którego częścią była Armia Czerwona[19].

W tej sytuacji kierownictwo partii bolszewickiej zdało sobie sprawę z tego, że Rosja Sowiecka potrzebuje czasu, aby odbudować swój potencjał i skonsolidować władzę, zanim rzuci wyzwanie Zachodowi i spróbuje *przenieść ogień rewolucji* przede wszystkim do burżuazyjnych Niemiec.

Taka była geneza ustaleń X zjazdu RKP(b), podczas którego odstąpiono od komunizmu wojennego i wprowadzono Nową Politykę Ekonomiczną (NEP). Bolszewicy

---

и т. д. Неурожай оказался громаднейший, и лучший, чем всё-таки мы ожидали, сбор продовольственных излишков оказался спутником такого обострения кризиса, который, может быть, готовит нам ещё большие трудности и бедствия в предстоящие месяцы" – za: *Diesiatyj sjezd Kommunisticzeskoj partii. Stenograficzeskij otcziot (8–16 marta 1921 g.)* – Moskwa 1921, wersja elektroniczna bez paginacji, http://leninism.su/works/82-tom-43/1038-x-sezd-rkpb.html [dostęp: 16 II 2015].

[13] L.H. Siegelbaum, *Soviet State and Society: Between Revolutions, 1918–1929*, Cambridge 1992, s. 68. Sowieci zdawali sobie sprawę z sytuacji, czego dowodem jest wypowiedź Lenina w czasie X Zjazdu RKP(b): *А у нас первая особенность, именно та, о которой я говорил и которая России свойственна в максимальной степени: мы имеем не только меньшинство, но и значительное меньшинство пролетариата и огромное большинство крестьянства*. Za: *Diesiatyj sjezd…*, http://leninism.su/works/82-tom-43/1038-x-sezd-rkpb.html [dostęp: 16 II 2015].

[14] R. Pipes, *Rosja bolszewików*…, s. 375.

[15] Na Tambowszczynie zgrupowanie zorganizowane przez Aleksandra Antonowa liczyło 50 tys. powstańców, rekrutowanych przez Związek Pracującego Chłopstwa.

[16] R. Pipes, *Rosja bolszewików*…, s. 376.

[17] Na X Zjeździe RKP(b) Zinowjew otwarcie powiedział, że klasa robotnicza (mająca być klasą przodującą) jest albo obojętna politycznie, albo wspiera mieńszewików lub Czarną Sotnię – por. *Diesiatyj sjezd…*, http://leninism.su/works/82-tom-43/1038-x-sezd-rkpb.html [dostęp: 16 II 2015]; por.: P. Kenez, *A History of the Soviet Union from the Beginning to the End*, Cambridge 2006, s. 48.

[18] Sowiecka władza miała powody do braku zaufania wobec Armii Czerwonej nie tylko z uwagi na wysoki odsetek maruderów i dezerterów, lecz także – przejawy buntu o podłożu ideologicznym. Dla przykładu w lipcu 1920 r. 9 Dywizja RKKA zbuntowała się i utworzyła formację pod nazwą *Krasnaja Armija Prawdy*.

[19] Por. R. Pipes, *Rosja bolszewików*…, s. 381–386. Por. wydarzenia poprzedzające X Zjazd RKP(b) – *Материалы к изучению …*, http://www.hrono.ru/sobyt/1900sob/1921_10sezd.php [dostęp: 16 II 2015].

jednak, na czele z Leninem, zakładali jedynie taktyczny charakter NEP, niezbędny do odtworzenia zrujnowanej gospodarki, administracji i armii[20]. Jak mówił Lenin:

> Proszę was, towarzysze, abyście jasno zrozumieli (…), że Nowa Ekonomiczna Polityka jest tylko chwilowym ustępstwem, oczyszczeniem przedpola do nowego i decydującego ataku świata pracy na pozycje międzynarodowego kapitalizmu[21].

Dla Rosji Sowieckiej zatem najważniejszym celem była odbudowa gospodarki zniszczonej podczas rewolucji i wojny domowej, do czego było konieczne zdobycie z Zachodu kapitału i technologii niezbędnych do wzrostu zapóźnionego i wyniszczonego sowieckiego przemysłu oraz nakłonienie kadr technicznych, potrzebnych do uruchomienia procesów technologicznych, do powrotu zza granicy do Rosji[22]. Aby to osiągnąć, należało zdobyć pełną kontrolę nad krajem rozdzieranym buntami chłopskimi, przyciągającymi uwagę zarówno rosyjskiej białej emigracji, jak i zachodnich służb, które wciąż rozpatrywały możliwość przeprowadzenia kolejnej interwencji zbrojnej w Rosji osłabionej wojną domową i zapaścią gospodarczą[23].

W celu odbudowy państwa Związek Sowiecki potrzebował tzw. *pieredyszki* (okresu spokoju), aby korzystając z uruchomionych procesów ekonomicznych, odtworzyć przemysł, skonsolidować państwo i unowocześnić armię. Inaczej mówiąc, bolszewicy dążyli do przejścia na pokojowe współistnienie z państwami burżuazyjnymi w celu odtworzenia potencjału gospodarczo-militarnego[24], a następnie – realizacji postulatu światowej rewolucji. *Pieredyszka* nie oznaczała więc odrzucenia celów strategicznych, a jedynie przesunięcie ich realizacji w czasie. NEP i pokojowe współistnienie były tylko manewrem taktycznym.

Takie założenia dotyczyły również polityki wobec II Rzeczpospolitej. Sowdepia nigdy nie pogodziła się z istnieniem niepodległej, burżuazyjnej Polski, zwłaszcza z jej rolą w kordonie sanitarnym, który Zachód (szczególnie Francja) budował wokół państwa sowieckiego[25]. Z powodu wewnętrznej słabości Rosja nie była jednak w stanie doprowadzić do upadku II RP, szczególnie w sytuacji, gdy w państwach Zachodu wciąż była żywa idea kolejnej wojny interwencyjnej, która mogła obalić osłabiony gospodarczo reżim bolszewicki. Z tego zaś wynikała prosta konkluzja: Rosja Sowiecka musiała dążyć do dekompozycji struktur państwa polskiego, nie przekraczając jednak granic otwartej agresji, aby nie narazić się na wspólną interwencję państw zachodnich, polskiej armii (w 1920 r. Rosjanie przekonali się o jej zdolności bojowej) oraz resztek wojsk białych, wciąż zachowujących struktury wojskowe, których kierownictwo było orędownikiem zbrojnego obalenia sowieckiego reżimu.

---

[20] Por.: fragmenty książki N. Chruszczowa *Wremia. Liudi. Wlast'* [online], http://www.hrono.ru/libris/lib_h/hrush03.php [dostęp: 16 II 2015].

[21] R. Pipes, *Rosja bolszewików*…, s. 372.

[22] W ówczesnej terminologii byli to tzw. specjaliści, czyli głównie inżynierowie i pozostała tzw. inteligencja pracująca, bez której funkcjonowanie sowieckiej gospodarki było niemożliwe. Należy podkreślić, że bolszewicy próbowali także sprowadzić do zrujnowanego kraju wysoko wykwalifikowaną siłę roboczą niepochodzącą z Rosji. Dla przykładu *Russko-Amierikanskaja Industrial'naja Korporacyja* (RAIK) zajmowała się werbowaniem amerykańskich wykwalifikowanych robotników do sowieckiego przemysłu włókienniczego.

[23] Por. CAW Oddział II SG, sygn. I.303.4.2161, *Sprawozdanie No 333/133* z 8 II 1923 r.

[24] Por. wypowiedź Lenina w czasie X Zjazdu*: Из тех узловых пунктов нашей работы, которые за этот год больше всего обращают на себя внимание и с которыми связано, на мой взгляд, больше всего наших ошибок, первым является переход от войны к миру*, http://leninism.su/works/82-tom-43/1038-x-sezd-rkpb.html [dostęp: 16 II 2015].

[25] W. Materski, *Tarcza Europy. Stosunki polsko-sowieckie 1918–1939*, Warszawa 1994, s. 83.

Co za tym idzie Sowdepia musiała zacząć realizować swoje cele środkami innymi niż polityka czy otwarta wojna. Z tego powodu opracowano koncepcję doprowadzenia do upadku młodego państwa polskiego za pomocą niejawnych metod, w których udział Rosji Sowieckiej byłby nie na tyle oczywisty, aby stanowić *casus belli.* Po podpisaniu traktatu ryskiego sytuacja w Polsce zdawała się sprzyjać takim rozwiązaniom.

Sytuacja społeczno-gospodarcza RP na początku lat 20. XX w.

Wskutek działań militarnych trwających niemal siedem lat na terytorium RP państwo polskie było w ruinie. W czasie I wojny światowej, nie licząc zmilitaryzowanego przemysłu węglowego, okupanci zlikwidowali w Kongresówce niemal cały przemysł. Z samej tylko Łodzi do Niemiec trafiły 4933 tony maszyn[26] oraz 350 tys. wykwalifikowanych robotników. Identycznie postępowały zarówno carskie, jak i sowieckie wojska, które w 1921 r. wywiozły z terenów polskich kilkaset zakładów przemysłowych oraz praktycznie cały tabor kolejowy[27].

Rzeczpospolita została „zlepiona" z trzech zaborów, wcześniej prawnie, mentalnie, gospodarczo i infrastrukturalnie związanych ze swoimi metropoliami[28], które w dodatku były wyniszczone działaniami zbrojnymi[29]. Ludność, po latach wojny i ponad stuleciu zaborów, była w większości okaleczona moralnie i w dużej mierze obojętna na hasła narodowe[30], skupiona na stricte biologicznym przetrwaniu[31].

U zarania odrodzonej polskiej państwowości pakiet przyjętych przez sejm ustaw stawiał Polskę w czołówce krajów nowoczesnych, realizujących to, co później zostało określone jako społeczna gospodarka rynkowa. Dla przykładu, uchwalono powszechne prawo wyborcze dla kobiet[32], wolność sumienia, słowa, zgromadzeń, zrzeszania się, strajków, równość wobec prawa, najkrótszy w Europie tydzień pracy (46-godzinny) i ochronę praw pracowniczych.

---

[26] J. Kowalski, *Zarys historii polskiego ruchu robotniczego 1918–1939*, Warszawa 1962, s. 15.

[27] Po podpisaniu traktatu ryskiego Sowieci zwrócili RP wyposażenie kilkunastu fabryk, mimo udowodnienia przez Polskę prawa do kilkuset. Zob. W. Materski, *Tarcza Europy...*, s. 177.

[28] Chodzi zarówno o stolice państw zaborczych, jak i – w szerszym sensie, stosowanym w badaniach nad kolonializmem – centra władzy zaborczej, narzucające podbitym terytoriom nie tylko swoje prawa, lecz także sposób postrzegania samych siebie.

[29] Poza Śląskiem (traktowanym przez Niemców jako integralna część cesarstwa), którego wytwórczość zasadniczo nie uległa dewastacji. Zniszczenia były tak poważne, że do 1939 r. polski przemysł nie osiągnął poziomu produkcji z 1913 r. (w 1938 r. było to 94,5% produkcji z 1913 r.).

[30] Chodzi nie tylko o niepowodzenie próby wywołania powstania w Kongresówce przez wkraczające Legiony, lecz także o opinie powszechnie panujące wśród osób aktywnych politycznie i świadomych narodowo, z których wynikało, że ruch narodowy był nieliczny. Por.: *Myliłby się, kto by sądził, że młodzi Polacy garnęli się masowo do ZWC* (I. Daszyński, *Pamiętniki*, t. 2, Kraków 1926, s. 44), [legiony to – przyp. aut.] *samotna walka nielicznych w Polsce Ludzi* (...) *wydawana wbrew własnemu narodowi* [przy doznawaniu – przyp. aut.] *lekceważeń i zniewag, niezrozumienia i tępoty otaczających nas we własnym społeczeństwie* (M. Sokolnicki, *Czternaście lat*, Warszawa 1936, s. 435), (...) *i teraz po roku wojny, jesteśmy tylko awangardą bez mas...* (rozkaz J. Piłsudskiego z 22 VIII 1914), *Polski przestali chcieć w olbrzymiej większości także i Polacy* (M. Sokolnicki, *Sprawa polska na terenie międzynarodowym.* „Niepodległość" 1930, t. 1, z. 2, s. 198). Może najbardziej lapidarnie ujmowała tę sytuację pierwotna wersja jednej ze strof piosenki *My, pierwsza brygada*: *Nie chcemy już od was uznania/ Ni waszej krwi, przelanych łez/ Skończyły się dni kołatania/ Do waszych serc, j..ał was pies*!

[31] Podczas bitwy warszawskiej z polskiej armii zdezerterowało 100 tys. żołnierzy (należy pamiętać, że w 1921 r. obowiązek służby wojskowej obejmował jedynie Polaków oraz obywateli RP narodowości żydowskiej, z pominięciem Ukraińców i Białorusinów. E.V. D'Abernon, *Osiemnasta decydująca bitwa w dziejach świata*, Warszawa 1932, s. 53.

[32] We Francji takie prawo zostało przegłosowane dopiero w 1946 r.

Szybko okazało się jednak, że egoizm klas posiadających doprowadził do wyjątkowo nierównego rozłożenia ciężarów podatkowych[33] i uniemożliwił korzystanie z większości praw socjalnych. Jednym z najważniejszych dla rozwoju ekonomicznego II RP aktów prawnych była ustawa o reformie rolnej[34], która przez całe dwudziestolecie nie doczekała się pełnej realizacji, choć niemal wszyscy ekonomiści podkreślali, że był to jedyny sposób, aby dać gospodarce impuls modernizacyjny[35].

Zniszczenie przemysłu oraz dominacja w gospodarce rolnej gospodarstw o niewielkim areale niezdolnych do produkcji sprawiały, że w miastach rosło bezrobocie, a w rolnictwie oceniano liczbę osób bez możliwości realnego zatrudnienia (tzw. zbędnych) na 4,5 miliona[36]. Dodatkowo z 27 176 tys. ludności ponad 30 proc. należało do mniejszości narodowych, które z różnych względów były wrogie wobec państwa polskiego lub w najlepszym przypadku – obojętne[37].

Wszelkie próby modernizacji państwa – oprócz oporu środowisk niechętnych zmianom (czyli głównie ziemiaństwa i kapitału zagranicznego[38]) – były niezwykle trudne do przeprowadzenia z uwagi na położenie geopolityczne Polski, które sprawiało, że lwią część wydatków państwowych pochłaniała armia[39]. W latach 1919–1920 wydatki zbrojeniowe stanowiły 53,7 proc. budżetu, w 1921 r., po podpisaniu traktatu ryskiego, spadły do poziomu 29,2 proc.[40], aby potem znów wzrosnąć w związku z narastającym zagrożeniem współpracy Niemiec i Rosji Sowieckiej.

Takie czynniki społeczno-gospodarcze sprawiały, że w ocenie sowieckich ideologów Polska miała być państwem słabym, rozdzieranym przez konflikty etniczne i walkę klas[41]. To zaś pozwalało wierzyć w możliwość wywołania zbrojnego powstania, zwanego w nomenklaturze propagandowej rewolucją[42].

---

[33] Dla ilustracji: najwyższe stawki podatku gruntowego płaciły gospodarstwa do 0,5 ha, najniższe zaś – te powyżej 2 tys. ha.

[34] Uchwalona przez sejm 15 VII 1920 r., lecz nigdy w pełni nie zrealizowana z powodu lobbingu środowiska ziemiańskiego silnego ekonomicznie i politycznie.

[35] Reforma rolna musiała być kołem zamachowym przemian społeczno-gospodarczych w sytuacji, gdy w II RP latyfundia (czyli 0,5% ogółu gospodarstw) zajmowały 45% ziemi uprawnej, niezdolne zaś do produkcji rynkowej minifundia zajmowały 14% areału, obejmując za to 64% ogółu gospodarstw.

[36] Aż 73,8% było zatrudnionych w rolnictwie, w przemyśle i górnictwie – 9,1%, w administracji, wojsku i wolnych zawodach – 5%. Za: Z. Landau, J. Tomaszewski, *Zarys historii gospodarczej Polski 1918–1939*, Warszawa 1960, s. 32, 35.

[37] W tym okresie w II RP zamieszkiwało 14,3% Ukraińców, 7,8% Żydów, 3,9% Białorusinów (Poleszuków), 3,9% Niemców. Za: *Rocznik statystyczny Rzeczpospolitej Polskiej za rok 1925/1926*, t. IV, Warszawa 1927, s. 26.

[38] Udział procentowy kapitału zagranicznego w gospodarce wynosił w okresie międzywojnia od 41% (w przemyśle, łączności i bankowości) do 83,2% w hutnictwie. Firmy zagraniczne były, co oczywiste, zainteresowane w utrzymaniu status quo.

[39] Dodatkowym czynnikiem zamrażającym ten stan rzeczy była podpisana 19 II 1921 r. konwencja wojskowa z Francją, która – w zamian za udział Francji w konflikcie – nakładała na RP obowiązek utrzymywania armii w sile 30 dywizji piechoty i 10 brygad kawalerii (P. Stawecki, *Polityka wojskowa Polski 1921–1926*, Warszawa 1981, s. 64). Powodowało to wydatki wojskowe z budżetu państwa w wysokości 42% (w stosunku do wydatków administracyjnych) lub 23,4% (w stosunku do wydatków ogólnopaństwowych). Za: P. Stawecki, *Polityka wojskowa Polski*..., s. 175.

[40] *Rocznik Statystyczny Rzeczypospolitej Polskiej 1920–1922*, cz. II, Warszawa 1923, s. 263.

[41] Por. R. Szeremietiew, *W obcym interesie*, Warszawa–Kościan 1991, s. 24–27.

[42] Teoretycznie niepowodzenie pochodu Tuchaczewskiego za Wisłę oraz towarzyszących mu inicjatyw politycznych (jak np. utworzenie 30 VII 1920 r. Tymczasowego Komitetu Rewolucyjnego Polski) powinny zmienić to nastawienie, jednak w RKP(b) plany wywołania rewolucji w II RP i w Niemczech były żywe do – minimum – 1923 r., kiedy nadzieje na realizację tego planu zgasły wraz z niepowodzeniem rewolucji niemieckiej.

Z kolei ostra walka polityczna wśród ówczesnych polskich elit, wzmacniana oskarżeniami o korupcję kierowanymi wobec partii rządzących (szczególnie wobec PSL „Piast”[43]) oraz działalnością terrorystyczną niektórych ugrupowań[44] sprawiały, że w ocenie planistów sowieckiego wywiadu wojskowego należało się liczyć z możliwością wybuchu wojny domowej, zwłaszcza gdyby doszło do poważnej prowokacji politycznej.

Oceny sowieckich sztabowców były przy tym tożsame z opiniami Lenina, który w liście do KPRP z 19 października 1921 r. wskazywał na niepowodzenie reformy rolnej, krach finansów RP oraz wrzenie chłopstwa, głównie na Kresach, jako na czynniki sprzyjające rewolucji[45]. Oznaczało to, że analizy wywiadowcze odbijały oficjalne stanowisko Sowdepii i, co za tym idzie, stawały się wykładnią strategii działań wobec RP uznaną przez władze sowieckie. Ta strategia została też przyjęta za sprawą ustaleń III Zjazdu KPRP, który za punkt wyjścia przewrotu uznał rewolucjonizowanie się mas robotniczych pod wpływem pogarszającej się sytuacji ekonomicznej i mas chłopskich w walce o ziemię oraz wrzenie na Kresach Wschodnich[46].

Plan destabilizacji państwa polskiego

Sowieckie służby specjalne, które dążyły do zdestabilizowania sytuacji politycznej II RP, musiały brać pod uwagę ryzyko, że w razie przekształcenia się operacji dywersyjno-terrorystycznej w otwarty konflikt między dwoma państwami zachodnie mocarstwa, odbudowawszy część potencjału utraconego w czasie wojny, mogą się zdecydować na interwencję zbrojną przeciwko ZSRS. Nawoływały do tego organizacje białogwardyjskie[47] oraz europejskie sztaby generalne rozważające wojnę prewencyjną jako środek na zakończenie *bolszewickiego zagrożenia*[48]. Działania przeciwko RP musiały więc być prowadzone tak, aby uderzać w podstawy funkcjonowania państwa, ale zarazem bez ściągania na słabą jeszcze Rosję zagrożenia interwencją koalicji państw zachodnich oraz resztek armii białych przebywających na ich terytorium i gotowych do przejęcia władzy po obaleniu bolszewickiego reżimu. Rosja Sowiecka była zmuszona prowadzić grę w taki sposób, żeby nie sprowokować zdecydowanej odpowiedzi Zachodu, który bardzo dobrze zdawał sobie sprawę z jej słabości i mógł wykorzystać ewentualną wojnę z Polską jako pretekst do szerszej interwencji. To mogło bowiem oznaczać koniec sowieckiego reżimu i restaurację dawnego porządku. Sowiecki wywiad stał więc przed zadaniem niezwykle trudnym: musiał prowadzić działania terrorystyczno-dywersyjne, chwilami sięgając do insurekcji mniejszości narodowych w warunkach

[43] Najbardziej znanymi, chociaż nie jedynymi aferami tego typu, były np.: sprawa dotycząca spółek powołanych przez członków PSL „Piast”, które wykorzystując swoje wpływy w ministerstwach, zawierały kontrakty na wyrąb lasów państwowych po wyjątkowo niskich cenach, czy też sprawa majątku Dojlidy, kupionego przez należący także do PSL „Piast” polsko-amerykański Bank Ludowy za zgodą Głównego Urzędu Ziemskiego za 75 mln marek polskich i natychmiast odsprzedanego ks. Lubomirskiemu za 410 mln marek polskich. O tych aferach informował z trybuny sejmowej poseł Stapiński w 1922 r. Zob. A. Próchnik, *Pierwsze piętnastolecie Polski Niepodległej (1918–1933)*, Warszawa 1933, reprint – Warszawa 1957, s. 124.

[44] Najjaskrawszym przykładem działalności terrorystycznej była aktywność Narodowej Demokracji (Endecji), zwłaszcza w okresie poprzedzającym zabójstwo prezydenta Gabriela Narutowicza oraz w czasie późniejszego fetowania jego zabójcy.

[45] J. Kowalski, *Zarys historii polskiego ruchu robotniczego 1918–1939*, Warszawa 1962, s. 209.

[46] J. Kowalski, *Zarys historii*…, s. 216.

[47] Głównie organizacja gen. P. Wrangla zachowująca strukturę wojskową, która powstała po ewakuacji armii białej z Krymu w 1920 r.

[48] R. Wraga, *Trust*, „Kultura” 1949, nr 4/21–5/22, s. 158–159.

konfliktu asymetrycznego charakterystycznego dla dzisiejszych czasów[49] (gdyż uderzenie koalicji państw zachodnich, Polski oraz armii gen. Wrangla łatwo mogłoby zniszczyć wciąż słabe i zacofane państwo sowieckie[50]).

Aktywność sowieckiego wywiadu stojącego za skrytym atakiem na Polskę[51] przejawiała się następująco: po pierwsze, zintensyfikowano[52] zmasowaną akcję propagandową skierowaną zarówno do Polaków (głównie robotników i szeregowych żołnierzy), jak i (w większym stopniu) do mniejszości narodowych zamieszkujących ówczesne Kresy Wschodnie (w nomenklaturze sowieckiej – zachodnią Ukrainę i zachodnią Białoruś). Dyskredytowano w niej instytucje państwa polskiego oraz nawoływano do oporu przy wykorzystaniu haseł rewolucyjnych[53]. Za realizację tych działań była odpowiedzialna utworzona w grudniu 1918 r. KPRP[54]. Przyjęcie przez KPRP tzw. 21 warunków III Kominternu[55] oznaczało między innymi obowiązek prowadzenia systematycznej pracy politycznej w wojsku[56] i wśród ludności cywilnej. KPRP (w 1924 r. przemianowana na KPP) stała się zatem narzędziem masowej propagandy antypaństwowej[57], którą kierowała Rosja Sowiecka. O powadze tego zagrożenia świadczy zarówno skala policyjnych represji wobec działaczy komunistycznych[58], jak i dynamika kulturalno-oświatowej działalności (czyli de facto propagandy antykomunistycznej) w Wojsku Polskim, o ile w 1919 r. w armii przeprowadzano 500 odczytów i pogadanek miesięcznie, to już w 1921 r. było ich 7 tys.[59] Warto dodać, że propaganda komunistyczna była prowadzona nie tylko w sposób nielegalny (tj. przez kolportaż ulotek i druków), lecz także przez

[49] Warto zauważyć, że Federacja Rosyjska w czasie obecnych działań prowadzonych przeciwko Ukrainie stoi przed identycznym wyzwaniem.

[50] W latach 1920–1921 produkcja przemysłowa w stosunku do roku 1913 spadła o 82% (w przemyśle metalurgicznym, istotnym na wypadek wojny, produkcja wynosiła 6% stanu z 1914 r.), wydajność pracy o 74%, zaś produkcja zbóż o 40%. Populacja miejska drastycznie zmniejszyła się (zwłaszcza w ośrodkach miejskich w północnej Rosji, zaopatrywanych w żywność przez południe kraju): liczba mieszkańców Piotrogrodu spadła o 70%, a Moskwy o 50%. Liczebność nierolniczej siły roboczej zmniejszyła się z 3,6 mln osób w 1917 r. do 1,5 mln. Towarzyszyły temu spadek o 1/3 płacy realnej robotników przemysłowych; R. Pipes, *Rosja bolszewików*…, s. 374–375, por. D. Koenker, W.G. Rosenberg, R.G. Suny, *Party, State, and Society*…, s. 58–61.

[51] Należy zauważyć, że choć zasadnicze zręby operacji były opracowane przez wywiad wojskowy, to wywiad cywilny GPU także odegrał w nich istotną rolę.

[52] Działalność propagandowa była bowiem prowadzona bezustannie. Jak donosił „Kurier Warszawski" z 29 kwietnia 1919 r.: *Bandy wschodnie pudami rozsypują przy odwrocie literaturę agitacyjną. Nie brak też i wewnątrz kraju zakonspirowanych wydawnictw i broszur, mających sączyć jad i gangrenę w szeregi...*

[53] Por. J. Kowalski, *Zarys historii*…, s. 154.

[54] Komunistyczna Partia Robotnicza Polski powstała ze zjednoczenia DSKPiL i PPS-Lewicy, które od zarania swej działalności wyrażały niechętny stosunek do kwestii narodowej. Por. R. Szeremietiew, *W obcym interesie*…, s. 8–14.

[55] Komintern (*Komunisticzeskij Internacjonał* – Międzynarodówka Komunistyczna) był organizacją zrzeszającą partie komunistyczne, założoną w Moskwie w marcu 1919 r. Jego celem było doprowadzenie do światowej rewolucji. Partie członkowskie musiały się zobowiązać do wspierania Rosji Sowieckiej oraz prowadzenia legalnej i nielegalnej walki o przejęcie władzy w swoich krajach. Komintern de facto był instrumentem umożliwiającym władzom Związku Sowieckiego wpływanie na politykę we wszystkich krajach członkowskich i ułatwiającym działalność sowieckiego wywiadu.

[56] I. Pawłowski, *Polityka i działalność wojskowa KPP 1918–1928*, Warszawa 1964, s. 31.

[57] Co ciekawe, ówcześni komuniści nie skrywali otwarcie antypolskiego, prosowieckiego charakteru działalności. Jak pisał „Czerwony Sztandar" (1920, nr 5: *Byliśmy i jesteśmy jedyną partią obrońców Sowieckiej Rosji...*).

[58] Dla ilustracji – po zamachu na prochownię w Cytadeli Warszawskiej polskie władze aresztowały ponad dwa tysiące działaczy komunistycznych podejrzewanych nie tylko o związki z nielegalną KPP, lecz także z agendami sowieckiego wywiadu. Por.: I. Pawłowski, *Polityka i działalność...*, s. 38.

[59] Tamże, s. 13.

wydawanie legalnie działającej prasy codziennej[60]. W celu zobrazowania skali tego zjawiska warto zaznaczyć, że np. w 1924 r. Centralna Technika KPP wydała 222 wydawnictwa nielegalne o nakładzie 1 881 500 egzemplarzy.

Z kolei w ocenie toruńskiego DOK we wrześniu 1923 r. aż 28 proc. oddziałów WP było obsadzonych przez komunistycznych agitatorów, a kompletna obsada personalna jaczejek komunistycznych w WP miała być ukończona dopiero w 1924 r.[61]

Po drugie, przez granicę masowo przerzucano prowokatorów, dywersantów, agitatorów i wreszcie szpiegów Polaków z zadaniem infiltrowania struktur wojskowo-administracyjnych państwa polskiego[62]. Wykorzystywano w tym celu nieudolną politykę imigracyjną młodego państwa, które bez jakichkolwiek procedur sprawdzających przyjmowało rzesze repatriantów ze Wschodu[63]. Oprócz zaskakująco liberalnej polityki pomagał w tym także chaos organizacyjny polskiego MSZ. Placówki w Rosji Sowieckiej miały (zwłaszcza w początkowym okresie funkcjonowania) charakter półoficjalny. Wystawiały więc różne wzory „kart legitymacyjnych" osobom deklarującym, że są Polakami. Pracownicy Państwowego Urzędu do Spraw Powrotu Jeńców, Uchodźców i Robotników nie byli w stanie zweryfikować tych kart (gdyż nie znali obsady personalnej polskich placówek, a więc i podpisów) oraz prawdziwości zawartych w nich informacji. Dopiero po 1924 r. do polskich władz dotarło, że dzięki temu do kraju przedostawali się dywersanci i działacze komunistyczni[64]. Polskie władze nie robiły przeszkód nawet Polakom żołnierzom RKKA albo funkcjonariuszom WCzeKa, pragnącym wrócić do kraju[65]. Na terenach przygranicznych za sprawą masowo przerzucanych sowieckich agentów na ogromną skalę powstawały siatki szpiegowskie, do których należała okoliczna ludność (bez względu na jej realne możliwości wywiadowcze), głównie po to, aby przygotować teren przygraniczny do działań dywersyjnych na wypadek wojny[66].

Po trzecie, za sprawą wyżej opisanej akcji propagandowej i grup bojowych (zarówno operujących na terytorium polskim, jak i działających z terenu Rosji Sowieckiej) sprowokowano wybuch powstania na Kresach, które mimo braku znaczących operacji wojskowo-partyzanckich doprowadziło do przejściowego paraliżu polskiej administracji na tych terenach oraz zdemoralizowania policji i formacji granicznych[67]. W celu

[60] Wydawano tytuły niepozwalające na jednoznaczną afiliację z KPP, np. „Trybuna Robotnicza", „Kultura Robotnicza" itp.

[61] I. Pawłowski, *Polityka i działalność*..., s. 172.

[62] Por. opis działalności KPP w Wojsku Polskim w: I. Pawłowski, *Polityka i działalność*..., J. Kowalski, *Zarys historii*..., s. 280.

[63] Do zakończenia negocjacji do RP powróciło 500 tys. osób, po czym, w okresie masowej repatriacji (wiosna–jesień 1921 r.) do kraju przyjechało dalszych 370 tys. osób. Zob. W. Materski, *Tarcza Europy*..., s. 90.

[64] W. Skóra, *Organizacja i działalność służby konsularnej Drugiej Rzeczypospolitej na terenach Rosji, Ukrainy i ZSRR w dwudziestoleciu międzywojennym (1918–1939)*, w: *Stosunki polityczne, wojskowe i gospodarcze Rzeczypospolitej Polskiej i Związku Radzieckiego w okresie międzywojennym*, J. Gmitruk, W. Włodarkiewicz (red.), Warszawa–Siedlce 2012, s. 268–271.

[65] Z książki Z. Iwańczuka, *Na granicy epok. Wspomnienia o udziale Polaków w Rewolucji Październikowej i wojnie domowej w Rosji 1917–1921* (Warszawa 1967) wynika, że ze 103 komunistów aktywnie uczestniczących w rewolucji 66 powróciło do RP.

[66] Por. A. Pepłoński, *Kontrwywiad II Rzeczypospolitej*, Warszawa 2002, s. 171.

[67] Tamże, s. 145 i in. Przykładem szokującej bezkarności sowieckich terrorystów był tzw. atak na Stołpce. W nocy z 3 na 4 VIII 1924 r. oddział dywersyjny, którego liczebność szacuje się na 50–150 osób, przedostał się do RP z terenu ZSRS i dołączył do gromadzących się mniejszych grup partyzanckich. Po przeprowadzonej koncentracji zgrupowanie zaatakowało Stołpce. Wskutek ataku została zniszczona komenda Policji Państwowej, podpalono dworzec kolejowy i budynek starostwa, a także zdewastowano i ograbiono wszystkie sklepy i magazyny handlowe. Uwolniono 150 więźniów – przede wszystkim przywódców Komunistycznej Partii Zachodniej Białorusi Josifa K. Loginowicza i Stanisława Mertensa.

skuteczniejszego oddziaływania na ludność zamieszkującą obszary objęte walkami wykreowano romantyczno-mityczną postać rzekomego dezertera z WP, Józefa Muchy-Michalskiego, który walcząc z Polakami, łączył w sobie cechy bohatera hajdamackiego i propagandy bolszewickiej. Jak pisał M. Rataj:

> (…) granica otwarta, bandy Muchy grasują jawnie w biały dzień. Policja nie wystarcza, źle rozmieszczona, zdemoralizowana przechodzi do bolszewików. Ludność, widząc bezkarność, traci zaufanie do siły państwa polskiego[68].

Dopiero zmilitaryzowanie administracji kresowej, utworzenie KOP[69] oraz wykorzystanie WP w tzw. akcjach asystencyjnych (czyli w pacyfikacjach wsi wymierzonych w likwidację komórek komunistycznych i oddziałów partyzanckich) przyniosły względny spokój na Kresach. Do 1939 r. ten obszar był jednak masowo infiltrowany zarówno przez wywiad sowiecki, jak i zakonspirowane komórki partyjne (do 1938 r. KPZU i KPZB) kierowane bezpośrednio z Moskwy.

Po czwarte, przeprowadzono serię ataków bombowych w centralnej Polsce, w tym na strategiczne cele wojskowe, np. na prochownię w Cytadeli Warszawskiej[70]. Ta akcja była koordynowana przez poselstwo sowieckie w Warszawie, które nie tylko organizowało ataki, posługując się lokalnymi strukturami KPRP, lecz także dostarczało materiały wybuchowe przywożone do Warszawy z Berlina[71].

Po piąte, próbowano wpływać na polską scenę polityczną przez zarówno probolszewickie ugrupowania, partie i frakcje sejmowe, jak i opozycję pozaparlamentarną[72]. Warto przypomnieć, że od 1921 r. KPRP wchłaniała mniejsze ugrupowania lewicowe (np. tzw. Komunistyczny Bund), rozszerzając w ten sposób swoje wpływy. W kolejnym roku partia wzięła udział w wyborach do sejmu i utworzyła legalny Związek Proletariatu Miast i Wsi, który zdobył 132 tys. głosów. To ugrupowanie wprowadziło do sejmu swoich przedstawicieli[73], którzy pod ochroną immunitetu poselskiego mogli odtąd realizować cele polityczne wysuwane przez Komintern (a więc – pośrednio – GPU). Komunistyczna Frakcja Poselska w Sejmie współpracowała także z innymi partiami o wyraźnie probolszewickim charakterze, jak np. z Niezależną Partią Chłopską[74] i Białoruską Włościańsko-Robotniczą Hromadą[75].

Po szóste, zgodnie z tezą Lenina o konieczności infiltrowania przez komunistów legalnie działających organizacji burżuazyjnych[76], przedstawiciele KPRP i agitatorzy byli wprowadzani do związków zawodowych, kas chorych, rad miejskich, organizacji spółdzielczych, Uniwersytetu Ludowego, Stowarzyszenia Wolnomyślicieli Polskich, wojska, Strzelca itp.[77]

---

[68] M. Rataj, *Pamiętniki*, Warszawa 1965, s. 208.

[69] Decyzję o utworzeniu KOP podjęto podczas specjalnego posiedzenia Rady Ministrów w dniach 21–22 VIII 1924 r. W dniu 12 IX 1924 r. Ministerstwo Spraw Wojskowych wydało rozkaz o utworzeniu Korpusu Ochrony Pogranicza, a pięć dni później w instrukcji opracowanej przez Sztab Generalny Wojska Polskiego określono wojskową strukturę tej formacji.

[70] Celami ataku były m.in. Kraków, Warszawa i Białystok. Zob. R. Juryś, *Kulisy wielkiej prowokacji*, Warszawa 1960, s. 11.

[71] G.Z. Biesiedowski, *Pamiętniki dyplomaty sowieckiego*, Katowice, bdw.

[72] Por. działania KPP i partii pokrewnych (m.in. Niezależnej Partii Chłopskiej, Białoruskiej Włościańsko-Robotniczej Hromady).

[73] J. Kowalski, *Zarys historii*…, s. 222.

[74] Utworzona w 1924 r. przez byłych posłów PSL „Wyzwolenie".

[75] Utworzona w 1925 r. przez byłych członków Białoruskiego Klubu Poselskiego.

[76] W.I. Lenin, *Dzieła wybrane*, t. II, Warszawa 1951, s. 669.

[77] Por.: J. Kowalski, *Zarys historii*…, s. 277.

Po siódme, agitatorzy KPRP namawiali robotników do zwiększania żądań i przygotowywali strajki w celu wywołania zamieszek i politycznej radykalizacji konfliktów o charakterze ekonomicznym. Trzeba nadmienić, że było to łatwe zadanie w związku z katastrofalnym stanem gospodarczym państwa polskiego, które nie potrafiło poradzić sobie z bezrobociem i brakiem finansów. To często prowadziło do zaostrzenia sytuacji i interwencji Policji Państwowej i wojska[78].

Po ósme, prowadzono kampanię mającą na celu zastraszenie polskich organów ścigania, dokonując zamachów na policyjnych prowokatorów, których kierownictwo KPRP słusznie uważało za największe zagrożenie w sytuacji, gdy ruch komunistyczny był nastawiony na pozyskiwanie nowych członków, wprowadzanych następnie w tajniki działalności partyjnej. Najbardziej znane były zamachy na prowokatorów policyjnych Kamińskiego (6 lutego 1925 r.)[79] oraz Cechnowskiego (pierwszy – nieudany – 17 lipca 1925 r. i drugi – zakończony jego śmiercią – 28 lipca 1925 r.)[80].

Po dziewiąte, sfingowano napad sowieckich agentów przebranych za działaczy endeckiej bojówki na dwór w Sulejówku z zamiarem zamordowania J. Piłsudskiego[81]. Sztab RKKA sądził, że wywoła to wojnę domową. Do zrealizowania planu jednak nie doszło. Sowiecki dyplomata uciekinier G. Biesiedowski utrzymywał w swoich wspomnieniach, że odstąpiono od niego po interwencji Feliksa Dzierżyńskiego, którego miał oburzyć zamiar skrytobójczego zamordowania Marszałka. Z uwagi jednak na biografię Żelaznego Feliksa ciężko zaakceptować myśl o odrzuceniu przez niego planu wywołania rebelii w imię ideałów kojarzonych z burżuazyjną wykładnią moralności, ale do zamachu istotnie nie doszło. Rzeczywiste przyczyny rezygnacji przez Razwiedupr z prowokacji pozostają nieznane.

Wnioski

Z powyższego, nieco pobieżnego przeglądu działań podejmowanych przez państwo sowieckie wobec Rzeczpospolitej na początku lat 20. XX w. wynika kilka wniosków:

1. Założenia tego, co obecnie jest nazywane wojną hybrydową, były wypracowane przez Razwiedupr i GPU na podstawie tez politycznych wysuniętych przez sowieckie kierownictwo, które traktowało swoje oceny jako oczywistą analizę sytuacji zachodniego sąsiada i wykorzystywało je m.in. w wojnie informacyjnej (czyli wielokanałowej propagandzie), będącej częścią tego, co dziś nazywamy wojną hybrydową[82].
2. Wszystkie działania realizowane wówczas przez różnego rodzaju agendy sowieckiego rządu, choć obejmowały tak drastyczne metody, jak częste przeprowadzanie zamachów bombowych, mordowanie funkcjonariuszy i współpracowników polskich organów ścigania oraz sprowokowanie insurekcji opartej na napięciach

[78] Najbardziej spektakularnym przykładem są tzw. wypadki krakowskie, tj. zamieszki trwające od nocy z 5 na 6 do 7 listopada 1923 r., które były w dużym stopniu sprowokowane przez nieudolność władz porządkowych. Zginęło w nich 18 osób cywilnych (w tym 15 robotniczych demonstrantów) i 14 żołnierzy, a robotnikom udało się rozbroić niemal 400 żołnierzy i policjantów, zdobywając dużą ilość broni oraz samochód pancerny. Szerzej zob.: T. Marszałkowski, *Zamieszki, ekscesy i demonstracje w Krakowie 1918–1939*, Kraków 2015.

[79] J. Kowalski, *Zarys historii*…, s. 316.

[80] R. Juryś, *Kulisy wielkiej prowokacji*, Warszawa 1960, s. 145, 160.

[81] G.Z. Biesiedowski, *Pamiętniki dyplomaty*…, s. 153–155.

[82] To przypomina obecną sytuację na Ukrainie, w której rząd rosyjski głosi tezy będące podstawą operacji propagandowych i zarazem uzasadnieniem działań separatystów w Zagłębiu Donieckim.

narodowościowo-ekonomicznych panujących na terenach przygranicznych, były elementami składowymi sowieckiej polityki, która konsekwentnie realizowała założenia wynikające z trzeźwych ocen własnych możliwości militarno-politycznych i postrzegania przez Sowdepię własnych interesów geopolitycznych.

3. Chociaż w prowadzonych działaniach wykorzystywano oddziaływanie militarne, wikłając Polskę w quasi-powstańczą, partyzancką wojnę na Kresach, to tak naprawdę służyło to podstawowemu celowi geopolitycznemu, tj. destabilizacji polskich struktur państwowych. Celem aktywności partyzanckich band (czyli ugrupowań złożonych z dywersantów przenikających przez granicę oraz członków lokalnych struktur komunistycznych) nie było oderwanie tych ziem od RP. Należy pamiętać, że podczas rokowań ryskich sowiecka delegacja proponowała stronie polskiej znacznie większe koncesje terytorialne na Wschodzie niż ostatecznie zostały uzgodnione. Wynikało to z zaleceń Lenina, aby wciągnąć Polskę w pułapkę konfliktu z zamieszkującymi te ziemie narodami, kulturowo i religijnie ciążącymi ku republikom wchodzącym w skład Rosji Sowieckiej, a przy tym, wskutek zapóźnienia i biedy, podatnymi na sowiecką propagandę. Trudno też było założyć, że zamachy bombowe (nawet tak poważne, jak wysadzenie prochowni w Cytadeli Warszawskiej) mogły mieć odczuwalny skutek w postaci osłabienia polskiego potencjału wojskowego lub też że mordowanie policyjnych agentów sparaliżuje działania polskich organów ścigania. Wszystkie te czynniki były bowiem podporządkowane głównemu celowi (który później, w latach 70. XX w., przyświecał lewackiemu terroryzmowi w Europie Zachodniej): sprowokowaniu państwa ofiary do brutalnych działań represyjnych uderzających w mniejszości narodowe i klasy pracujące. Taki krok miał obnażyć opresyjny charakter władzy, co z kolei miało doprowadzić do delegitymizacji młodego państwa. Innymi słowy, sowiecka aktywność zmierzała do przeciwstawienia aparatu państwowego II RP wieloetnicznemu społeczeństwu, dzięki czemu spodziewano się na tyle poważnych wstrząsów społecznych, aby utorować drogę do władzy ugrupowaniom sprzyjającym Rosji Sowieckiej, a dysponującym zbyt małym poparciem wśród ludności, by przejąć władzę w ramach zwykłych procedur demokratycznych. W pewnym sensie Sowieci w Polsce usiłowali powtórzyć sytuację, która w 1917 r. przyniosła sukces bolszewikom: skompromitować aparat państwa, wprowadzić chaos polityczny wywołany walką partii, stronnictw i koterii partyjnych, doprowadzić do kryzysu gospodarczego, którego koszty klasy rządzące przerzuciłyby na grupy ludności ekonomicznie słabe, i wreszcie zasiać poczucie niepewności jutra, tymczasowości i kompromitacji legalnej władzy. Należy zakładać, że to rozciągnięte w czasie oddziaływanie na polskie społeczeństwo, mające doprowadzić do władzy liczebnie słabą KPRP, było skutkiem niepowodzenia taktyki z 1920 r., czyli przeniesienia rewolucji do Polski na bagnetach RKKA. Fałsz założeń stojących za tą koncepcją chyba najlepiej ocenił J. Piłsudski, pisząc:

> Zapytać jednak wolno, czy nie ma jakiego błędu w rachunkach i kalkulacjach p. Tuchaczewskiego? Gdy po zwycięstwach jego odniesionych nad nami, praca budownictwa u nas, pod wpływem tych zwycięstw, zamarła, gdy rękę swą wyciągał już po centrum naszego życia, stolicę Warszawę, gdy więc bagnety zrobiły już swoje, rewolucja sowiecka jednak pozostała tylko na bagnetach, nie mając wtedy wartości wewnętrznej w Polsce.

A przecie cały rachunek p. Tuchaczewskiego i jego państwa nie na czym innym się opierał, jak na tym, że bagnety dają tylko hasło i dają możność przejawienia siły tejże rewolucji sowieckiej wewnątrz kraju, do którego przyszły[83].

4. Sowieci, zrozumiawszy w 1920 r., że nie mogą liczyć na wybuch polskiej rewolucji pod wpływem sytuacji na froncie (gdyż do powstania nie doszło, mimo zbliżania się do Warszawy Armii Czerwonej), zrobili to samo, co Austriacy przed I wojną światową. Po wojnie w Bośni i Hercegowinie wywiad austriacki zaczął wywierać wpływ na wrogie państwo za pośrednictwem partii opozycyjnej[84]. Sowieci postawili zatem na KPRP, zakładając, że w sytuacji kompromitacji instytucji państwowych sprowokowany wybuch społecznego niezadowolenia doprowadzi do przejęcia władzy przez tę partię i powoła ona w Warszawie rząd, którego polityka trwale zwiąże Polskę z Rosją Sowiecką.
5. Komunistyczna Partia Robotnicza Polski, która w myśl powyższych założeń miała stać się reprezentantem interesów sowieckich w Polsce, miała kilka cech, które predestynowały ją w oczach Sowdepii do odegrania napisanej dla niej roli, ale też i kilka takich, które uniemożliwiły jej zrealizowanie założonego scenariusza. KPRP była bowiem kontynuatorem długiej linii lewicowej myśli politycznej odrzucającej walkę o niepodległość Polski: Socjaldemokracja Królestwa Polskiego (potem SDKPiL) już w 1894 r. powtórzyła tezy Socjalno-Rewolucyjnej Partii „Proletaryat", uznając za swe historyczne zadanie (...) *by proletariat polski nie brał na swe barki niepodległości Polski*[85]. Działaczka SDKP Róża Luksemburg pisała: (...) *niech nam dadzą spokój z niepodległą Polską*[86]. Pod jej wpływem SDKPiL przyjął, że celem partii jest jedynie autonomia, (...) *gdyż Polska stanowi realną część Rosji, a niepodległość Polski jest szkodliwa dla międzynarodowej rewolucji socjalnej*[87]. KPRP od momentu powstania przyjęła te założenia, odrzucając problemy samookreślenia, niepodległości i granic[88]. Realizowano też od początku plan zbrojnego przejęcia władzy. W tym celu zorganizowano Czerwoną Gwardię i wywoływano bunty w wojsku, z których najbardziej znana była próba opanowania Zamościa przez żołnierzy 35 Pułku Piechoty[89]. Po klęsce Armii Czerwonej na przedpolach Warszawy, pomimo zdecydowanej akcji władz porządkowych (które przeprowadziły masowe aresztowania zarówno na tyłach wojsk polskich, jak i na terenach opuszczonych przez Sowietów, gdzie ujawniły się komórki komunistyczne w postaci Komitetów Wojenno-Rewolucyjnych i grupy podatne na bolszewicką propagandę, dołączające do przejmowania folwarków i fabryk[90]) aktywność KPRP bardzo szybko zaczęła powtórnie rosnąć. Już w 1921 r. II Kongres Kominternu uznał, że wybuch rewolucji światowej jest bliski, a więc konieczne było usunięcie przeszkody na drodze komunizmu na zachód Europy. W tym celu należało wykorzystać wszelkie możliwe metody[91],

[83] J. Piłsudski, *Rok 1920*, Gdańsk 1989, s. 147.
[84] *Pamiętniki generała Rybaka*, Warszawa 1954, s. 10.
[85] R. Szeremietiew, *W obcym interesie*..., s. 8.
[86] Tamże, s. 9.
[87] Tamże, s. 11.
[88] Tamże, s. 14.
[89] Tamże, s. 18.
[90] J. Kowalski, *Zarys historii*..., s. 161.
[91] R. Szeremietiew, *W obcym interesie*..., s. 27.

m.in. wdrożyć wcześniej opisane działania sowieckiego wywiadu. KPRP nie potrafiła jednak przejąć władzy, mimo wyjątkowo trudnej sytuacji polityczno-ekonomicznej, w której znajdowała się RP. Można zaryzykować stwierdzenie, że sowiecka działalność dążąca do poderwania autorytetu władzy, osłabienia instytucji państwowych i generowania społecznego buntu do pewnego stopnia utorowała drogę J. Piłsudskiemu, zamiast pozwolić polskim komunistom na przejęcie władzy na fali społecznego niezadowolenia. Partia wybrana przez Sowdepię do kierowania młodym państwem polskim miała bowiem kilka cech, które niezwykle utrudniały realizację tego celu. Po pierwsze, deklarowała ona charakter robotniczy, choć w 60 proc. składała się z inteligencji i tylko w 10 proc. z robotników[92]. Po drugie, mianowała się ugrupowaniem polskim, a w ponad 60 proc.[93] należały do niej osoby o narodowości innej niż polska. Po trzecie zaś, KPRP nie potrafiła wystarczająco szybko zająć odpowiedniego stanowiska w starciu między Lwem Trockim a Józefem Stalinem. To oznaczało, że w polskim społeczeństwie, w większości chłopskim (a więc tradycyjnie religijnym, antysemickim i zachowawczym) hasła KPRP nie mogły znaleźć szerokiego oddźwięku[94]. Z tego powodu w 1923 r., czyli w szczycie akcji strajkowej i kryzysu ekonomicznego, wspomniana partia miała zaledwie 5193 członków[95]. Nie była to duża liczba, więc nie miała ona dużej możliwości dotarcia do mas ludowych. Dodatkowym elementem były zapewne problemy w nawiązywaniu kontaktu z owymi masami w sytuacji, gdy KPRP składała się głównie z inteligentów, językowo i kulturowo obcych ludziom, do których starali się trafić ze swoimi hasłami[96]. W dodatku KPRP, niewystarczająco szybko opowiadając się po stronie Stalina, stała się *ex definitione* podejrzana dla Moskwy. To ostatecznie doprowadziło do jej likwidacji w 1938 r. i utworzenia cztery lata później PPR, która nie powtórzyła już błędów ideologicznych swojej poprzedniczki i włączyła w swoje działania propagandowe patriotyczną frazeologię[97]. Otwarte pozostaje pytanie: Dlaczego w II RP w 1923 r. nie doszło do komunistycznego powstania, choć wybuchło ono w wielu innych krajach? Nakreślona wyżej charakterystyka narodowościowo-klasowa partii mającej odegrać rolę zapalnika niepokojów społecznych pozwala jednak zrozumieć, chociażby częściowo, przyczynę niepowodzenia sowieckiej strategii.

Zakończenie

Przedstawiony powyżej mechanizm destabilizacji II RP przez sowieckie służby z pewnością nie wyczerpuje tematu, skupia się jedynie na najbardziej znanych wydarzeniach i procesach historycznych. Pozwala jednak wyciągać wnioski na temat podobnych działań, realizowanych w dzisiejszych czasach, w ramach analizy porównawczej. Może

[92] Tamże, s. 55.

[93] Tamże, s. 56.

[94] Por.: J.A. Reguła, *Historia Komunistycznej Partii Polski w świetle dokumentów i faktów*, Toruń 1994, s. 56–57.

[95] J. Kowalski, *Zarys historii...*, s. 277.

[96] Dobrym przykładem takiego zjawiska może być manifest tzw. republiki Litbiełu, utworzonej przez Sowietów na zajętych terenach Litwy, wydany nie w języku litewskim, ale w polskim i w jidysz.

[97] R. Szeremietiew, *W obcym interesie...*, s. 59. Warto zaznaczyć, że zapewne m.in. dzięki temu PPR – w przeciwieństwie do KPRP i KPP – bardzo szybko stał się organizacją masową i liczył w 1948 r. ponad milion członków.

najistotniejszą konstatacją płynącą z powyższych rozważań jest spostrzeżenie, że akcje quasi-militarne są tylko niewielką częścią tego, co obecnie jest nazywane wojną hybrydową. Tego typu konflikt jest szerokim spektrum działań zmierzających do osiągania strategicznych celów geopolitycznych metodami jawnymi i niejawnymi w sytuacji, gdy państwo oddziałujące jest za słabe, aby ryzykować otwartą wojnę, a państwo ofiara nie dysponuje wystarczającymi zasobami, żeby uznać ukrytą agresję państwa oddziałującego za *casus belli*[98].

II Rzeczpospolita wytrzymała nacisk ze strony ZSRS przez kilkanaście lat, ale wszystkie stosowane przez nią środki obronne miały charakter wyłącznie reaktywny, co przesądziło o ostatecznym rezultacie tego starcia. Polskie władze walczyły z destabilizowaniem państwa, używając głównie metod policyjnych. Nie dostrzegały tego, że pozostawiając Rosji Sowieckiej inicjatywę i jedynie odpowiadając na kolejne prowokacje, pozycja państwa stale się osłabiała. Przez całe dwudziestolecie międzywojenne nie udało się wytworzyć takiego systemu sojuszy polityczno-wojskowych, które pozwoliłyby państwu polskiemu na przejęcie polityczno-militarnej inicjatywy i odwrócenie ról, co zmusiłoby ZSRS do rezygnacji z agresywnej polityki na rzecz działań defensywnych. W starciu ze służbami specjalnymi przeciwnika przyjęcie strategii reaktywnej nie może przynieść korzystnych rezultatów, a co najwyżej może zablokować działania wrogiej służby. Ta zaś, nawet nie realizując przejściowo swoich celów, bez końca może podejmować próby i stosować coraz bardziej skuteczne metody dzięki rozpoznawaniu możliwości obronnych państwa ofiary.

Takie właśnie zjawisko zaszło w dwudziestoleciu międzywojennym. Sowieci, którzy realizowali długofalowy plan destabilizacji państwa polskiego, wykorzystywali wszystkie dostępne narzędzia – od środków dywersyjno-terrorystycznych i quasi-militarnych, przez zmasowaną propagandę antypolską w RP i na Zachodzie Europy[99] aż po zakulisowe działania polityczne. W ich rezultacie już od 1922 r. Polska stanęła przed nierozwiązywalnym problemem sojuszu dwóch państw sąsiadujących, pod każdym względem przewyższających potencjałem wojskowo-gospodarczym możliwości słabego ekonomicznie państwa polskiego. Jedynym wyjściem było zbudowanie takiego systemu sojuszy, który pozwoliłby II RP na przejęcie inicjatywy i aktywną realizację dalekosiężnych planów Marszałka. Piłsudski chciał wykorzystać sowieckie „bezhołowie" i ucisk do – jak mawiał – rozdarcia ZSRS po narodowych szwach, w sytuacji, gdy Rosja Sowiecka nie mogłaby odpowiedzieć wypowiedzeniem wojny na agresywne działania służb specjalnych. Tylko zdecydowane osłabienie ZSRS i uwikłanie go w działania defensywne mogło gwarantować zaprzestanie przez sowietów podejmowania prób destabilizacji zachodniego sąsiada.

Jednak słabość II RP stawiała państwo polskie w sytuacji pasywnego obiektu coraz bardziej agresywnych działań wschodniego sąsiada, który w 1939 r. w końcu zrealizował pierwotne założenia i zlikwidował je, a następnie – przekształcił w satelitę Moskwy aż do rozpadu sowieckiego imperium.

[98] Z tego powodu w obecnym konflikcie w Donbasie Ukraina, choć otwarcie deklaruje, że na terytorium Donbasu operują oddziały regularnej armii rosyjskiej, do dziś nie potraktowała tego jako *casus belli*, Rosja zaś konsekwentnie zaprzecza, by jej żołnierze znajdowali się na terytorium Ukrainy.

[99] Niemal każdy proces działaczy KPRP i KPP oskarżanych o działalność wywrotową był przedstawiany na Zachodzie jako represje polityczne, którym miały towarzyszyć zbrodnicze działania polskiej policji politycznej i wojska.

Bibliografia:

1. Biesiedowski G.Z., *Pamiętniki dyplomaty sowieckiego*, Katowice 1929, bw.
2. Chruszczow N. *Wremia. Liudi. Własť* [online], http://www.hrono.ru/libris/lib_h/hrush03.php [dostęp: 16 II 2015].
3. D'Abernon E.V., *Osiemnasta decydująca bitwa w dziejach świata*, reprint wydania z 1932 r., Warszawa 1990, „Herold-Press".
4. Daszyński I., *Pamiętniki*, t. 2, Kraków 1926, Drukarnia Ludowa.
5. Juryś R., *Kulisy wielkiej prowokacji*, Warszawa 1960, Książka i Wiedza.
6. Kenez P., *A History of the Soviet Union from the Beginning to the End*, Cambridge 2006, Cambridge University Press.
7. Kowalski J., *Zarys historii polskiego ruchu robotniczego 1918–1939*, Warszawa 1962, Książka i Wiedza.
8. Landau Z., Tomaszewski J., *Zarys historii gospodarczej Polski 1918–1939*, Warszawa 1960, Książka i Wiedza.
9. „Kurier Warszawski" z 29 kwietnia 1919 r.
10. Lenin W.I., *Dzieła wybrane*, t. 2, Warszawa 1951, Książka i Wiedza.
11. Marszałkowski T., *Zamieszki, ekscesy i demonstracje w Krakowie 1918–1939*, Kraków 2015, Arcana.
12. Materski W., *Tarcza Europy. Stosunki polsko-sowieckie 1918–1939*, Warszawa 1994, Książka i Wiedza.
13. *Na granicy epok: Wspomnienia o udziale Polaków w rewolucji październikowej i wojnie domowej w Rosji 1917–1921*, Z. Iwańczuk i in. (red.), Warszawa 1967, Książka i Wiedza.
14. Nikulin L., *Miortwaja zyb'* [online], http://royallib.ru/book/nikulin_lev/mertvaya_zib.html [dostęp: 21 XI 2013].
15. *Pamiętniki generała Rybaka*, Warszawa 1954, Czytelnik.
16. *Party, State, and Society in the Russian Civil War*, D. Koenker, W.G. Rosenberg, R.G. Suny (red.), Bloomington 1989, Indiana University Press.
17. Pawłowski I., *Polityka i działalność wojskowa KPP 1918–1928*, Warszawa 1964, Wydawnictwo Ministerstwa Obrony Narodowej.
18. Pepłoński A., *Kontrwywiad II Rzeczypospolitej*, Warszawa 2002, Bellona.
19. Piłsudski J., *Rok 1920*, Gdańsk 1989, Graf.
20. Pipes R., *Rosja bolszewików*, Warszawa 2005, Magnum.
21. Próchnik A., *Pierwsze piętnastolecie Polski Niepodległej (1918–1933)*, Warszawa 1933, reprint Warszawa 1957, Książka i Wiedza.
22. Rataj M., *Pamiętniki*, Warszawa 1965, Ludowa Spółdzielnia Wydawnicza.
23. Reguła J.A., *Historia Komunistycznej Partii Polski w świetle dokumentów i faktów*, Toruń 1994, Portal.
24. *Rocznik Statystyki Rzeczypospolitej Polskiej 1920–1922*, cz. II, Warszawa 1923, Główny Urząd Statystyczny Rzeczypospolitej Polskiej.
25. Rotfeld A., *Putin walczy o duszę Rosji*, „Gazeta Wyborcza" z 26 marca 2014.
26. W. Skóra, *Organizacja i działalność służby konsularnej Drugiej Rzeczypospolitej na terenach Rosji, Ukrainy i ZSRR w dwudziestoleciu międzywojennym (1918–1939)*, w: *Stosunki polityczne, wojskowe i gospodarcze Rzeczypospolitej Polskiej i Związku Radzieckiego w okresie międzywojennym*, J. Gmitruk, W. Włodarkiewicz (red.), Warszawa–Siedlce 2012, s. 259–283.
27. Sokolnicki M., *Czternaście lat*, Warszawa 1936, bw.

28. Sokolnicki M., *Sprawa polska na terenie międzynarodowym,* „Niepodległość" 1930, t. 1, z. 2.
29. Stawecki P., *Polityka wojskowa Polski 1921–1926*, Warszawa 1981, Wydawnictwo Ministerstwa Obrony Narodowej.
30. Szeremietiew R., *W obcym interesie (zarys historii Komunistycznej Partii Polski)*, Warszawa–Kościan 1991, Książnica Polska.
31. *Wojna hybrydowa*, Z. Nawrocki (red.), „Przegląd Bezpieczeństwa Wewnętrznego" 2015, wydanie specjalne.
32. Wraga R., *Trust*, „Kultura" 1949, nr 4/21–5/22.

Źródła internetowe:

1. http://leninism.su/works/82-tom-43/1038-x-sezd-rkpb.html [dostęp: 23 III 2016].
2. http://svr.gov.ru/history/ar.htm [dostęp: 14 II 2016].
3. http://www.hrono.ru/sobyt/1900sob/1921_10sezd.php [dostęp: 10 II 2016].

Abstrakt

Autor, analizując w artykule genezę wojny hybrydowej, stwierdza, że jej założenia teoretyczne zostały wypracowane przez rosyjskie służby specjalne na początku lat 20. XX w. Sowieci dążyli do zdestabilizowania sytuacji w II RP, aby stało się możliwe przejęcie władzy przez partię komunistyczną sterowaną bezpośrednio z Moskwy. Wojna hybrydowa w tym ujęciu jest traktowana jako instrument sowieckiej (a później rosyjskiej) polityki. W przypadku tego typu wojny czynnik militarny ma znaczenie jedynie pomocnicze – jej głównym celem jest osiągnięcie strategicznego celu politycznego za sprawą działań dezinformacyjno-wywrotowych wymienionych w opracowaniu.

Słowa kluczowe: wojna hybrydowa, Związek Sowiecki, sowieckie służby wywiadowcze, operacje dezinformacyjno-wywrotowe, Komunistyczna Partia Robotnicza Polski, destabilizacja II RP.

Abstract

In the article the author analyzes the genesis of a hybrid warfare and argues that its theoretical assumptions were developed by the Soviet secret service at the beginning of the 1920s in order to destabilize the situation in Poland to a degree which would enable the Polish Communist Party controlled directly from Moscow to take over the power in the coutry. The hybrid warfare in this sense is considered as an instrument of the Soviet (and later Russian) foreign policy. In this kind of warfare the military factor plays only an auxiliary role, aiming – along with a variety of disinformation-subversive activities – to achieve the strategic political objectives.

Keywords: hybrid warfare, Soviet Union, soviet intelligence, disinformation-subversive operations, Communist Party of Poland, state destabilization.

Dariusz Pożaroszczyk

Wywiad Chińskiej Republiki Ludowej – charakterystyka działalności i zagrożenia dla Polski

Historia państwa chińskiego liczy ponad 4 tys. lat[1]. Najnowszy etap w dziejach Chin rozpoczął się w 1978 r.[2] wraz z dojściem do władzy Deng Xiaopinga[3]. Mimo represji[4], których doznał w okresie Rewolucji Kulturalnej, przez całe życie pozostał wierny ideom komunizmu[5], a także marzeniu swego poprzednika Mao Zedonga[6], aby uczynić Chiny najpotężniejszym państwem nie tylko w ramach bloku socjalistycznego, lecz także na całym świecie. Inaczej jednak niż w przypadku „Wielkiego Sternika"[7], dla Deng Xiaopinga zapewnienie Chinom pozycji światowego mocarstwa wiodło przede wszystkim przez wzmocnienie gospodarki. Dojście w 1978 r. Deng Xiaopinga do władzy oznaczało więc odsunięcie spraw ideologicznych na boczny tor i skoncentrowanie wysiłków na rozwoju potencjału ekonomicznego i wojskowego, a w konsekwencji również politycznego Chińskiej Republiki Ludowej. Na posiedzeniu Trzeciego Plenum KC KPCh[8] jedenastej kadencji w grudniu 1978 r. został przyjęty zaproponowany przez Denga nowy kurs, w którym położono nacisk na reformy gospodarcze. Głębokie zmiany wprowadzone w Chinach po 1978 r. umożliwiły Państwu

[1] Wskazanie dokładnych początków państwowości chińskiej jest trudne. Za historycznie potwierdzoną uchodzi dynastia Shang, której okres panowania rozpoczął się około 1600 p.n.e. Niektórzy historycy za pierwszą chińską dynastię uznają jednak panującą wcześniej (mniej więcej w latach 2200–1600 p.n.e.) dynastię Xia, zob. F. Hauser, V. Häring, *China–Handbuch: Erkundungen im Reich der Mitte*, Berlin 2005, s. 28–32; Shuyang Su, *China: eine Einführung in Geschichte, Kultur und Zivilisation*, Gütersloh – München 2008, s. 44, 46–47; W. Scott Morton, Ch.M. Lewis, *Chiny. Historia i kultura*, tłum. B.S. Zemanek, Kraków 2007, s. 15–20. W tradycji chińskiej od czasu wybitnego historyka z okresu dynastii Han Sima Qiana za początek Państwa Środka przyjmuje się okres panowania legendarnego Huangdi (Żółtego Cesarza) przypadający na lata 2697–2597 p.n.e., zob. J. Wardęga, *Chiński nacjonalizm. Rekonstruowanie narodu w Chińskiej Republice Ludowej*, Kraków 2014, s. 27.

[2] Rok 1978 jest oficjalnym początkiem wielkich reform gospodarczych w Państwie Środka prowadzonych na podstawie racjonalności w ekonomii. W rzeczywistości pierwsze próby odejścia od zarządzania gospodarką, przede wszystkim wykorzystanie doktryny maoistycznej, miały miejsce już w połowie lat 70. XX w. pod patronatem ówczesnego premiera Zhou Enlaia, zob. B. Woliński, *Restrukturyzacja i prywatyzacja chińskich przedsiębiorstw*, „Azja–Pacyfik" 2006, nr 9, s. 160 i 171; B. Kikolski, *Plany rozwoju gospodarczego Chin*, „Azja-Pacyfik" 1998 nr 1, s. 132; B. Góralczyk, *Miejsce Polski w strategii gospodarczej i polityce zagranicznej Chin po przekazaniu władzy na XVIII zjeździe KPCh*; Ekspertyzy GoChina [online], http://www.gochina.gov.pl/ekspertyzy_gochina [dostęp: 28 I 2017].

[3] Nazwisko i imię zapisane w transkrypcji hanyu pinyin. Transkrypcja hanyu pinyin jest podstawową formą zapisu nazw chińskich stosowaną w niniejszym artykule. W przypadku nazw, które w Polsce przyjęły się w transkrypcji Wade'a i Gilesa, dodatkowo jest podawana również ta transkrypcja.

[4] Po rozpoczęciu Rewolucji Kulturalnej Deng Xiaoping został pozbawiony piastowanych stanowisk i zesłany do pracy w fabryce traktorów w charakterze ślusarza. Represje dotknęły również jego rodzinę. Najstarszy syn Deng Xiaopinga – Deng Pufang został wyrzucony (według innych źródeł zmuszony do skoku) przez czerwonogwardzistów z czwartego piętra, w wyniku czego został trwale sparaliżowany, zob. E.F. Vogel, *Deng Xiaoping and the Transformation of China*, Cambridge (MA) 2011, s. 15; D. Goodman, *Deng Xiaoping and the Chinese Revolution: A Political Biography*, London 1994, s. 78–79.

[5] B. Góralczyk, *Miejsce Polski w strategii*…, s. 2.

[6] Według transkrypcji Wade-Giles: Mao Tse-tunga.

[7] Jeden z przydomków Mao Zedonga, zob. N.N. Huang, *"East is Red": A Musical Barometer for Cultural Revolution. Politics and Culture*, Los Angeles 2008, s. 19.

[8] Komitet Centralny Komunistycznej Partii Chin.

Środka wejście na ścieżkę dynamicznego wzrostu, którego imponujące tempo utrzymuje się od ponad 30 lat [9]. Sukcesy gospodarcze, które spowodowały wzrost bogactwa Chińskiej Republiki Ludowej, stworzyły z kolei możliwość przeznaczania ogromnych kwot na rozwój armii[10]. Wskazane procesy doprowadziły pod koniec XX w. do uzyskania przez państwo chińskie statusu światowego mocarstwa. Ma to istotne znaczenie dla działań ChRL na arenie międzynarodowej. Pozycja i imperialne aspiracje Chin powodują, że ten kraj prowadzi coraz więcej interesów również poza tradycyjnym, ograniczonym do krajów sąsiednich, obszarem. Dowodem na rozszerzanie się zakresu spraw znajdujących się w sferze zainteresowania ChRL jest m.in. wzrastająca aktywność Państwa Środka w krajach Afryki i Ameryki Południowej[11]. Powiększaniu się strefy chińskich interesów odpowiada również systematyczne zwiększanie obszaru, w którym do działań jest przygotowywana chińska marynarka wojenna. Ten proces określa się jako przejście od floty brązowych wód (działania w strefie przybrzeżnej) do floty błękitnych wód (działania na otwartych wodach oceanicznych)[12].

Duży i stale poszerzający się obszar chińskiego oddziaływania bezsprzecznie wywiera istotny wpływ na zadania i funkcjonowanie służb wywiadowczych ChRL. Udział i znaczenie tego kraju w kreowaniu sytuacji międzynarodowej wymusił przekształcenia jego służb wywiadowczych – spośród których główną rolę odgrywają[13] Guójiā Ānquánbù nazywane też Guó'ān bù (Ministerstwo Bezpieczeństwa Państwowego)[14], Gōng'ān bù (Ministerstwo Bezpieczeństwa Publicznego)[15] i Qíngbàobù (Departament Wywiadu)[16] – w instytucje o charakterze globalnym, które działają we wszystkich państwach oraz sferach życia i starają się uzyskać jak najszerszy dostęp do wartościowych informacji.

Warto zatem odpowiedzieć na pytanie, czy działalność chińskich tajnych służb jest zagrożeniem również dla Polski, jej pozycji i dobrobytu oraz interesów zamieszkujących ją osób. Aby tego dokonać, niezbędne jest przeanalizowanie wywiadowczej aktywności prowadzonej przez Chińską Republikę Ludową, zwłaszcza stosunku władz do niejawnego zdobywania informacji, skali prowadzonej działalności wywiadowczej, słabości

[9] B. Góralczyk, *Miejsce Polski w strategii…*, s. 7; B. Kikolski, *Plany rozwoju gospodarczego*…, s. 141.

[10] A. Krzyżanowska, *Biała Księga Obronności Chin – pokojowe deklaracje i realia*, „Bezpieczeństwo Narodowe" 2011, nr 20, s. 71.

[11] K. Zajączkowski, *ChRL wobec krajów Południa (na przykładzie Afryki Subsaharyjskiej). Szansa czy zagrożenie dla międzynarodowej pozycji UE*, w: *Chiny-Indie. Ekonomiczne skutki rozwoju*, K. Kłosiński (red.), Lublin 2008, s. 329–346; A. Krzyżanowska, *Biała Księga Obronności*..., s. 57.

[12] Ł. Ho Thanh, P. Behrendt, *Zbrojenia morskie a mocarstwowość państw Azji i Pacyfiku*, w: *Azjatyckie strategie bezpieczeństwa u progu XXI wieku*, J. Marszałek-Kawa (red.), Toruń 2014, s. 13.

[13] Precyzyjne wskazanie wszystkich instytucji państwowych wykonujących w ChRL działania wywiadowcze nie jest możliwe ze względu na utajnienie części danych oraz znaczne skomplikowanie systemu służb specjalnych Państwa Środka i innych podmiotów zajmujących się zbieraniem informacji, zob. schemat służb wywiadowczych ChRL w: R. Faligot, *Tajne służby chińskie. Od Mao do igrzysk olimpijskich*, tłum. O. Hedemann, A. Rasińska-Bóbr, Katowice 2009, s. 508. Liczne organy, instytucje i organizacje zaangażowane w zbieranie danych naukowych wymieniają W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*, London – New York 2013, s. 18–47.

[14] Oficjalna nazwa to: Zhōnghua Rénmín Gònghé Guó Guójiā Ānquánbù (Chińskiej Republiki Ludowej Ministerstwo Bezpieczeństwa Państwowego).

[15] Oficjalna nazwa: Zhōnghua Rénmín Gònghé Guó Gōng'ān bù (w dosłownym tłumaczeniu: Chińskiej Republiki Ludowej Ministerstwo Bezpieczeństwa Publicznego). Gong an Bu pełni przede wszystkim funkcję policji i kontrwywiadu. W jego strukturze znajdują się jednak również komórki odpowiedzialne za wywiad.

[16] Oficjalna nazwa: Zhōngguó Rénmín Jiěfàng Jūn Zǒng Cānmóu Bù Qíngbàobù (w dosłownym tłumaczeniu: Chińskiej Armii Ludowo-Wyzwoleńczej Sztabu Generalnego Departament Wywiadu). W ramach tego Departamentu wywiadem zajmują się przede wszystkim Wydział II i Wydział III, za: https://fas.org/irp/world/china/pla/gen_staff.htm [dostęp: 15 II 2017].

i mocnych stron służb chińskich oraz kierunków pracy operacyjnej. Należy także przedstawić okoliczności, które mogą wpływać na zwiększenie bądź zmniejszenie wywiadowczego zainteresowania Polską.

Opisując pozycję, jaką zajmuje działalność wywiadowcza w komunistycznych Chinach, należy wskazać, że była ona i nadal jest kształtowana w dużej mierze przez tradycję. Zapiski o sztuce wywiadu pojawiają się w literaturze chińskiej już w pismach żyjącego w latach 544–496 p.n.e. generała Sun Zi[17], przy czym, w przeciwieństwie do kultury europejskiej, działanie w charakterze szpiega w Państwie Środka od zawsze cieszyło się dużym szacunkiem[18]. Innymi okolicznościami, które zwłaszcza w okresie przejęcia władzy przez Deng Xiaopinga spowodowały konieczność sięgnięcia po wyniki pracy wywiadu, były zacofanie i upadek chińskiej gospodarki spowodowane nieodpowiedzialną polityką Mao Zedonga[19] oraz równoczesne odcięcie Chin od możliwości pozyskania nowoczesnych technologii w ramach bloku socjalistycznego na skutek konfliktu z ZSRR[20]. Ówcześni komunistyczni decydenci ChRL, z których w przeszłości wielu było zaangażowanych w działalność szpiegowską[21], doskonale wiedzieli, że zdobywanie i wykorzystywanie zarówno jawnych[22], jak i poufnych informacji jest niewątpliwie jednym z najskuteczniejszych instrumentów służących do stymulowania rozwoju poszczególnych gałęzi gospodarki[23]. Przytoczone okoliczności powodują, że Chińska Republika Ludowa jest państwem, w którym działania wywiadowcze znajdują szerokie, zakorzenione w tradycji i aktualnych dążeniach wsparcie władz[24]. Te czynniki tworzą niewątpliwie korzystny klimat do podejmowania działań szpiegowskich. Równocześnie komunistyczne Chiny dzięki ekonomicznemu rozwojowi ostatnich lat i potencjałowi ludzkiemu dysponują środkami umożliwiającymi prowadzenie działalności wywiadowczej na ogromną skalę. Dokładne dane dotyczące nakładów na służby specjalne, w tym wywiad, ze względu na niejawność tych informacji nie są oczywiście znane. Można jednak opisać pewne zjawiska związane z chińskim szpiegostwem, które przynajmniej w przybliżeniu pozwolą zobrazować skalę i charakter tej działalności.

---

[17] Według transkrypcji Wade-Giles: Sun Tzu. Rozdział XIII słynnego traktatu o sztuce wojny nosi tytuł *Użycie szpiegów*, zob. Sun Tzu, *The Art of War by Sun Tzu – Classic Edition*, tłum. angielskie L. Giles, B. Wiliams, S. Kim, El Paso 2009, s. 48–51.

[18] *Spies are **the most important*** (podkreślenie autora – przyp. red.) *element in war, because on them depends an army's ability to move* (*Szpiedzy są najważniejszym elementem w czasie wojny, ponieważ od nich zależy zdolność armii do ruchu* – tłum. aut.), cyt. za: Sun Tzu, *The Art*…, s. 51.

[19] Szczególnie negatywne skutki dla potencjału ekonomicznego Chin miały reformy z lat 1958–1962 określane jako Wielki Skok oraz polityka znana jako Rewolucja Kulturalna, prowadzona w latach 1966–1969 (oficjalnie) i 1969–1975 (w rzeczywistości), zob. W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese Industrial*…, s. 4, 5, 9, 11.

[20] Więcej o konflikcie Chin i ZSRR zob. L.M. Lüthi, *Chiny ZSRR. Zimna wojna w świecie komunistycznym*, tłum. J. Pawłowski, K. Urban-Pawłowska, Warszawa 2011.

[21] Tajną działalność na terenie Francji w latach 20. XX w. prowadzili m.in. Zhou Enlai oraz Deng Xiaoping, zob. R. Faligot, *Tajne służby chińskie*…, s. 29–33.

[22] O roli tzw. białego wywiadu w ChRL zob. rozdział zatytułowany *China's use of open source*, w: W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese Industrial*…, s. 18–47, przede wszystkim s. 18–20, 33 i 44.

[23] Ogólnie o roli wywiadu gospodarczego zob. Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009, s. 125–130 oraz K. Mackrakis, *The crown jewels and the importance of scientific–technical intelligence*, w: *East German Foreign Intelligence: Myth, Reality and Controversy*, K. Macrakis, T. Wegener Friis, H. Müller-Enbergs (red.), New York 2010, s. 185–201. Znaczeniu wywiadu gospodarczego dla rozwoju ChRL jest poświęcona w całości praca przywołana w przypisie 13 autorstwa W.C. Hannas, J. Mulvenon, A.B. Puglisi.

[24] W.C. Hannas, J. Mulvenon, A.B. Puglisi, *Chinese Industrial*..., s. 44.

Zidentyfikowaną właściwością służb chińskich jest wykorzystywanie do celów wywiadowczych diaspory chińskiej oraz wzrastającego zainteresowania państwem chińskim, a zwłaszcza jego kulturą i językiem[25]. Analizując rolę migrantów pochodzenia chińskiego w działalności wywiadowczej, należy wskazać na wiele czynników, które powodują, że w poszczególnych krajach mniejszości chińskie są ważnym środowiskiem plasowania agentury i pozyskiwania osobowych źródeł informacji. Po pierwsze, liczebność społeczeństwa chińskiego[26] oraz to, że gospodarka (mimo swoich rozmiarów i ciągłego wzrostu) nie jest w stanie zapewnić pracy wszystkim, którzy jej szukają, powodują, że z Chin co roku wyjeżdża ogromna liczba osób w poszukiwaniu lepszego życia[27]. To zjawisko prowadzi do szybkiego powiększania się chińskich społeczności imigranckich w poszczególnych miejscach docelowych[28]. Po drugie, ze względu na bariery kulturową i językową mniejszość chińska zazwyczaj w bardzo ograniczonym zakresie integruje się ze społecznością miejscową, tworząc zamknięty i hermetyczny świat[29]. Ewentualne przeniknięcie do tego świata agentury kontrwywiadowczej państwa przyjmującego jest niezwykle trudne, podobnie jak i pozyskanie informatorów[30]. Inaczej przedstawia się sytuacja chińskiego wywiadu, jeśli chodzi o zdobywanie osobowych źródeł informacji. Ten, będąc narzędziem władzy państwa autorytarnego, ma zwiększone i ułatwione możliwości wykorzystywania chińskiej diaspory do swoich celów. Często już sama możliwość wyjazdu z Chin jest uzależniona od zgody na nawiązanie niejawnej współpracy z wywiadem[31]. Wobec tych obywateli, którym udało się wyjechać, służby chińskie nierzadko stosują szantaż, grożąc represjami wobec członków rodzin pozostawionych w kraju w razie odmowy dostarczania pożądanych informacji[32]. Należy również wskazać, że w przypadku Chińczyków, którzy zajmują się handlem towarami importowanymi z ojczyzny, brak zgody na pomoc służbom specjalnym może oznaczać zamknięcie możliwości robienia interesów przez odcięcie od źródeł zaopatrzenia.

[25] B. Góralczyk, *Chińskie wyzwanie nad Wisłą?* [online], http://www.instytutobywatelski.pl/12966/lupa-instytutu/chinskie-wyzwanie-nad-wisla [dostęp: 28 I 2017].

[26] Szacowana w lipcu 2016 r. liczba ludności Chin wynosiła 1 373 541 278, za: *The World Factbook, China* [online], https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html [dostęp: 28 I 2017].

[27] Chińska diaspora licząca 80–100 mln osób jest uważana na najliczniejszą i równocześnie najbogatszą diasporę świata, zob. P. Picquart, *Imperium chińskie. Historia i teraźniejszość chińskiej diaspory*, tłum. I. Kałużyńska, Warszawa 2006, s. 18–21. J. Kurlantzick podaje dane, według których dysponuje ona zawrotną kwotą półtora biliona dolarów, zob. J. Kurlantzick, *Charm Offensive: How China's Soft Power Is Transforming the World*, New Haven – Conn – London 2007, s. 75.

[28] P. Picquart, *Imperium chińskie. Historia*…, s. 207–212.

[29] J. Kurlantzick*, Charm Offensive: How China's*…, s. 73. Hermetyczność chińskiej diaspory wymaga komentarza. Analiza społeczności imigranckich w poszczególnych krajach dokonana przez P. Picquarta pozwala postawić tezę, że na asymilację Chińczyków z miejscową ludnością wpływa czas trwania ruchu migracyjnego. W krajach, do których Chińczycy przebywają od wieków, są na ogół dobrze zintegrowani i często odgrywają ważną rolę w życiu społecznym. Przykładami są: Sułtanat Brunei, Birma, Wietnam Kambodża, Malezja, Filipiny, Indonezja i Tajlandia, zob. P. Picquart, *Imperium chińskie. Historia*…, s. 111–128 i 153. Ze względu na dużą liczebność Chińczyków i odniesione przez nich sukcesy gospodarcze są również dość dobrze zintegrowani w Stanach Zjednoczonych, Kanadzie oraz Australii. Na ten proces pozytywny wpływ wywarło rozpoczęcie migracji na te obszary już w XIX w. Najsłabiej zintegrowani, a w konsekwencji najbardziej zamknięci, wydają się być Chińczycy przybywający do Europy, szczególnie do krajów Europy Środkowej i Wschodniej, gdyż migracje w te rejony zaczęły się dopiero na początku lat 90. XX w.

[30] Zwraca na to uwagę m.in. były szef UOP gen. Gromosław Czempiński, http://www.gazetakrakowska.pl/artykul/201494,general-czempinski-chinscy-szpiedzy-sa-juz-w-polsce,id,t.html [dostęp: 28 I 2017].

[31] H. Shen, *Instytut Konfucjusza – chiński urok czy ukryty Mao* [online], http://www.fronda.pl/a/instytut-konfucjusza-chinski-urok-czy-ukryty-mao,3870.html [dostęp: 28 I 2017].

[32] R. Faligot, *Tajne służby chińskie*…, s. 224.

Z pewnością wśród chińskich imigrantów znajduje się także wielu, którzy współpracę ze służbami specjalnymi swego kraju podejmują całkowicie dobrowolnie, kierując się uczuciami patriotycznymi[33]. Dodatkowo mniejszość chińska, która jest już trwałym elementem wielu społeczeństw, pozwala na lokowanie kadrowych funkcjonariuszy wywiadu w charakterze tzw. nielegałów[34], przy czym możliwości „zalegendowania"[35] takich osób są bardzo szerokie. Przykładem wykorzystywania przedstawicieli diaspory w działalności szpiegowskiej jest między innymi sprawa Mo Hailonga, znanego także jako Robert Mo. Będąc legalnym rezydentem w USA jako pracownik Dabeinong Technology Group Company, próbował wykraść sekrety dotyczące zmodyfikowanych genetycznie ziaren, czym działał na szkodę spółek DuPont Pioneer and Monsanto i za co ostatecznie w 2016 r. został skazany na trzy lata pozbawienia wolności[36]. Znacznie poważniejsza odpowiedzialność grozi Edwardowi C. Lin, porucznikowi marynarki wojennej USA pochodzącemu z Tajwanu. W 2016 r., osiem lat po otrzymaniu amerykańskiego obywatelstwa, został on oskarżony o szpiegostwo na rzecz Chin, za co grozi mu kara śmierci[37]. Kolejnym przykładem amerykańskiego obywatela pochodzenia chińskiego oskarżonego w 2016 r. o szpiegostwo, któremu grozi kara dożywotniego pozbawienia wolności, jest fizyk nuklearny Szuhsiung Ho „Allen Ho"[38] posiadający amerykańskie obywatelstwo od 1983 r. Problem z wykorzystaniem mniejszości chińskiej jako źródła informacji przez wywiad ChRL mają również inne kraje. W Niemczech w 2011 r. został skazany za działalność na rzecz wywiadu chińskiego obywatel niemiecki John Zhou, który zajmował się rozpracowywaniem członków sekty Falun Gong[39], Z kolei w Szwecji w 2010 r. za szpiegostwo przeciwko mniejszości ujgurskiej na rzecz ChRL przed sądem stanął obywatel szwedzki pochodzenia chińskiego – 61-letni Babur Maihesuti[40].

Niewątpliwie jedną z najlepszych opcji lokowania funkcjonariuszy wywiadu jest zakładanie spółek prawa handlowego[41]. Tworzenie podmiotów prawych prowadzących

[33] W literaturze poświęconej Chinom zwraca się uwagę na znaczenie patriotyzmu dla Chińczyków i podkreśla się, że ideologia komunistyczna jako siła jednocząca zróżnicowane społeczeństwo jest powoli zastępowana przez nacjonalizm, zob. J. Wardęga, *Chiński nacjonalizm*…, s. 367–368. Przykładem motywacji patriotycznej dla zaangażowania się w działalność szpiegowską jest sprawa byłego inżyniera spółki Boeing, Dongfana „Grega" Chunga, który w 2010 r. został skazany na 15 lat pozbawienia wolności. Jako powód swojej działalności szpiegowskiej wprost wskazał on chęć przysłużenia się swojej ojczyźnie, zob. więcej https://www.theguardian.com/technology/2016/aug/11/espionage-arrest-of-nuclear-engineer-fuels-us-suspicions-of-chinese-tactics [dostęp: 28 I 2017].

[34] Przez określenie n i e l e g a ł w środowisku służb specjalnych rozumie się funkcjonariusza wywiadu, który działa na terytorium państwa obcego i nie jest chroniony immunitetem dyplomatycznym.

[35] Z a l e g e n d o w a n i e to działanie polegające na stworzeniu fikcyjnego lub częściowo fikcyjnego życiorysu, mające na celu ukrycie wszelkich związków funkcjonariusza wywiadu z jego służbą i równocześnie umożliwiające jak najgłębsze wejście w rozpracowywane środowisko.

[36] Zob. więcej: https://www.justice.gov/opa/pr/chinese-national-sentenced-prison-conspiracy-steal-trade-secrets [dostęp: 27 I 2017].

[37] Zob. https://www.washingtonpost.com/news/checkpoint/wp/2016/04/11/the-fall-of-edward-lin-the-navy-pilot-accused-of-espionage-and-patronizing-a-prostitute/?utm_term=.8b919c896471 [dostęp: 27 I 2017].

[38] https://www.justice.gov/opa/pr/us-nuclear-engineer-china-general-nuclear-power-company-and-energy-technology-international [dostęp: 28 I 2017].

[39] Zob. https://webspeicher.wordpress.com/2011/06/10/spionage-chinas-stasi-chinas-spion-deutschland-gericht-11294831/ [dostęp: 27 I 2017].

[40] Zob. http://facet.interia.pl/styl-zycia/ciekawostki/news-chinscy-szpiedzy-sa-wsrod-nas,nId,448718 [dostęp: 27 I 2017].

[41] W materiałach szkoleniowych Bundesamt für Verfassungsschutz zwrócono uwagę na to zagrożenie, zob. *Wirtschaftsspionage. Risiko für Unternehmen, Wissenschaft und Forschung*, Köln 2014, Bundesamt für

działalność gospodarczą lub ich przejmowanie przez funkcjonariuszy wywiadu pozwala nie tylko na plasowanie kadr wywiadowczych w interesujących środowiskach[42], lecz także umożliwia uzyskiwanie dodatkowych dochodów z prowadzonej działalności gospodarczej, które mogą wspierać działania wywiadowcze. Obecnie na terenie Polski działa co najmniej kilka tysięcy spółek z kapitałem chińskim. Podanie dokładnej liczby działających w Polsce spółek, które są powiązane z obywatelami ChRL, nie jest możliwe. Należy wskazać, że tylko na terenie Wólki Kosowskiej, będącej wielkim centrum handlu towarami importowanymi z Azji, działa kilkaset takich podmiotów[43]. Wiele spółek, które w rzeczywistości należą do obywateli ChRL, jest rejestrowanych na osoby mające polskie obywatelstwo. Statystykę spółek związanych chińskim kapitałem zaciemnia dodatkowo to, że wiele tych podmiotów jest zakładanych jedynie na krótki czas i po wystawieniu fikcyjnych faktur, znikają[44], co jest spowodowane ich uczestniczeniem w nielegalnej działalności. Wobec wielu chińskich spółek istnieją podejrzenia, niekiedy potwierdzone zarzutami prokuratorskimi[45], że ich działalność jest związana z powodującymi wielomilionowe szkody przestępstwami gospodarczymi. Najprostszym, a przy tym niezwykle dochodowym przestępstwem, w którym uczestniczą chińscy obywatele prowadzący działalność gospodarczą na terytorium Polski, jest ukrywanie realnej wartości sprowadzanych towarów, co skutkuje istotnym zaniżaniem należności celnych. Wobec słabości polskich służb skarbowych[46] wydaje się być kwestią czasu, kiedy przedstawiciele mniejszości chińskiej zaczną angażować się w bardziej wyrafinowane przestępstwa podatkowe polegające na nadużywaniu mechanizmów wewnątrzwspólnotowej dostawy towarów i ich sprzedaży oraz na organizowaniu tzw. karuzel podatkowych. W tym miejscu należy podkreślić, że prawdopodobnie większa cześć przywołanych powyżej przestępstw jest popełniania przez zwykłych, nieuczciwych przedsiębiorców oraz osoby powiązane z chińską przestępczością zorganizowaną. Nie można jednak wykluczyć, że za pewnymi przestępstwami gospodarczymi z udziałem obywateli ChRL stoją oficerowie wywiadu poszukujący dodatkowych dochodów na działalność operacyjną[47].

Verfassungsschutz für die Verfassungsschutzbehörden des Bundes und der Länder, s. 14; zob. też R. Faligot, *Tajne służby chińskie*…, s. 298–299 i 324.

[42] Na niebezpieczeństwo wynikające z ukrywania się w chińskiej diasporze prowadzącej działalność gospodarczą setek, a nawet tysięcy agentów wskazuje R. Faligot, *Tajne służby chińskie*…, s. 366.

[43] R. Fabisiak, *China made in Poland* [online], http://weekend.pb.pl/2391587,23084,china-made-in-poland [dostęp: 28 I 2017].

[44] Zob. wypowiedź R. Nawrota przytoczoną w: M. Piekarski, *Miliardy złotych nielegalnie przelewane z Polski do Chin* [online], http://www.rmf24.pl/fakty/polska/news-miliardy-zlotych-nielegalnie-przelewane-z-polski-do-chin,nId,388590? [dostęp: 28 I 2017].

[45] D. Walczak, *Wietnamska mafia wyprowadza z Polski gigantyczne pieniądze* [online], http://sledczy.focus.pl/afery-kryminalne/wietnamska-mafia-wyprowadza-z-polski-gigantyczne-pieniadze-154?strona=3 [dostęp: 28 I 2017].

[46] Dowodem na potwierdzenie tej pesymistycznej tezy jest powiększająca się nieprzerwanie w latach 2006–2015 r. tzw. luka podatkowa, która w 2013 r. osiągnęła od 37 do prawie 59 mld zł (w zależności od szacowanych rozmiarów), zob. *Raport PWC, Straty Skarbu Państwa w VAT – luka podatkowa, oszustwa, wyłudzenia oraz problematyka podatku od towarów i usług w Polsce*, Warszawa 2013, s. 14. W 2015 r. wysokość luki była szacowana na około 49 mld zł. Według prognoz na 2016 r. wielkość luki ma po raz pierwszy się zmniejszyć w stosunku do roku poprzedniego. Jej wysokość nadal jednak będzie kilkakrotnie większa niż dekadę temu i wyniesie około 45 mld zł, zob. http://www.pwc.pl/pl/media/2016/2016-11-23-luka-vat-2016.html [dostęp: 28 I 2017].

[47] Leszek Szymowski wprost wskazuje na osłanianie chińskich przestępców działających w Polsce przez chiński wywiad. Powołuje się on m.in. na wypowiedź anonimowego funkcjonariusza ABW oraz byłych szefów UOP – Gromosława Czempińskiego i Andrzeja Kapkowskiego. Zob. L. Szymowski, *Chińska mafia wkracza do Polski* [online], http://www.polskatimes.pl/artykul/156020,chinska-mafia-wkracza-do-polski,id,t.html

Duże możliwości wywiadowcze stwarza również wykorzystywanie przez władze ChRL społeczności akademickiej. Chińskie władze aktywnie promują wyjazdy swoich obywateli za granicę w celu zdobycia wykształcenia[48], nierzadko jednak stypendium i zgoda na wyjazd łączą się z koniecznością nawiązania kontaktów z wywiadem[49]. Przykładem wykorzystywania w działalności szpiegowskiej studentów jest głośna kilka lat temu we Francji sprawa chińskiej doktorantki Li Li Whuang, która została oskarżona o kradzież poufnych danych koncernu Valeo. Ostatecznie Chince nie udowodniono szpiegostwa i została skazana jedynie na niską karę z tytułu naruszenia zasad poufności[50].

Innym, często stosowanym sposobem zdobywania informacji przez służby wywiadowcze ChRL jest zalecana już przez Suz Tzu[51] tzw. zagrywka kobiecym wdziękiem. Na wykorzystywanie tej metody wskazują doniesienia prasy zachodniej, informującej o odwołaniu z Chin holenderskiego ambasadora, który rzekomo wdał się w romans z chińską pracownicą ambasady. Kilka lat wcześniej (w 2008 r.) noc w hotelu spędzona przez członka delegacji premiera Wielkiej Brytanii z przypadkowo poznaną Chinką zakończyła się dla owego urzędnika kradzieżą posiadanych dokumentów z poufnymi informacjami[52]. Wykorzystywanie pociągu seksualnego przez chińskie służby jest na tyle znane, że w 2016 r. Brytyjski rząd oficjalnie ostrzegł swoich pracowników udających się do ChRL na szczyt grupy G-20 przed możliwością podstawiania im atrakcyjnych kobiet[53].

Zagrożenie wywiadowcze stwarza także zainteresowanie chińską kulturą. Wraz ze wzrostem międzynarodowego znaczenia Chin można zaobserwować coraz większe zafascynowanie językiem oraz kulturą Państwa Środka[54]. Chińskie władze pozytywnie odbierają to zainteresowanie. Znamienna w tym kontekście jest wypowiedź Hu Sou-qinga, deputowanego Ogólnochińskiego Zgromadzenia Przedstawicieli Ludowych, który w wywiadzie dla gazety „China Daily" stwierdził, że promocja używania języka chińskiego przyczyni się do rozprzestrzenienia chińskiej kultury i w konsekwencji do wzrostu globalnego wpływu Chin[55]. Od 2004 r. na całym świecie są zakładane tzw. Instytuty Konfucjusza, które mają na celu promowanie języka i kultury Chin[56]. Według danych z 2014 r. na całym świecie działało już ponad 480 instytutów[57], z tego cztery w Polsce[58]. Instytuty Konfucjusza są miejscem w sposób naturalny przyciągającym oso-

[dostęp: 28 I 2017].

[48] W.C. Hannas, J. Mulvenon, A.B. Puglisi podają, że od 1978 r. na zagraniczne studia wyjechało ponad 2240 tys. chińskich studentów i z biegiem lat liczba wyjeżdżających się zwiększa, *Chinese Industrial*…, s. 138.

[49] Informacje na temat wykorzystywania studentów do zdobywania poufnych informacji można znaleźć w think tanku o nazwie European Strategic Intelligence and Security Center. Według zawartych tam informacji w Europie działa sieć chińskich studentów, koordynowana z Belgii, która zajmuje się szpiegostwem gospodarczym, zob. więcej http://www.spacedaily.com/news/china-05zw.html [dostęp: 27 I 2017].

[50] J. Garwood, *Scientific espionage*, „Labtimes" 2008, nr 3, s. 19–20.

[51] Sunzi, *Sztuka wojny i 36 forteli*, tłum J. Zawadzki, Seattle 2012, s. 223. W języku chińskim ta metoda jest znana pod nazwą měirén jì, co dosłownie można przetłumaczyć jako „podstęp ślicznotki".

[52] http://www.faz.net/aktuell/gesellschaft/spionage-china-setzt-frauen-auf-botschafter-an-14490421.html [dostęp: 28 I 2017].

[53] https://www.rt.com/uk/358191-g20-uk-chinese-honeytrap/ [dostęp: 28 I 2017].

[54] S. Czepielewski, *Lingua franca made in China* [online], http://www.jows.pl/node/216 [dostęp: 28 I 2017].

[55] *In fact, promoting the use of Chinese among overseas people has gone beyond purely cultural issues, It can help build up our national strength and should be taken as a way to develop our country's soft power* [online], http://www.chinadaily.com.cn/english/doc/2006–03/10/content_530648.htm [dostęp: 23 III 2015].

[56] Pierwszy Instytut Konfucjusza powstał 21 XI 2004 r. w Seulu.

[57] http://www.instytutkonfucjusza.uj.edu.pl/o-nas/historia [dostęp: 28 I 2017].

[58] Pierwszy Instytut Konfucjusza w Polsce powstał w Krakowie, następne zostały założone w Opolu, Wrocławiu i Poznaniu.

by zainteresowane Chinami. To środowisko niewątpliwie znajduje się w kręgu zainteresowań chińskich służb specjalnych. Istnieje ryzyko, że agenci wywiadu ChRL mogą podejmować próby nawiązania przyjacielskich relacji z osobami uczęszczającymi do instytutów. Najbardziej obiecujące dla służb może być fundowanie wyjazdów do Chin. Dla osoby uczącej się języka chińskiego jest on wielką szansą, równocześnie jednak wiąże się z istotnymi zagrożeniami. We własnym kraju służby specjalne Chin mają większe możliwości werbunku, w tym opartego na agresywnych metodach pracy operacyjnej w postaci gróźb i szantażu[59]. Należy wspomnieć, że sama obecność i działalność instytutów również budzi kontrowersje. Instytuty są oskarżane o bycie narzędziem w polityce zagranicznej ChRL, wykorzystywanym jako element *soft power*[60].

Oprócz opisanych już wcześniej czynników, takich jak ogromne środki finansowe i osobowe, pozytywny stosunek chińskich władz do działalności szpiegowskiej, naturalne, szerokie możliwości lokowania agentury i pozyskiwania osobowych źródeł informacji oraz hermetyczność chińskiej diaspory utrudniająca penetrację kontrwywiadowczą, do zjawisk, które sprzyjają działalności szpiegowskiej ChRL, należy zaliczyć ogólne osłabienie reżimu kontrwywiadowczego w wielu krajach narażonych na działalność szpiegowską. Jest ono spowodowane nie tylko znacznymi ograniczeniami budżetowymi dotykającymi służby kontrwywiadowcze, ale także zliberalizowaniem sankcji za szpiegostwo. Przykładowo polski kodeks karny (kk) za udział w działalności szpiegowskiej na podstawie art. 130 § 1 kk przewiduje karę od roku do 10 lat. Tak określone zagrożenie penalne powoduje, że w obecnym kodeksie karnym, w przeciwieństwie do kodeksu z 1969 r. (zob. art. 124 kk z 1969 r.), udział w działalności obcego wywiadu nie jest już zbrodnią. Najwyższa sankcja przewidziana przez art. 130 kk jest związana z organizowaniem działalności obcego wywiadu lub kierowaniem nią. Za popełnienie tych czynów art. 130 § 4 kk przewiduje karę nie niższą niż lat 5 lub karę 25 lat pozbawienia wolności. Tak więc nawet za najpoważniejszą formę udziału w obcym wywiadzie nie grozi w Polsce kara dożywotniego pozbawienia wolności, tym bardziej kara śmierci, usunięta z polskiego kodeksu karnego w 1997 r. Dla porównania – art. 110 kodeksu karnego ChRL za akt szpiegostwa przewiduje karę pozbawienia wolności nie niższą niż 10 lat lub karę dożywotniego pozbawienia wolności. W sytuacji spowodowania przez działalność szpiegowską poważnych szkód dla kraju i obywateli i gdy równocześnie okoliczności popełnienia czynu są szczególnie nikczemne, art. 113 kk ChRL przewiduje możliwość zasądzenia kary śmierci. Zaostrzeniem represji za szpiegostwo przeciwko ChRL jest ponadto możliwość orzeczenia konfiskaty majątku (art. 113 kk ChRL), a nie tylko przepadku, jak jest to możliwe na podstawie art. 139 polskiego kodeksu karnego. Jedynie w tzw. mniejszych przypadkach, zgodnie z art. 110 kk zd. 2 ChRL, kara nie może być niższa niż 3 lata i wyższa niż 10 lat[61]. Szpiegowskiej działalności ChRL sprzyja rów-

[59] W obliczu opisanego zainteresowania chińskim państwem, kulturą i językiem, wykorzystywanego przez wywiad ChRL, zasadne wydaje się objęcie odpowiednią profilaktyką kontrwywiadowczą osób uczących się tego języka, a zwłaszcza osoby wyjeżdżające na stypendia do Chin.

[60] Zob. wypowiedź byłego szefa Departamentu Azji i Pacyfiku Canadian Security Intelligence Service, który stwierdził, że działalność instytutów jest zagrożeniem dla bezpieczeństwa Kanady, za: http://www.theepochtimes.com/n3/1018292-hosting-confucius-institute-a-bad-idea-says-intelligence-veteran/ [dostęp: 27 I 2017]. Dogłębną analizę działań Instytutów Konfucjusza na rzecz rządu ChRL przedstawia R. Auethavornpipat, *Revealing China's Hegemonic Project in Thailand: How the Confucius Institute Furthers the Chinese State's International Ambitions*. *Paper presented at the 12th International Conference on Thai Studies 22-24 April 2014 University of Sydney* [online], http://sydney.edu.au/southeast-asia-centre/documents/pdf/auethavornpipat-ruji.pdf [dostęp: 27 I 2017].

[61] W artykule autor wykorzystał tekst kk ChRL w języku angielskim umieszczony na stronie Asian Legal

nież jej intensywny rozwój technologiczny, który umożliwia prowadzenie coraz bardziej zaawansowanych i wyrafinowanych ataków w cyberprzestrzeni[62]. Obecnie Chiny są uważane za kraj, którego aktywność w cyberprzestrzeni jest jednym z największych zagrożeń dla danych informatycznych[63].

Równocześnie, mimo ogromnego postępu technologicznego, chińskie służby wciąż pozostają w tyle za amerykańskim wywiadem. Wyraźna rasowa odrębność Chińczyków, która z jednej strony ułatwia penetrację wywiadowczą własnej diaspory, z drugiej jest istotnym utrudnieniem przy wchodzeniu w inne środowiska. Szczególnie w Europie, Stanach Zjednoczonych i Kanadzie osoby narodowości chińskiej zawsze będą traktowane jako przedstawiciele obcej, odległej cywilizacji i w związku z tym będą obarczone pewną dozą nieufności, co z pewnością stanowi poważną przeszkodę w dogłębnej infiltracji środowisk zachodnich. Wydaje się również, że na Zachodzie pewien rodzaj operacji jest w sposób naturalny wyłączony dla chińskich szpiegów. Trudno bowiem wyobrazić sobie, aby chiński szpieg po przybyciu do kraju cywilizacji zachodniej jako nielegał mógł skutecznie podszyć się pod osobę narodowości tego kraju i penetrować miejscowe środowisko, niebędące środowiskiem imigranckim[64]. Na pracy chińskich służb specjalnych negatywnie mogą się odbijać także pewne strukturalne słabości komunistycznych Chin. W realiach Państwa Środka faktyczną elitę, często stojącą ponad prawem, stanowią członkowie Komunistycznej Partii Chin. Powszechnym zjawiskiem jest przy tym swoista sukcesja władzy objawiająca się zajmowaniem najwyższych stanowisk państwowych przez dzieci wpływowych rodziców. W obliczu takiego działania nie można wykluczyć, że – podobnie jak to jest w przypadku służb rosyjskich[65] – kluczowe stanowiska w chińskim wywiadzie nie są przydzielane na podstawie umiejętności, lecz ze względu na układy towarzyskie i koneksje rodzinne[66]. Taka sytuacja, jeśli rzeczywiście ma miejsce, nie tylko istotnie pomniejsza jakość chińskich służb specjalnych, powodując, że najważniejsze stanowiska w tych instytucjach zajmują osoby pozbawione odpowiednich kompetencji, lecz także stwarza dodatkowe zagrożenia. Funkcjonariusze, którzy mają dużą wiedzę i umiejętności oraz odnoszą sukcesy, ale nie mają odpowiednich znajomości, nie są

Information Institute pod adresem http://www.asianlii.org/cn/legis/cen/laws/clotproc361/ [dostęp: 28 I 2017].

[62] Zob. więcej w rozdziale zatytułowanym *Cyber War*, w: D.F. Poindexter, *The Chinese information war: espionage, cyberwar, communications control and related threats to United States interests*, Jefferson 2013, s. 83–112.

[63] B. Gertz, *China Continuing Cyber Attacks on U.S. Networks* [online], http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/ [dostęp: 28 I 2017]; podobnie: P. Navarro, *China's State-Sponsored Cyber Attacks Must Stop* [online], http://www.theglobalist.com/china-united-states-cyber-crime-politics/ [dostęp: 28 I 2017].

[64] Warto podkreślić, że operacje z udziałem nielegalnych oficerów wymagają wielkich nakładów finansowych i, przede wszystkim, czasu. Równocześnie są to działania niezwykle efektywne i trudne do zneutralizowania przez kontrwywiad, co stwarza ogromne perspektywy wywiadowcze, zob. P. Wieczorek, *Wywiad nielegalny FR w Europie Zachodniej – casus małżeństwa Anschlag*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne. OSW", Warszawa 2013, s. 128 i nast.

[65] O patologii w rosyjskich służbach specjalnych, która objawia się m.in. powszechnym nepotyzmem i kumoterstwem skutkującymi doborem na najwyższe stanowiska na podstawie kryteriów towarzysko-rodzinnych, piszą np. G. Wodolejew, S. Sidorienko, *Spiecnużdy i spiecsłużby*, Sankt Petersburg 2009, cyt za: M. Świerczek, *G. Wodolejew, S. Sidorienko, Spiecnużdy i spiecsłużby, czyli rosyjskie służby specjalne bez makijażu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10, s. 231–232.

[66] Przedstawiona hipoteza jest bardziej prawdopodobna, jeśli uwzględni się rolę, jaką w społeczeństwie i kulturze chińskiej odrywają nieoficjalne kontakty i powiązania znane jako „guānxi". Na temat znaczenia „guānxi" zob. W. Wardęga, *Chiński nacjonalizm*…, s. 367; P. Picquart, *Imperium chińskie. Historia…*, s. 68 i 73; W. Scott Morton, Ch.M. Lewis, *Chiny*..., s. 310–311.

wystarczająco doceniani, mogą czuć się głęboko sfrustrowani. Rozczarowanie i poczucie niesprawiedliwości są zaś ważnymi czynnikami umożliwiającymi wrogim służbom nakłonienie takich osób do podjęcia z nimi współpracy.

Przy analizowaniu kierunków pracy wywiadu ChRL należy rozwinąć podkreślaną już wcześniej charakterystykę tajnych służb chińskich jako instytucji totalnych, wykazujących zainteresowanie wszelkimi informacjami. Nieograniczony zakres danych, którymi jest zainteresowany wywiad ChRL, nie stoi jednak na przeszkodzie określeniu pewnych priorytetów. Najważniejsze cele mogą zostać wyznaczone ze względu na kryteria podmiotowe oraz przedmiotowe. Szczególnym zainteresowaniem wywiadowczym ze względu na kryteria podmiotowe są objęte kraje mające podstawowe znaczenie w polityce międzynarodowej ChRL[67]. Może to wynikać z globalnej pozycji danego państwa oraz wspólnej granicy z ChRL[68]. Ze względu na zajmowaną pozycję we współczesnym świecie na działalność chińskich służb szczególnie są narażone Stany Zjednoczone, Niemcy, Wielka Brytania, Kanada, Francja, Włochy, Rosja i Japonia[69], a także Brazylia, RPA i Indie[70]. Rosja i Japonia są poddane szczególnie intensywnej działalności szpiegowskiej z powodu bezpośredniego sąsiedztwa z ChRL oraz z uwagi na niełatwe wzajemne stosunki. Intensywniejsze działania wywiadowcze są prowadzone na kierunku amerykańskim ze względu na status USA jako najpotężniejszego mocarstwa współczesnego świata i definiowanie przez władze w Pekinie tego kraju jako głównego konkurenta w starciu o pozycję globalnego hegemona. Spośród krajów będących bezpośrednimi sąsiadami ChRL szczególne znaczenie mają także stosunki z Koreą Północną, Wietnamem, Pakistanem i Indiami oraz z Afganistanem, co przekłada się na zainteresowanie wywiadowcze[71].

Po zbadaniu aktywności chińskiego wywiadu na podstawie kryterium przedmiotowego można wskazać następujące obszary jego zainteresowania: gospodarka światowa, nowoczesne technologie, strategie zarządzania[72], trendy w polityce międzynarodowej. W kręgu zainteresowań znalazły się także środowiska nastawione opozycyjnie wobec władz komunistycznych Chin. Szczególnie aktywnie są rozpracowywane mniejszości: tybetańska i ujgurska[73], członkowie sekty Falun Gong[74] oraz środowiska liberalne dążące do demokratyzacji chińskiego systemu politycznego[75].

Po przeanalizowaniu działalności chińskich służb specjalnych przez pryzmat najważniejszych kierunków operacyjnych wyróżnionych na podstawie kryterium podmiotowego, należy stwierdzić, że Polska, nieposiadająca statusu mocarstwa regionalnego

[67] N. Eftimiades, *China*, w: *Routledge Companion to Intelligence Studies*, R. Dover, M.S. Goodman, C. Hillebrand (red.), Abingdon, Oxon 2014, s. 194.

[68] Chiny graniczą z 14 państwami. Są to: Afganistan, Bhutan, Indie, Kazachstan, Kirgistan, Korea Północna, Laos, Myanmar, Mongolia, Nepal, Pakistan, Rosja, Tadżykistan, Wietnam.

[69] Wszystkie wymienione państwa należą do tzw. Grupy G-8 skupiającej najbardziej uprzemysłowione państwa świata; ale członkostwo Federacji Rosyjskiej po aneksji Krymu w marcu 2014 r. zostało zawieszone.

[70] Brazylia, RPA i Indie, oprócz Rosji i Chin, należą do tzw. Grupy BRICS. Państwa zaliczane do tej grupy są uważane za kraje, które w przeciągu najbliższych lat mogą uzyskać status światowych potęg.

[71] Na temat priorytetów chińskiej polityki zagranicznej w kontekście działań wywiadu pisze N. Eftimiades, *China*…, s. 194.

[72] B. Góralczyk, *Miejsce Polski w strategii*…, s. 6.

[73] E.V.W. Davis, *Minority Unrest and Security in China*, w: *China and International Security: History, Strategy, and 21st–Century Policy*, t. 2, D.C. Chau, T. M. Kane (red.), Santa Barbara 2014, s. 37–44.

[74] Falun Gong to współczesny ruch duchowy założony przez Li Hongzhi. Praktykowanie Falun Gong ma na celu doskonalenie jednostki ludzkiej przez ćwiczenia fizyczne, mentalną dyscyplinę i przestrzeganie zasad moralnych, zob. B. Penny, *The Religion of Falun Gong*, Chicago–London 2012, s. 4.

[75] N. Eftimiades, *China*…, s. 194.

ani tym bardziej światowego oraz niemająca wspólnej granicy z ChRL, nie znajduje się w kręgu szczególnego zainteresowania[76]. Istotnymi czynnikami wpływającymi na wzrost zainteresowania Polską ze strony chińskich służb specjalnych są natomiast: członkostwo Polski w Unii Europejskiej, będącej jednym z kluczowych partnerów ChRL, oraz obecność w NATO. Interesujące dla ChRL mogą być również relacje ze Stanami Zjednoczonymi, Niemcami oraz Federacją Rosyjską[77].

Także ze względu na kryterium przedmiotowe zainteresowania chińskich służb Polska nie jest priorytetowym celem, niemniej jednak nie jest też całkowicie pomijana. Terytorium Rzeczpospolitej może przede wszystkim być miejscem służącym do rozpracowania mniejszości chińskich i innych emigracyjnych środowisk opozycyjnych wobec władz w Pekinie. Duża sympatią cieszy się w Polsce idea wolnego Tybetu[78], a ponadto Rzeczpospolita graniczy bezpośrednio z Niemcami – krajem ze znaczną liczebnie mniejszością ujgurską[79]. W latach 80. XX w. szczególne zainteresowanie, a nawet niepokój, ChRL budziła działalność Niezależnego Samorządnego Związku Zawodowego „Solidarność”[80]. Nie można również wykluczyć tego, że Polska jest miejscem wykorzystywanym do zalegendowania oficerów chińskiego wywiadu, którzy pobyt w naszym kraju wykorzystują do zatarcia śladów łączących ich z wywiadem ChRL[81]. Chińskie służby, podobnie jak czynią to w innych krajach, starają się także w Polsce realizować chińskie interesy i wykorzystują do tego działania określane jako *soft power*. Ta strategia sprowadza się do promowania pozytywnego wizerunku Państwa Środka i wykorzystywania zainteresowania jego kulturą[82]. W literaturze poświęconej służbom ChRL zwraca się uwagę na to, że Chińczycy są nastawieni na działania długofalowe[83]. Objawia się to między innymi poszukiwaniem, już na wczesnym etapie, osób, które w przyszłości mogą odgrywać istotną rolę w życiu danego państwa. W tym celu monitoruje się elitarne kierunki

[76] B. Góralczyk, *Miejsce Polski w strategii*…, s. 23–24.

[77] Tamże, s. 28.

[78] K. Bańbor, *Tybetańczycy mogą się uczyć od Polaków. Rozmowa z Yeshim Lhosarem* [online], http://www.wiadomosci24.pl/artykul/tybetanczycy_moga_sie_uczyc_od_polakow_rozmowa_z_yeshim_lhosarem_233827.html [dostęp: 28 I 2017].

[79] Mniejszość ujgurska w Niemczech jest bardzo aktywna. Regularnie urządza protesty przeciwko władzom w Pekinie, zob. B.T. Wieliński, *Niemiecka policja ściga chińskich szpiegów* [online], http://wiadomosci.gazeta.pl/wiadomosci/1,114881,7290092,Niemiecka_policja_sciga_chinskich_szpiegow.html [dostęp: 23 III 2015]. Dodatkowo w Monachium ma swoją siedzibę Światowy Kongres Ujgurów. Według informacji znajdujących się na oficjalnej stronie tej organizacji celem WUC (World Uyghur Congress) jest promowanie demokracji, wolności i praw człowieka oraz sprzeciwianie się okupacji Wschodniego Turkiestanu [online], http://www.uyghurcongress.org/en/?cat=150 [dostęp: 28 I 2017].

[80] M. Goldman, E.J. Perrys, *Changing Meanings of Citizenship in Modern China*, Cambridge 2009, s. 183; *China in the era of Deng Xiaoping: a decade of reform*, M. Ying-Mao Kau, S.H. Marsh (red.), Armonk 1993, s. 312.

[81] Należy pamiętać, że zasadniczo art. 130 kk penalizuje działalność szpiegowską przeciwko Polsce. W związku z tym działalność agentów chińskich prowadzona na terytorium RP, ale wymierzona w interesy innego państwa, nie skutkuje wypełnieniem znamion czynów zabronionych z art. 130 kk. Wyjątkowo, na podstawie art. 138 § 2 kk, art. 130 kk stosuje się odpowiednio, jeżeli czyn zabroniony popełniono na szkodę państwa sojuszniczego, a to państwo zapewnia wzajemność.

[82] Zagadnieniu wykorzystania *soft power* przez ChRL jest poświęcona w całości książka J. Kurlantzicka przywołana w przypisie nr 27; zob. B. Góralczyk, *Miejsce Polski w strategii*..., s. 9.

[83] R. Faligot, *Tajne służby chińskie*…, s. 335; zob. też J. Warrick, C. Johnson, *Chinese Spy 'Slept' In U.S. for 2 Decades* [online], http://www.washingtonpost.com/wp-dyn/content/article/2008/04/02/AR2008040203952.html [dostęp: 28 I 2017]; D. McElroy, *Chinese defector's spy claim* [online], http://www.theage.com.au/news/world/agent-reveals-chinas-web-of-spies/2005/07/03/1120329325678.html [dostęp: 28 I 2017].

studiów, a nawet prestiżowe licea. Osobom wyróżniającym się są oferowane różnego rodzaju stypendia i programy rozwojowe. Celem takich poczynań jest wykreowanie jak najlepszego obrazu Państwa Środka[84].

Podsumowując, należy zaznaczyć, że Polska nie jest najważniejszym podmiotem w polityce ChRL, jednak ze względu na globalny charakter chińskich służb specjalnych, posiadane środki oraz nastawienie władz w Pekinie do działalności szpiegowskiej jest ona narażona na działalność chińskich tajnych służb, a wywiad tego kraju jest jednym z bardziej aktywnych na terenie Rzeczypospolitej.

Chińskie służby mają ułatwione zadanie ze względu na możliwość wykorzystywania hermetycznej i trudnej do rozpracowania przez rodzime służby kontrwywiadowcze chińskiej diaspory oraz swoiste zauroczenie Państwem Środka. Wobec powyższego należy zdecydowanie wzmocnić służby odpowiedzialne za przeciwdziałanie aktywności szpiegowskiej ChRL, gdyż wraz ze wzrostem jej międzynarodowego znaczenia, służby specjalne tego kraju stają się podstawowym oprócz służb rosyjskich zagrożeniem dla bezpieczeństwa Polski.

Bibliografia:

1. Bańbor K., *Tybetańczycy mogą się uczyć od Polaków. Rozmowa z Yeshim Lhosarem* [online], http://www.wiadomosci24.pl/artykul/tybetanczycy_moga_sie_uczyc_od_polakow_rozmowa_z_yeshim_lhosarem_233827.html [dostęp: 28 I 2017].
2. *China in the era of Deng Xiaoping: a decade of reform*, M. Ying-Mao Kau, S.H. Marsh (red.), Armonk 1993, Routledge.
3. Czepielewski S., *Lingua franca made in China* [online], http://www.jows.pl/node/216 [dostęp: 28 I 2017].
4. Davis E.V.W., *Minority Unrest and Security in China*, w: *China and International Security: History, Strategy, and 21st–Century Policy*, t. 2, D.C. Chau, T.M. Kane (red.), Santa Barbara 2014, Praeger.
5. Eftimiades N., *China*, w: *Routledge Companion to Intelligence Studies,* R. Dover, M.S. Goodman, C. Hillebrand (red.), Abingdon 2014, Routledge.
6. Fabisiak R., *China made in Poland* [online], http://weekend.pb.pl/2391587,23084,china-made-in-poland [dostęp: 28 I 2017].
7. Faligot R., *Tajne służby chińskie. Od Mao do igrzysk olimpijskich*, tłum. O. Hedemann, A. Rasińska-Bóbr, Katowice 2009, Sonia Draga.
8. Garwood J., *Scientific espionage*, „Labtimes" 2008, nr 3.
9. Gertz B., *China Continuing Cyber Attacks on U.S. Networks* [online], http://freebeacon.com/national-security/china-continuing-cyber-attacks-on-u-s-networks/ [dostęp: 28 I 2017].
10. Goldman M., Perrys E.J., *Changing Meanings of Citizenship in Modern China*, Cambridge 2009, Harvard University Press.
11. Goodman D., *Deng Xiaoping and the Chinese Revolution: A Political Biography*, London 1994, Routledge.
12. Góralczyk B., *Chińskie wyzwanie nad Wisłą?* [online], http://www.instytutobywatelski.pl/12966/lupa-instytutu/chinskie-wyzwanie-nad-wisla [dostęp: 28 I 2017].

[84] J. Kurlantzick, *Charm Offensive: How China's*…, s. 69.

13. Góralczyk B., *Miejsce Polski w strategii gospodarczej i polityce zagranicznej Chin po przekazaniu władzy na XVIII zjeździe KPCh*; Ekspertyzy GoChina [online], http://www.gochina.gov.pl/ekspertyzy_gochina [dostęp: 28 I 2017].
14. Hannas W.C., Mulvenon J., Puglisi A.B., *Chinese Industrial Espionage: Technology Acquisition and Military Modernisation*, London – New York 2013, Routledge.
15. Hauser F., Häring V., *China-Handbuch: Erkundungen im Reich der Mitte*, Berlin 2005, Trescher.
16. Ho Thanh Ł., Behrendt P., *Zbrojenia morskie a mocarstwowość państw Azji i Pacyfiku,* w: *Azjatyckie strategie bezpieczeństwa u progu XXI wieku*, J. Marszałek-Kawa (red.), Toruń 2014, Adam Marszałek.
17. Huang N.N., *"East is Red": A Musical Barometer for Cultural Revolution. Politics and Culture*, Los Angeles 2008, University of Southern California.
18. Kikolski B., *Plany rozwoju gospodarczego Chin*, „Azja-Pacyfik" 1998, nr 1.
19. Krzyżanowska A., *Biała Księga Obronności Chin – pokojowe deklaracje i realia*, „Bezpieczeństwo Narodowe" 2011, nr 20.
20. Kurlantzick J., *Charm Offensive: How China's Soft Power Is Transforming the World*, New Haven–London 2007, Yale University Press.
21. Lüthi L.M., *Chiny – ZSRR. Zimna wojna w świecie komunistycznym*, tłum. J. Pawłowski, K. Urban-Pawłowska, Warszawa 2011, Dialog.
22. Mackrakis K., *The crown jewels and the importance of scientific-technical intelligence,* w: *East German Foreign Intelligence: Myth, Reality and Controversy*, K. Macrakis, T. Wegener Friis, H. Müller-Enbergs (red.), New York 2010, Routledge.
23. McElroy D., *Chinese defector's spy claim* [online], http://www.theage.com.au/news/world/agent-reveals-chinas-web-of-spies/2005/07/03/1120329325678.html [dostęp: 28 I 2017].
24. Navarro P., *China's State-Sponsored Cyber Attacks Must Stop* [online], http://www.theglobalist.com/china-united-states-cyber-crime-politics/ [dostęp: 28 I 2017].
25. Penny B., *The Religion of Falun Gong*, Chicago – London 2012, The University of Chicago Press.
26. Picquart P., *Imperium chińskie. Historia i teraźniejszość chińskiej diaspory*, tłum. I. Kałużyńska, Warszawa 2006, Dialog.
27. Piekarski M., *Miliardy złotych nielegalnie przelewane z Polski do Chin* [online], http://www.rmf24.pl/fakty/polska/news-miliardy-zlotych-nielegalnie-przelewane-z-polski-do-chin,nId,388590? [dostęp: 28 I 2017].
28. Poindexter F., *The Chinese information war: espionage, cyberwar, communications control and related threats to United States interests*, Jefferson 2013, McFarland.
29. *Revealing China's Hegemonic Project in Thailand: How the Confucius Institute Furthers the Chinese State's International Ambitions. Paper presented at the 12th International Conference on Thai Studies 22-24 April 2014 University of Sydney* [online], http://sydney.edu.au/southeast-asia-centre/documents/pdf/auethavorn-pipat-ruji.pdf [dostęp: 27 I 2017].
30. Scott Morton W., Lewis Ch.M., *Chiny. Historia i kultura*, tłum. B.S. Zemanek, Kraków 2007, Wydawnictwo Uniwersytetu Jagiellońskiego.
31. Shen H., *Instytut Konfucjusza – chiński urok czy ukryty Mao* [online], http://www.fronda.pl/a/instytut-konfucjusza-chinski-urok-czy-ukryty-mao,3870.html [dostęp: 28 I 2017].

32. Siemiątkowski Z., *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009, Aspra.
33. *Straty Skarbu Państwa w VAT – luka podatkowa, oszustwa, wyłudzenia oraz problematyka podatku od towarów i usług w Polsce* [online], Warszawa 2013, PwC, https://www.pwc.pl/pl/publikacje/assets/pwc_straty_skarbu_panstwa_w_vat.pdf [dostęp: 28 I 2017].
34. Su S., *China: eine Einführung in Geschichte, Kultur und Zivilisation,* Gütersloh–München 2008, Chronik.
35. Sun Tzu, *The Art of War by Sun Tzu – Classic Edition,* tłum. angielskie L. Giles, B. Wiliams, S. Kim, El Paso 2009, El Paso Norte Press.
36. Sunzi, *Sztuka wojny i 36 forteli*, tłum J. Zawadzki, Seattle 2012, CreateSpace.
37. Szymowski L., *Chińska mafia wkracza do Polski* [online], http://www.polskatimes.pl/artykul/156020,chinska-mafia-wkracza-do-polski,id,t.html [dostęp:28 I 2017].
38. Świerczek M., *G. Wodolejew, S. Sidorienko, Spiecnużdy i spiecsłużby, czyli rosyjskie służby specjalne bez makijażu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10.
39. *The World Factbook, China* [online], https://www.cia.gov/library/publications/the-world-factbook/geos/ch.html [dostęp: 28 I 2017].
40. Vogel F., *Deng Xiaoping and the Transformation of China*, Cambridge 2011, Harvard University Press.
41. Walczak D., *Wietnamska mafia wyprowadza z Polski gigantyczne pieniądze* [online], http://sledczy.focus.pl/afery-kryminalne/wietnamska-mafia-wyprowadza-z-polski-gigantyczne-pieniadze-154?strona=3 [dostęp: 28 I 2017].
42. Wardęga J., *Chiński nacjonalizm. Rekonstruowanie narodu w Chińskiej Republice Ludowej,* Kraków 2014, Wydawnictwo Uniwersytetu Jagiellońskiego.
43. Warrick J., Johnson C., *Chinese Spy 'Slept' In U.S. for 2 Decades* [online], http://www.washingtonpost.com/wp-dyn/content/article/2008/04/02/AR2008040203952.html [dostęp: 28 I 2017].
44. Wieczorek P., *Wywiad nielegalny FR w Europie Zachodniej – casus małżeństwa Anschlag,* „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie Specjalne" 2013, COS ABW, OSW.
45. Wieliński B.T., *Niemiecka policja ściga chińskich szpiegów* [online], http://wiadomosci.gazeta.pl/wiadomosci/1,114881,7290092,Niemiecka_policja_sciga_chinskich_szpiegow.html [dostęp: 23 III 2015].
46. *Wirtschaftsspionage. Risiko für Unternehmen, Wissenschaft und Forschung*, Köln 2014, Bund Länder.
47. Wodolejew G., Sidorienko S., *Spiecnużdy i spiecsłużby*, Sankt Petersburg 2009, Izdatiel'skij Dom Azbuka-Klassika.
48. Woliński B., *Restrukturyzacja i prywatyzacja chińskich przedsiębiorstw*, „Azja–Pacyfik" 2006, nr 9.
49. Zajączkowski K., *ChRL wobec krajów Południa (na przykładzie Afryki Subsaharyjskiej). Szansa czy zagrożenie dla międzynarodowej pozycji UE*, w: *Chiny–Indie. Ekonomiczne skutki rozwoju*, K. Kłosiński (red.), Lublin 2008,Wydawnictwo KUL.

Źródła internetowe:

1. http://facet.interia.pl/styl-zycia/ciekawostki/news-chinscy-szpiedzy-sa-wsrodnas,nId,448718 [dostęp: 27 I 2017].
2. https://fas.org/irp/world/china/pla/gen_staff.htm [dostęp: 15 II 2017].
3. https://webspeicher.wordpress.com/2011/06/10/spionage-chinas-stasi-chinas-spion-deutschland-gericht-11294831/ [dostęp: 27 I 2017].
4. http://www.asianlii.org/cn/legis/cen/laws/clotproc361/ [dostęp: 28 I 2017].
5. http://www.chinadaily.com.cn/english/doc/2006–03/10/content_530648.htm [dostęp: 23 III 2015].
6. http://www.faz.net/aktuell/gesellschaft/spionage-china-setzt-frauen-auf-botschafter-an-14490421.html [dostęp: 28 I 2017].
7. http://www.gazetakrakowska.pl/artykul/201494,general-czempinski-chinscy-szpiedzy-sa-juz-w-polsce,id,t.html [dostęp: 28 I 2017].
8. http://www.instytutkonfucjusza.uj.edu.pl/o-nas/historia [dostęp: 28 I 2017].
9. https://www.justice.gov/opa/pr/chinese-national-sentenced-prison-conspiracy-steal-trade-secrets [dostęp: 27 I 2017].
10. https://www.justice.gov/opa/pr/us-nuclear-engineer-china-general-nuclear-power-company-and-energy-technology-international [dostęp: 28 I 2017].
11. http://www.pwc.pl/pl/media/2016/2016-11-23-luka-vat-2016.html [dostęp 28 I 2017].
12. https://www.rt.com/uk/358191-g20-uk-chinese-honeytrap/ [dostęp: 28 I 2017].
13. http://www.spacedaily.com/news/china-05zw.html [dostęp: 27 I 2017].
14. http://www.theepochtimes.com/n3/1018292-hosting-confucius-institute-a-bad-idea-says-intelligence-veteran/ [dostęp: 27 I 2017].
15. https://www.theguardian.com/technology/2016/aug/11/espionage-arrest-of-nuclear-engineer-fuels-us-suspicions-of-chinese-tactics [dostęp: 28 I 2017].
16. http://www.uyghurcongress.org/en/?cat=150 [dostęp: 28 I 2017].
17. https://www.washingtonpost.com/news/checkpoint/wp/2016/04/11/the-fall-of-edward-lin-the-navy-pilot-accused-of-espionage-and-patronizing-a-prostitute/?utm_term=.8b919c896471 [dostęp: 27 I 2017].

Abstrakt

Zamierzeniem artykułu jest udzielenie odpowiedzi na pytanie, czy działalność wywiadu Chińskiej Republiki Ludowej stanowi zagrożenie dla bezpieczeństwa państwa polskiego oraz interesów jego obywateli. W artykule przedstawiono wybrane aspekty działalności służb wywiadowczych ChRL. Omówiono nastawianie władz chińskich do działań szpiegowskich oraz znaczenie niejawnie zdobytych informacji dla rozwoju gospodarczego i politycznego Państwa Środka. Przedstawiono również główne metody i sposoby działań służb wywiadowczych ChRL, w tym aktywne wykorzystywanie licznej diaspory chińskiej. Przeanalizowano skalę działań podejmowanych przez Chińską Republikę Ludową w celu uzyskania istotnych informacji oraz rozmiar zaangażowanych środków. W dalszej części artykułu zaprezentowano główne kierunki, zarówno podmiotowe, jak i przedmiotowe, zainteresowania wywiadu ChRL. Przeanalizowanie wskazanych wyżej aspektów szpiegowskiej działalności podejmowanej przez Państwo Środka prowadzi do wniosku, że służby wywiadowcze Chin osiągnęły status służb globalnych, działają-

cych z ogromnym rozmachem we wszystkich zakątkach świata. Ta konstatacja prowadzi z kolei do wniosku, że wywiad ChRL jest istotnym zagrożeniem także dla bezpieczeństwa Polski.

Słowa kluczowe: wywiad, Chiny, szpiegostwo, Guó'ān bù, Gōng'ān bù.

Abstract

The main goal of the presented paper is to answer the question if the activity of the Chinese intelligence poses a threat to Polish state, its interest and welfare of its citizens. To fulfill this task, the presented paper depicts the chosen aspects of the activities of the Chinese intelligence services. The paper is concerned, inter alia, with the attitude of the Chinese government towards intelligence activity and with the importance of a confidential data to development of the Chinese industry. There have also been presented the main means and methods, used by Chinese services to acquire coveted data, including the activities and wide utilization of the so called Overseas Chinese. A passage is also devoted to the issue of the scale of conducted actions and the magnitude of means that are used to collect important information. The further part of the paper describes the major, both subjective as well as objective, directions of the Chinese intelligence's interests.

The analyses lead to the conclusions that the Chinese intelligence services have attained the position of global, spy institutions that operate in any country and seek any information. These statement in turn, allows to enunciate the thesis that the Chinese intelligence poses a real threat to Poland as well.

Keywords: China, intelligence, espionage, Guó'ān bù, Gōng'ān bù.

Karol Falandys

Wybrane aspekty tworzenia Narodowego Systemu Odzyskiwania Obywateli RP – środka służącego zwiększeniu bezpieczeństwa Polaków przebywających poza granicami państwa

Książę lub generał najlepiej zademonstruje swój geniusz, planując operacje dokładnie tak, by idealnie balansować między maksymalizacją celów operacyjnych w stosunku do zaplecza, jakim dysponuje tak, by nie zrobić za dużo ani za mało.

Carl von Clausewitz

Praca organizacji nigdy nie dobiega końca, a jej struktura musi być stale modyfikowana w stosunku do zmieniającego się otoczenia.

Ralph J. Cordiner, amerykański biznesmen, prezes i dyrektor generalny General Electric

W obecnych czasach istotnym problemem wielu państw spoza cywilizacji zachodniej są regionalne i wewnątrzpaństwowe konflikty powodujące m.in. destabilizację społeczno-polityczną. Ubocznym skutkiem tego jest m.in. zwiększająca się liczba porwań dla okupu – jednego ze sposobów finansowania konfliktów zbrojnych, walk narodowo-wyzwoleńczych i separatystycznych, a także funkcjonowania ugrupowań terrorystycznych. Jednocześnie ten przestępczy proceder jest dla niektórych grup społecznych jedynym źródłem przetrwania[1].

W czasach, kiedy można swobodnie przekraczać granice, ten problem zaczyna coraz częściej dotyczyć również obywateli Rzeczpospolitej Polskiej. Potwierdzeniem tego stanu rzeczy jest analiza szefa Zakładu Studiów Strategicznych Uniwersytetu Adama Mickiewicza w Poznaniu, prof. Sebastiana Wojciechowskiego, przeprowadzona kilka lat temu na zlecenie Ministerstwa Spraw Wewnętrznych i Administracji RP stwierdzająca, że **Polacy są coraz bardziej narażeni na porwania**[2].

Kłopot z zapewnieniem bezpieczeństwa Polakom przez państwo polskie można było zauważyć podczas „arabskiej wiosny", kiedy to wystąpiły problemy ze sprowadzeniem do kraju polskich turystów z Egiptu oraz Polaków zatrudnionych w firmach wydobywczych w Libii. Ewakuacja tych ostatnich była możliwa dzięki siłom i środkom Wielkiej Brytanii oraz Republiki Federalnej Niemiec, które przy okazji operacji odzyskiwania swoich obywateli pomogły również Polakom[3].

[1] K. Falandys, *Zjawisko izolacji (bezprawnego przetrzymywania) – jego skala i regionalizacja*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 178–194.

[2] G. Starzak, *Polacy coraz częściej stają się ofiarami porwań za granicą* [online], http://www.dziennikpolski24.pl/pl/aktualnosci/kraj/903679-polacy-coraz-czesciej-staja-sie-ofiarami-porwan-za-granica.html [dostęp: 17 IX 2016].

[3] K. Falandys, *Zjawisko izolacji*…, s. 194.

Jedną z zasad demokratycznego państwa prawa jest m.in. ochrona wartości istotnych ze społecznego punktu widzenia oraz zapewnienie obywatelom minimum bezpieczeństwa. Warto przytoczyć art. 36 *Konstytucji Rzeczypospolitej Polskiej*, który stanowi, że (…) *Podczas pobytu za granicą obywatel polski ma prawo do opieki ze strony Rzeczypospolitej Polskiej*[4]. Z tego zapisu wynika, że każdy porwany lub zaginiony obywatel RP ma prawo oczekiwać podjęcia stosownych działań ze strony państwa polskiego mających na celu jego uwolnienie i sprowadzenie do kraju[5].

W dokumentach wytworzonych przez Zespół do Spraw Sytuacji Szczególnych przy ministrze obrony narodowej jest mowa o innym ważnym problemie. Mianowicie, odzyskiwanie obywateli izolowanych[6] stanowi niezwykle ważny czynnik integrujący społeczeństwo z państwem i jego strukturami, przez co zwiększa się zaufanie do instytucji państwowych, a to może wzmacniać (…) *śmiałość i gotowość do uczestnictwa w realizacji trudnych zadań, związanych nawet z wysokim stopniem ryzyka*[7].

Jednocześnie powinno się mieć na względzie, że:

> (…) w ostatnich dwóch dekadach sytuacje dotyczące personelu narażonego na ryzyko izolacji oraz osób wziętych jako zakładników stały się przedmiotem ogromnego zainteresowania mediów oraz opinii społecznej. Powszechny dostęp do informacji oraz możliwość informowania społeczeństwa na bieżąco o sytuacji bezprawnie przetrzymywanych może kreować zarówno sytuację polityczną, jak i prowadzić do zasadniczej zmiany planów politycznych (rezygnacja z realizacji planów lub podjęcie działań) bądź zmiany koncepcji prowadzenia operacji militarnej czy użycia sił specjalnych[8].

Odkąd Polska została członkiem Paktu Północnoatlantyckiego i Unii Europejskiej zgodziła się wypełniać zobowiązania sojusznicze i międzynarodowe, w tym zbudować

---

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

[5] K. Falandys, *Zjawisko izolacji*…, s. 180.

[6] Personel Izolowany (ang. *Isolated Personnel* – IP) – personel wojskowy lub cywilny, który jest odłączony od jednostki lub organizacji, do której należy, w sytuacji gdy oczekując na uwolnienie, może on być zmuszony do walki o przetrwanie, ucieczki lub przeciwstawiania się wykorzystywaniu, *NATO Joint Doctrine for Personnel Recovery*, MCASB (Military Committee Air Standardisation Board), 2007, AJP-3.3.9 (SD-8), s. 4.

To określenie jest również propozycją na oficjalną definicję dla NATO i UE. Za osobę izolowaną można też uznać tego, kto zatrzymał się w podróży z powodu braku paliwa w aucie, którym podróżuje, lub został zmuszony do przerwania podróży ze względu na jakąkolwiek awarię lub wypadek, niezależnie od tego, czy takie zdarzenie zostało spowodowane interwencją osób trzecich. Zob. *Personnel Recovery,* JAPCC (Joint Air Power Competence Centre), 2011, s. 1.

Izolowanie personelu może nastąpić w czterech przypadkach:

1) **prowadzenia działań bojowych na teatrze** (ang. *isolated*) – dotyczy to przede wszystkim żołnierzy oraz funkcjonariuszy biorących udział w działaniach bojowych,

2) **zagubienia, braku orientacji w terenie lub wskutek wypadku** (ang. *missing*) – dotyczy zarówno żołnierzy, funkcjonariuszy biorących udział w działaniach bojowych, jak i cywilów przebywających w danym rejonie geograficznym, takich jak żeglarze, podróżnicy itp.,

3) **zatrzymania przez siły rządowe, władze lokalne** (ang. *detained*) – dotyczy przede wszystkim pracowników misji dyplomatycznych, turystów łamiących lokalne prawo itp.,

4) **uprowadzenia przez bojowników lub ugrupowania przestępcze i terrorystyczne** (ang. *captured*) – dotyczy wszystkich grup obywateli RP przebywających poza granicami kraju, cyt. za: *Odzyskiwanie izolowanego personelu (DD/3.3.9)*, Warszawa 2010, s. 6.

[7] *Koncepcja i ogólne zasady funkcjonowania Narodowego Systemu Odzyskiwania Personelu Wojskowego,* Warszawa 2008, s. 10.

[8] K. Falandys, *Zjawisko izolacji*…, s. 179.

narodowy system odzyskiwania swoich obywateli. Poprzestała jednak na utworzeniu narodowego systemu odzyskiwania personelu[9] wojskowego, rezygnując niejako ze stworzenia kompleksowego narodowego systemu odzyskiwania obywateli RP[10], co w ocenie autora było błędem.

W obecnej sytuacji międzynarodowej wydaje się istotne, aby przyszły narodowy system odzyskiwania obywateli RP był traktowany

> (…) jako element systemu ponadnarodowego, opartego na strukturze organizacyjnej Paktu Północnoatlantyckiego i Unii Europejskiej. Tym samym, poza dążeniem do stworzenia w ramach tych organizacji systemu odzyskiwania personelu, ważnym jest wdrożenie uniwersalnych rozwiązań określających procedury działania, jak i charakterystykę wykorzystywanego potencjału. Zadaniem państwa polskiego w zakresie budowy narodowego systemu odzyskiwania personelu jest więc zarówno stworzenie systemu działań w ramach NATO i UE oraz opracowanie i wdrożenie narodowych rozwiązań w pełni skorelowanych z procedurami tych dwóch organizacji[11].

W Polsce dobrze funkcjonuje system ratownictwa lotniczego i morskiego[12], niestety ogranicza się on tylko do działań poszukiwawczo-ratowniczych na terenie kraju w czasie pokoju. *Tymczasem istotą Personnel Recovery jest działanie w sytuacji kryzysu i poza granicami państwa*[13].

Do operacji odzyskiwania personelu prowadzonych najczęściej na terytorium obcego państwa, jak również w sytuacjach możliwego występowania zagrożenia ze strony przeciwnika, możemy zaliczyć: **bojowe akcje poszukiwawczo-ratownicze** (*Combat Search and Rescue* – CSAR) oraz **bojowe odzyskiwanie** (*Combat Recovery* – CR). Przy bardzo dużym rzeczywistym zagrożeniu ze strony przeciwnika, po wyczerpaniu wszystkich innych możliwości odzyskania osób izolowanych, będzie przeprowadzane **niekonwencjonalne odzyskiwanie personelu** (*Non-conventional Assisted Recovery* – NAR) i **uwalnianie zakładników** (*Hostage Rescue* – HR). Ponadto może wystąpić również potrzeba **odzyskania ekwipunku** (*Recovering Equipment*) oraz tzw. **personelu pozostałego**[14] (*Other Personnel*), wobec którego stosuje się działania określane jako **akcja ewakuacyjna** (*Non-combatant Evacuation Operation* – NEO)[15].

Aby narodowy system odzyskiwania obywateli RP mógł spełniać swoje podstawowe zadania polegające m.in. na przeprowadzaniu powyższych operacji odzyskiwania

---

[9] Odzyskiwanie Izolowanego Personelu (ang. Personnel Recovery – PR) – jest sumą działań wojskowych, dyplomatycznych i cywilnych mających na celu odzyskanie i reintegrację IP. Zob. *Odzyskiwanie izolowanego personelu...*, s. 6. Powyższa definicja ma zostać przedstawiona jako ostateczna zarówno dla NATO, jak i dla UE. To oznacza, że będzie podjęte każde działanie mające na celu odzyskanie personelu, za który ponosi się odpowiedzialność, gdy tylko znajdzie się on w sytuacji zagrożenia. Definicja celowo nie podaje ograniczonej listy środków, z których można korzystać w czasie działań. Zob. *Personnel Recovery,* JAPCC, 2011, s. 1.

[10] Tamże, s. 178–179.

[11] K. Falandys, *Uwarunkowania prawne determinujące kształt Narodowego Systemu Odzyskiwania Obywateli Rzeczypospolitej Polskiej*, „Rocznik Bezpieczeństwa Wewnętrznego" 2015, t. 9, nr 2, s. 141.

[12] Do tego systemu możemy zaliczyć np. Morską Służbę Poszukiwania i Ratownictwa, powołaną do życia 1 I 2002 r. Zob. http://www.sar.gov.pl/pl/podstawy-prawne [dostęp: 18 IX 2016].

[13] K. Falandys, *Uwarunkowania prawne*…, s. 146.

[14] Tak określa się wszystkie osoby znajdujące się na terenie operacyjnym i jednocześnie nieposiadające statusu urzędnika państwowego (instytucji ponadnarodowej). Dotyczy to zwłaszcza członków organizacji pozarządowych, reporterów itp.

[15] *Personnel Recovery*, JAPCC, 2011, s. 2.

personelu, niezbędne są siły – w postaci wyspecjalizowanej jednostki poszukiwawczo-ratowniczej[16] – i środki – ustanowienie przepisów umożliwiających utworzenie nowej bazy danych *ISOPREP*[17], zawierającej informacje niezbędne do przeprowadzenia operacji *Personnel Recovery.* Konieczne jest także umiejscowienie wspomnianej jednostki w odpowiednich strukturach administracji państwowej. Jednocześnie autor publikacji proponuje przyjęcie poniższej definicji narodowego systemu odzyskiwania obywateli RP:

> Zespół wzajemnie uzupełniających się militarnych, politycznych i cywilno-prawnych przedsięwzięć organizacyjnych, planistycznych i szkoleniowych, mających na celu przygotowanie personelu, sił i środków do wykonywania zadań związanych z udzieleniem pomocy lub odzyskaniem personelu znajdującego się w nieznanym, niedostępnym lub wrogim środowisku na skutek zagubienia, przechwycenia lub uprowadzenia[18].

Umiejscowienie jednostki w odpowiednich strukturach administracji państwowej

W operacjach odzyskiwania personelu izolowanego jednym z najważniejszych elementów (jeśli nie najważniejszym) jest czas, gdyż największe prawdopodobieństwo odzyskania osób występuje w fazach porwania i transportu. Dlatego też autor wskazuje na potrzebę maksymalnego skrócenia drogi podejmowania decyzji politycznej o rozpoczęciu jednej ze wskazanych wcześniej operacji odzyskiwania.

Podporządkowanie systemu ministrowi obrony narodowej – niejako automatycznie – będzie skutkowało potrzebą uruchomienia długotrwałej procedury wysłania kontyngentu wojskowego poza granice kraju. Ponadto wysyłanie żołnierzy Sił Zbrojnych RP na terytorium innego państwa może powodować problemy natury politycznej na arenie międzynarodowej.

Ministerstwo Spraw Wewnętrznych i Administracji, w ocenie autora, nie jest w stanie przeprowadzić bojowej operacji odzyskiwania personelu poza granicami państwa, gdyż funkcjonariusze MSWiA nie mają przygotowania wojskowego niezbędnego do zorganizowania i przeprowadzenia tak skomplikowanej operacji.

Na podobne problemy natknęły się służby niemieckie podczas operacji odzyskiwania frachtowca „Hans Stavanger". Pojawiły się wówczas doniesienia o trudnościach w organizacji i współdziałaniu między Ministerstwem Obrony i Marynarką Wojenną Niemiec z jednej strony a Ministerstwem Spraw Wewnętrznych i GSG 9 z drugiej[19].

Najwłaściwszą instytucją do przeprowadzania tego typu operacji jest, w ocenie autora, Ministerstwo Spraw Zagranicznych, co wynika z ustawowego obowiązku tegoż resortu, tj. że reprezentuje on Rzeczpospolitą Polską i jej obywateli na arenie międzynarodowej[20]. *Rolą MSZ jest podjęcie natychmiastowych działań ukierunkowanych na odzyskanie izolowanej osoby lub mienia, także przy wykorzystaniu środków pozostających*

---

[16] Nazwa robocza zaproponowana przez autora.

[17] *ISOPREP* (ang. ***ISO****lated* ***P****ersonnel* ***Rep****ort*) – deklaracja personelu narażonego na izolację.

[18] K. Falandys, *The development process of the national polish citizens recovery system,* „Zeszyty Naukowe WSOWL" 2015, t. 47, nr 3, s. 6.

[19] Zob. K. Kubiak, *Przemoc na oceanach. Współczesne piractwo i terroryzm morski*, Warszawa 2009, s. 144.

[20] Art. 13 i 32 *Ustawy z dnia 4 września 1997 r. o działach administracji rządowej* (tekst jednolity: Dz.U. z 2016 r. poz. 543) oraz § 1 *Rozporządzenia Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Spraw Zagranicznych* (Dz.U. z 2015 r. poz. 1899, ze zm.).

w gestii innych resortów[21]. Taką możliwość daje artykuł 5 ustawy z 8 sierpnia 1996 r. o Radzie Ministrów, który stanowi, że *W celu wykonania zadań i kompetencji określonych w Konstytucji Rzeczypospolitej Polskiej i ustawach, Prezes Rady Ministrów może w szczególności:*

1) wyznaczyć ministrowi zakres spraw, w których minister ten działa z upoważnienia Prezesa Rady Ministrów[22].

Czynności powinny być prowadzone od chwili zaistnienia zdarzenia i uwzględniać przedsięwzięcia dyplomatyczne w państwie izolacji oraz na arenie międzynarodowej. Przede wszystkim w państwie izolacji należy podjąć działania w celu uwolnienia przetrzymywanych, a w dalszej kolejności – uzyskać zgodę na personalne wzmocnienie placówki, zwiększenie jej ochrony oraz uzyskanie wiz dla osób kierowanych do państwa wystąpienia izolacji, których zadaniem jest odzyskanie obywateli RP. Jednocześnie powinny być prowadzone działania dyplomatyczne w celu uzyskania międzynarodowej aprobaty dla operacji poszukiwawczo-ratowniczych, a także należy postarać się o stosowne pozwolenia, np. na przelot statków powietrznych biorących udział w odzyskiwaniu izolowanego personelu[23]. Główna rola resoru spraw zagranicznych w działaniach ukierunkowanych na uwolnienie bezprawnie izolowanych polskich obywateli wynika z uwarunkowań o charakterze operacyjnym. Działania prowadzące do odzyskania personelu sprowadzają się do szybkiego przemieszczenia sił odzyskujących we właściwy rejon. Istotą takiej operacji jest uwolnienie i ewakuacja przetrzymywanych osób, przeprowadzone przy użyciu minimalnych sił i przez szybkie ich zorganizowanie oraz wycofanie się. Ponadto operacja odzyskiwania i ewakuacji powinna być poprzedzona przedsięwzięciami mającymi na celu lokalizację uprowadzonych osób, uzyskanie informacji o otoczeniu i warunkach, w jakich przebywają, oraz ewentualnie o ich stanie psychofizycznym. Te dane będą pozyskiwane właśnie dzięki placówkom dyplomatycznym. Osobami najlepiej znającymi środowisko zdarzenia izolacji będą pracownicy misji dyplomatycznych, ich kontakty osobowe oraz pracownicy organizacji rządowych, pozarządowych lub międzynarodowych, zaprzyjaźnieni z Polską.

Innym czynnikiem o charakterze operacyjnym, podkreślającym rolę MSZ i placówek dyplomatycznych, jest problem konsekwencji politycznych operacji. Ważne są przygotowania do podjęcia działań odzyskujących prowadzonych na terenie obcego państwa. Te działania będą przebiegały przy zainteresowaniu mediów, nawet jeżeli zostanie otrzymana zgoda władz tego kraju. Tym samym konieczne jest nie tylko zapewnienie skrytości działań, lecz także niwelowanie konsekwencji, jakie może spowodować skierowanie uzbrojonego komponentu na terytorium obcego państwa. Nagłośnienie przez media prowadzonych działań odzyskujących może kreować sposób nastawienia społecznego i pośrednio wpływać na decyzje władz politycznych. Zadaniem placówek dyplomatycznych będzie więc prowadzenie czynności ograniczających negatywne skutki działań przygotowawczych.

Ewentualnym najpoważniejszym ograniczeniem w odniesieniu do czynności dyplomatycznych prowadzonych w fazie przygotowań do operacji odzyskiwania personelu izolowanego przez resort spraw zagranicznych jest istota prowadzenia działań dyplomatycznych. Ich celem jest nienaruszanie poprawnych stosunków między państwami. Tymczasem efektywność wymaga, aby operacje *Personnel Recovery* były wykonane w odpowiednim czasie, który powinien być poprzedzony rozwinięciem sił – w tym roz-

[21] K. Falandys, *The development process*…, s. 14.

[22] *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 marca 2012 r. w sprawie ogłoszenia jednolitego tekstu ustawy o Radzie Ministrów* (Dz.U. z 2012 r. poz. 392).

[23] K. Falandys, *The development process*…, s. 13–14.

poznawczych i łącznikowych – oraz prowadzeniem działań zapobiegawczych. To może doprowadzić do konfliktu pomiędzy wymaganiami dyplomatycznymi i wojskowymi, co w rezultacie może spowodować, że dyplomaci uznają operację odzyskiwania za rozwiązanie ostateczne i decyzja o jej rozpoczęciu zapadnie zbyt późno[24].

Podobne obawy zostały również ujęte w sojuszniczej doktrynie AJP – 3.4.2[25], która wskazuje, że *Ewakuacje zagrożonego personelu niewojskowego są inicjatywami dyplomatycznymi*[26]. Do kompetencji placówek dyplomatycznych każdego państwa należy obowiązek podjęcia działań dyplomatycznych mających na celu odzyskanie własnych obywateli i mienia, a także przygotowanie planów ewakuacji oraz zapewnienie bezpieczeństwa ewakuowanym osobom[27].

Zadania związane z odzyskiwaniem obywateli RP nałożone na ministra spraw zagranicznych muszą skutkować zobowiązaniem służb specjalnych Rzeczpospolitej Polskiej do pełnego informowania ministra i przekazywania mu wszelkich informacji dotyczących spraw związanych z uprowadzonymi obywatelami RP.

W podsumowaniu powyższych rozważań należy jednoznacznie zauważyć, że efektywność operacji odzyskiwania obywateli wymaga tego, aby proces decyzyjny był krótki. Zdaniem autora minister spraw zagranicznych powinien otrzymać uprawnienia do samodzielnego podejmowania decyzji w sprawie przeprowadzenia operacji CSAR, CR, NEO oraz – jeśli będzie to dotyczyło sprzętu niewojskowego istotnego ze względu na bezpieczeństwo państwa – odzyskania ekwipunku. Natomiast w przypadku operacji NAR i HR minister spraw zagranicznych powinien uprzednio uzyskać zgodę Prezesa Rady Ministrów na przeprowadzenie tego typu operacji[28].

Powołanie wyspecjalizowanej jednostki poszukiwawczo-ratowniczej

Na podstawie obserwacji funkcjonowania narodowego systemu odzyskiwania personelu wojskowego można pokusić się o stwierdzenie, że aby narodowy system odzyskiwania obywateli RP mógł działać efektywnie, to powinna się w nim znaleźć – oprócz wyżej wymienionych elementów – wyspecjalizowana jednostka poszukiwawczo-ratownicza, przygotowana do prowadzenia operacji odzyskiwania osób.

Przy opracowywaniu, funkcjonowaniu[29] oraz prowadzeniu operacji odzyskiwania najważniejsza powinna być ta sama zasada, która towarzyszy operacjom bezpieczeństwa (ang. *Operations Security* – OPSEC):

> Operacja bezpieczeństwa, lub OPSEC, jest procesem, w którym chronimy informacje jawne mogące być wykorzystane przeciwko nam. Ten typ operacji wymaga, aby spojrzeć na siebie oczami przeciwnika (osób, grup, państw, organizacji). Zasadniczo każdy, kto może zaszkodzić ludziom, środkom lub misji, jest uważany za przeciwnika.
>
> OPSEC powinny być wykorzystywane do ochrony informacji, a tym samym – uniemożliwić przeciwnikowi przeciwdziałanie[30].

[24] Tamże, s. 14–15.

[25] *Połączona doktryna sojusznicza prowadzenie operacji ewakuacji personelu niewojskowego NATO*, AJP – 3.4.2, 2007 r., s. 18.

[26] Tamże, s. 23.

[27] K. Falandys, *The development process*…, s. 13.

[28] Tamże, s. 14.

[29] Na przykład struktura, posiadane siły, środki itp.

[30] Tłumaczenie autora. Zob. http://www.dodea.edu/Offices/Safety/OPSEC.cfm [dostęp: 25 IX 2016].

Odejście od skrytości działań może mieć duży wpływ na niepowodzenie operacji, co może się przełożyć na śmierć osób izolowanych bądź osób wchodzących w skład sił odzyskujących. Potwierdzeniem konieczności stosowania zasady OPSEC niech będą dwa poniższe przykłady. W dniu 8 marca 2012 r. ekstremiści z Boko Haram z powodu nieudanej akcji odbicia zakładników przez siły nigeryjsko-brytyjskie przeprowadzili egzekucję dwóch europejskich inżynierów: Brytyjczyka Chrisa McManusa i Włocha Franka Lamolinara. Kilka miesięcy później, 31 maja 2012 r., z powodu uzyskania informacji o przygotowaniach do odbicia zakładnika, bojownicy tejże organizacji zastrzelili Niemca porwanego w styczniu tego samego roku[31].

Wydaje się zasadne, aby skład postulowanej jednostki poszukiwawczo-ratowniczej tworzyli żołnierze, funkcjonariusze i pracownicy MON, AW, SWW, ABW, SKW, MSZ. Struktura organizacyjna natomiast powinna zawierać następujące komórki:

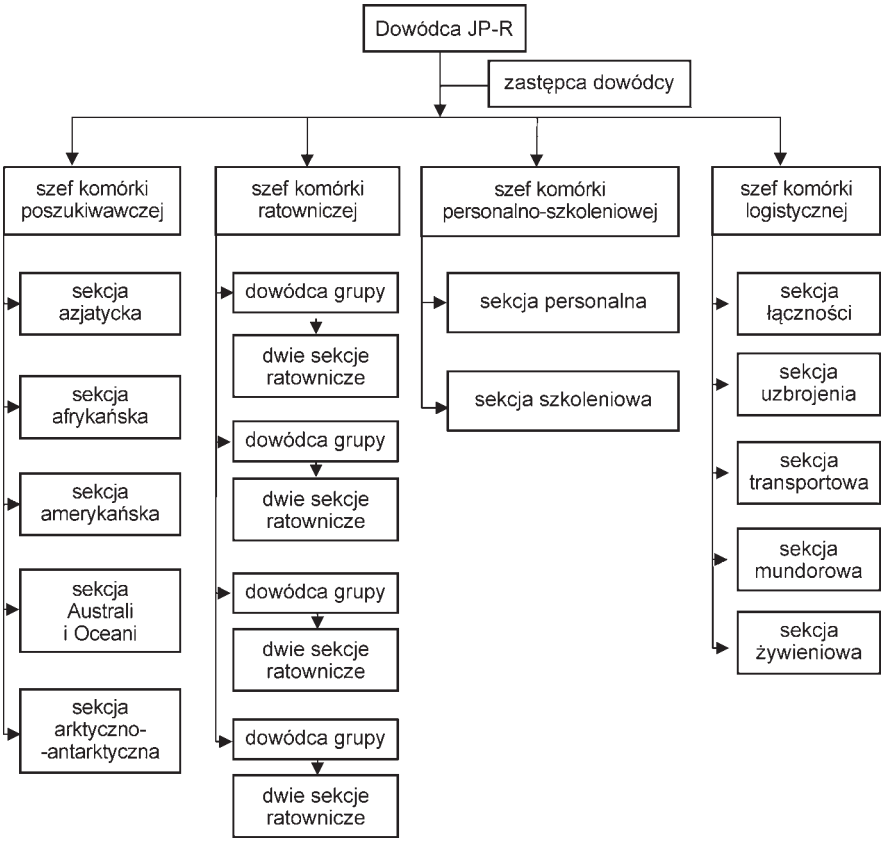
- poszukiwawczą – w celu prowadzenia działań operacyjnych ukierunkowanych na zlokalizowanie i niesiłowe odzyskanie personelu. W jej skład powinni wchodzić funkcjonariusze i pracownicy AW, SWW i MSZ,
- ratowniczą – w celu fizycznego przeprowadzania operacji odzyskiwania personelu. Ta komórka powinna się składać z wyselekcjonowanych żołnierzy i funkcjonariuszy MON,
- personalno-szkoleniową – w celu prowadzenia szkoleń SERE dla funkcjonariuszy i pracowników MSZ, MSW, AW, ABW, SWW, SKW, Kancelarii Sejmu i Kancelarii Senatu oraz innych instytucji, organizacji i firm. Ponadto powinna ona zajmować się wytwarzaniem, przetwarzaniem, przechowywaniem i udostępnianiem kart *ISOPREP* oraz sprawami kadrowymi jednostki. Powinni do niej być oddelegowani żołnierze i funkcjonariusze MON oraz ABW,
- zabezpieczenia logistycznego – której zadanie polegałoby na wyposażaniu jednostki w odpowiedni sprzęt specjalistyczny. W jej skład powinni wchodzić żołnierze i funkcjonariusze MON.

Do operacji odzyskiwania personelu izolowanego niezbędne są statki powietrzne pozwalające przerzucać siły i środki potrzebne podczas akcji poszukiwawczo-ratunkowych. Zapewnienie tego rodzaju sprzętu byłoby możliwe dzięki zakupowi statków powietrznych odpowiednio wyposażonych do przeprowadzania operacji odzyskiwania personelu w ramach planu modernizacji lotnictwa Sił Powietrznych, a następnie wydzielenie i podporządkowanie tych maszyn do wyłącznej dyspozycji dowódcy jednostki poszukiwawczo-ratowniczej.

Stan etatowy jednostki autor szacuje na minimum 125–135 osób (nie wliczając w to członków załóg latających oraz personelu naziemnego niezbędnego do obsługi statków latających)[32]. Obok znajduje się schemat proponowanej struktury organizacyjnej omawianej jednostki poszukiwawczo-ratowniczej.

[31] *Nigeryjscy islamiści z organizacji Boko Haram zagrozili, że zabiją francuską rodzinę* [online], http://www.swietapolska.com/news/swpolska4377.html [dostęp: 25 IX 2016].

[32] K. Falandys, *The development process*…, s. 6–10.



Schemat 1. Propozycja struktury organizacyjnej jednostki poszukiwawczo-ratowniczej.

Źródło: Opracowanie własne. K. Falandys, *The development process*…, s. 11.

Baza danych *ISOPREP*

Żeby siły prowadzące operację Personnel Recovery mogły skutecznie odzyskać izolowanych obywateli, muszą przede wszystkim wiedzieć, kogo mają szukać. Jest to o tyle istotne, że niektóre operacje odzyskiwania personelu izolowanego mogą trwać nawet kilka lat. Jako przykład można tutaj przytoczyć operację odzyskania izraelskiego żołnierza Gilada Szalita, uprowadzonego przez Hamas, którego izraelskie służby poszukiwały przez pięć lat. W tym czasie Szalit był niemal co noc przewożony przez członków organizacji w coraz to nowe miejsca. Takie działanie zmusiło izraelski rząd do negocjacji, łamiąc tym samym zasadę, że z terrorystami się nie negocjuje. Premier Binjamin Netanjahu zdawał sobie jednak sprawę z tego, jak negatywny wpływ na morale pozostałych żołnierzy ma pozostawienie tego jednego w rękach terrorystów, i dlatego zgodził się na wymianę. W jej wyniku za uwolnienie Gilada Szalita z izraelskich więzień wypuszczono 1027 palestyńskich więźniów. Ten przykład pokazuje, jak bardzo istotna dla izraelskich rządzących i opinii publicznej jest sprawa odzyskiwania personelu izolowanego[33].

[33] Zob. http://www.polskieradio.pl/9/863/Artykul/458645,Tysiac-wiezniow-za-izraelskiego-kaprala [dostęp: 23 IX 2016].

Wygląd osób przebywających w izolacji może się z upływem czasu zmienić, np. z powodu braku możliwości golenia, strzyżenia, umycia się itp. albo w wyniku świadomych zabiegów porywaczy dokonanych po to, aby utrudnić rozpoznanie poszukiwanych osób. Należy również brać pod uwagę to, iż osoba izolowana nie żyje, np. z powodu katastrofy komunikacyjnej bądź dlatego, że została zamordowana. W takiej sytuacji bardzo pomocne w ustaleniu tożsamości odzyskiwanej osoby (lub ciała) są jej dane zawarte w *ISOPREP*, m.in.: wzrost, waga, kolor oczu i włosów, znaki szczególne, zdjęcia, odciski palców, DNA, ustalone wcześniej „hasła rozpoznawcze".

Aby móc zbierać, przetwarzać i udostępniać takie informacje, musi powstać baza danych, która według autora powinna znaleźć się w strukturach jednostki poszukiwawczo-ratowniczej powołanej do odzyskiwania obywateli RP. Takie umiejscowienie bazy ma na celu maksymalne zmniejszenie obiegu danych.

Deklaracje *ISOPREP* powinny być wykonywane w postaci elektronicznej, w okresie przygotowania do wyjazdu za granicę (a nie w miejscu docelowym poza granicami kraju) przez osoby narażone na izolację, a następnie uaktualniane przy każdej zmianie danych – nie rzadziej niż co pięć lat. W przypadku wystąpieniu izolacji deklaracja *ISOPREP* danej osoby powinna być przekazana do komórek zajmujących się odzyskiwaniem obywateli. Samo przekazanie powinno się odbywać przez zabezpieczoną sieć teleinformatyczną lub przez wyznaczone osoby.

Oczywiście nie jest możliwe, aby każdy polski obywatel został ujęty w bazie *ISOPREP*. Z jednej strony jest to niewykonalne, a z drugiej – niepraktyczne. Dlatego też autor proponuje przyjęcie podziału osób zakwalifikowanych do wypełnienia deklaracji *ISOPREP* ze względu na zajmowane stanowisko służbowe oraz wykonywaną pracę.

Do bazy danych *ISOPREP* powinny być obowiązkowo zakwalifikowane osoby piastujące poniższe funkcje:

- prezydent RP,
- ministrowie w Kancelarii Prezydenta RP,
- szef Biura Bezpieczeństwa Narodowego,
- premier RP,
- ministrowie RP,
- posłowie i senatorowie RP,
- szef Sztabu WP,
- dowódcy Rodzajów Sił Zbrojnych WP,
- szefowie służb specjalnych,
- Prokurator Generalny,
- inne osoby, które nie piastują powyższych stanowisk, a zostały skierowane w rejony świata uznane za szczególnie niebezpieczne z ważnych powodów służbowych.

Wyżej wskazane osoby ze względu na zajmowane stanowisko znają informacje istotne dla bezpieczeństwa i obronności państwa. Z tego powodu przy okazji podróży zagranicznych mogą stać się celem niezgodnych z prawem działań różnego rodzaju grup ekstremistycznych i terrorystycznych albo może dojść do celowo spowodowanej lub przypadkowej awarii środka transportu, którym się poruszają[34].

Do bazy *ISOPREP* powinny być także obowiązkowo wprowadzone dane osób, takich jak:

[34] K. Falandys, *The development process*…, s. 16.

- personel (np. funkcjonariusze Biura Ochrony Rządu) towarzyszący w podróżach zagranicznych wyżej wymienionym osobom,
- żołnierze, funkcjonariusze i pracownicy cywilni wchodzący w skład Polskich Kontyngentów Wojskowych,
- piloci oraz personel pokładowy latający statkami powietrznymi zarejestrowanymi w RP,
- żołnierze, funkcjonariusze oraz personel zaokrętowany na pokładach statków (okrętów), którzy są obywatelami RP,
- pracownicy Ministerstwa Spraw Zagranicznych wykonujący obowiązki służbowe za granicą RP,
- funkcjonariusze i pracownicy służb specjalnych pełniący służbę za granicą,
- funkcjonariusze i pracownicy pozostałych służb mundurowych wykonujący obowiązki służbowe za granicą,
- fotoreporterzy i korespondenci wojenni przebywający w rejonach świata uznanych za szczególnie niebezpieczne,
- obywatele RP – pracownicy organizacji międzynarodowych (np. ONZ, OBWE, UE) – przebywający w rejonach świata uznanych za szczególnie niebezpieczne,
- obywatele RP – pracownicy organizacji humanitarnych (np. Lekarze bez Granic, Polska Akcja Humanitarna) – niosący pomoc w rejonach świata uznanych za szczególnie niebezpieczne,
- księża, zakonnicy i zakonnice – przebywający na misjach w rejonach świata uznanych za szczególnie niebezpieczne,
- pracownicy polskich firm (np. PGNiG, PKN ORLEN) prowadzący interesy i zatrudniający pracowników w państwach uznanych za szczególnie niebezpieczne,
- polscy podróżnicy, odkrywcy, udający się do najbardziej odległych i niebezpiecznych rejonów świata,
- inne osoby, których nie można zaliczyć do powyższych kategorii, a które z ważnych powodów służbowych lub prywatnych zostały skierowane w rejony świata uznane za szczególnie niebezpieczne.

Powyższy podział obejmuje osoby, które ze względu na swoją pracę, powołanie lub pasję przebywają w rejonach świata uznanych za szczególnie niebezpieczne. Dotyczy on również żołnierzy (funkcjonariuszy) służb mundurowych, którzy mają dostęp do informacji stanowiących tajemnicę ważną dla bezpieczeństwa i obronności Polski. Te osoby – z wyjątkiem żołnierzy i funkcjonariuszy – pozostając na terenach szczególnie niebezpiecznych, nie są uzbrojone i stają się łatwym celem dla terrorystów, ekstremistów i służb specjalnych państwa, na którego terytorium przebywają[35].

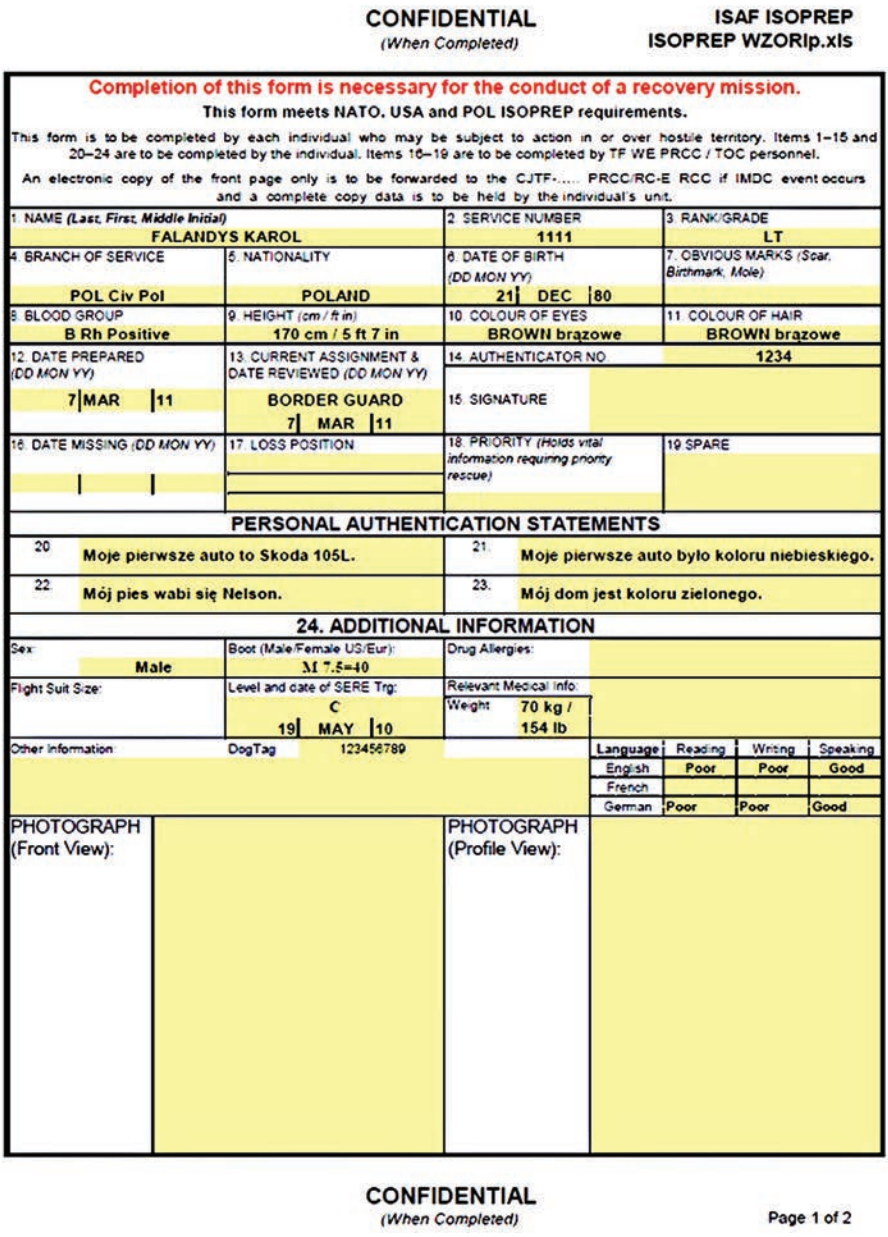
ISOPREP zawiera m.in. następujące dane:

1) imię i nazwisko osoby udającej się w niebezpieczny rejon,
2) numer ID,
3) stopień (jeśli posiada),
4) przynależność, np. do określonej struktury lub organizacji,
5) narodowość,
6) datę urodzenia,
7) znaki szczególne,
8) grupę krwi,

[35] Tamże, s. 16–17.

9) wzrost,
10) kolor oczu,
11) kolor włosów,
12) datę przygotowania *ISOPREP*-u,
13) stanowisko i datę zapisu,
14) numer identyfikacyjny (służący do identyfikowania się np. przez radio podczas przebywania w izolacji),
15) własnoręczny podpis,
16) datę zaginięcia (wypełnia komórka zajmująca się odzyskiwaniem),
17) ostatnie miejsce przebywania (pozycję) przed izolowaniem (wypełnia komórka zajmująca się odzyskiwaniem),
18) priorytet (wypełnia komórka zajmująca się odzyskiwaniem),
19) inne istotne informacje (wypełnia komórka zajmująca się odzyskiwaniem),
20) cztery zdania potwierdzające tożsamość,
21) płeć,
22) rozmiar obuwia,
23) uczulenia na leki,
24) rozmiar ubrania,
25) poziom oraz datę szkolenia SERE,
26) wagę,
27) istotne informacje medyczne,
28) inne ważne informacje,
29) numer nieśmiertelnika (jeśli posiada),
30) znajomość języków obcych (w mowie, piśmie i czytaniu),
31) dwie fotografie (z przodu i z profilu),
32) odciski palców (z obu rąk),
33) inne informacje, np. DNA.

Na stronie obok został umieszczony przykład wypełnionej pierwszej strony deklaracji *ISOPREP*. Na drugiej stronie umieszcza się odciski palców oraz jest tam miejsce na dodatkowe zdjęcia, np. znaków szczególnych itp. Inne dane, jak np. DNA, mogą być dodatkowo załączone.



CONFIDENTIAL
(When Completed)

ISAF ISOPREP
ISOPREP WZORIp.xls

Completion of this form is necessary for the conduct of a recovery mission.

This form meets NATO, USA and POL ISOPREP requirements.

This form is to be completed by each individual who may be subject to action in or over hostile territory. Items 1–15 and 20–24 are to be completed by the individual. Items 16–19 are to be completed by TF WE PRCC / TOC personnel.

An electronic copy of the front page only is to be forwarded to the CJTF-..... PRCC/RC-E RCC if IMDC event occurs and a complete copy data is to be held by the individual's unit.

1. NAME (Last, First, Middle Initial)		2. SERVICE NUMBER	3. RANK/GRADE
FALANDYS KAROL		1111	LT
4. BRANCH OF SERVICE	5. NATIONALITY	6. DATE OF BIRTH (DD MON YY)	7. OBVIOUS MARKS (Scar, Birthmark, Mole)
POL Civ Pol	POLAND	21 DEC 80	
8. BLOOD GROUP	9. HEIGHT (cm / ft in)	10. COLOUR OF EYES	11. COLOUR OF HAIR
B Rh Positive	170 cm / 5 ft 7 in	BROWN brązowe	BROWN brązowe
12. DATE PREPARED (DD MON YY)	13. CURRENT ASSIGNMENT & DATE REVIEWED (DD MON YY)	14. AUTHENTICATOR NO.	1234
7 MAR 11	BORDER GUARD 7 MAR 11	15. SIGNATURE	
16. DATE MISSING (DD MON YY)	17. LOSS POSITION	18. PRIORITY (Holds vital information requiring priority rescue)	19. SPARE

PERSONAL AUTHENTICATION STATEMENTS

20.	Moje pierwsze auto to Skoda 105L.	21.	Moje pierwsze auto było koloru niebieskiego.
22.	Mój pies wabi się Nelson.	23.	Mój dom jest koloru zielonego.

24. ADDITIONAL INFORMATION

Sex:	Boot (Male/Female US/Eur):	Drug Allergies:	
Male	M 7.5=40		
Flight Suit Size:	Level and date of SERE Trg:	Relevant Medical Info:	
	C 19 MAY 10	Weight: 70 kg / 154 lb	
Other Information:	DogTag 123456789		

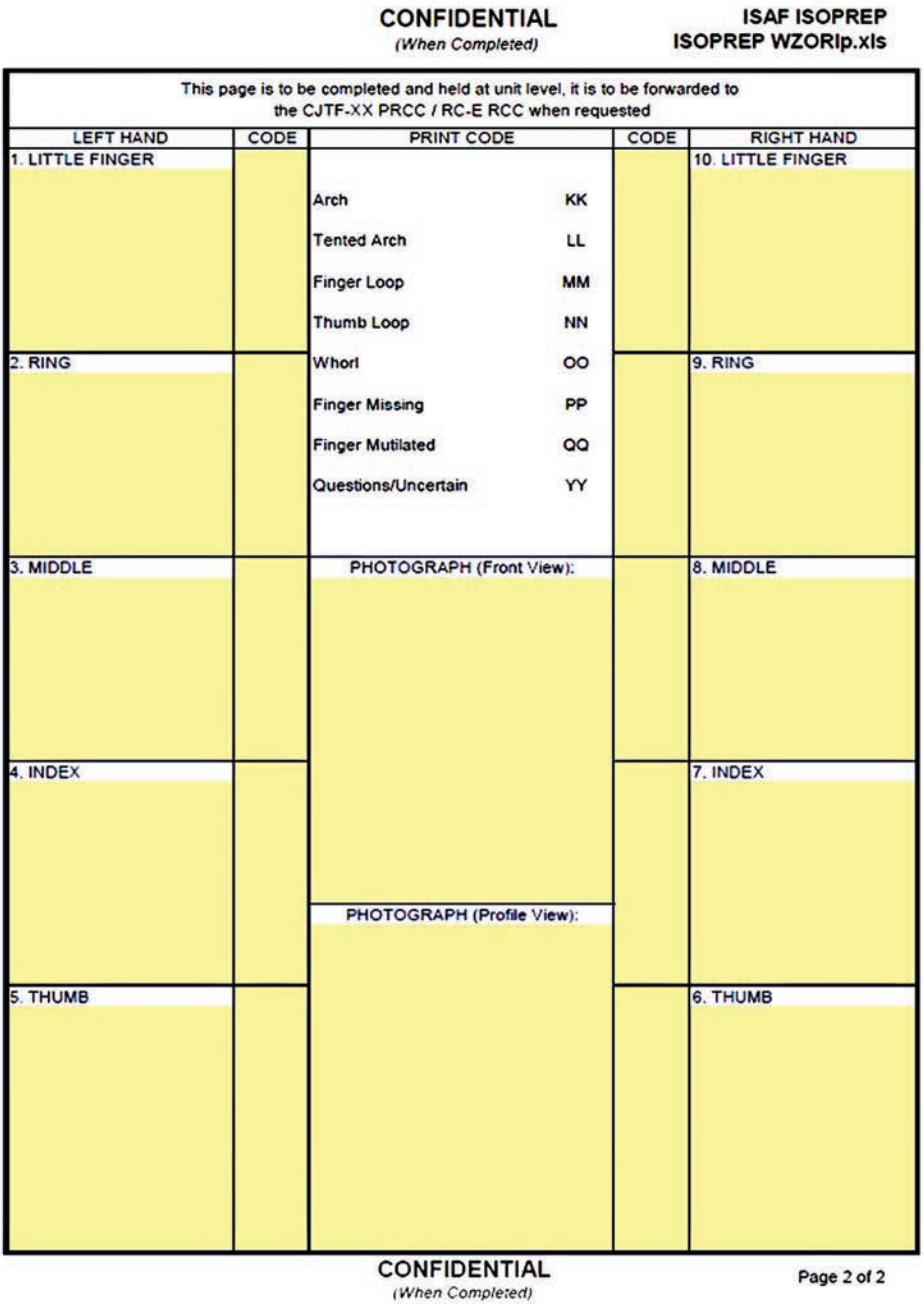
Language	Reading	Writing	Speaking
English	Poor	Poor	Good
French			
German	Poor	Poor	Good

PHOTOGRAPH (Front View):		PHOTOGRAPH (Profile View):	

CONFIDENTIAL
(When Completed)

Page 1 of 2

Rys. 1. Przykład wypełnionej deklaracji *ISOPREP* – strona 1.



CONFIDENTIAL
(When Completed)

ISAF ISOPREP
ISOPREP WZORIp.xls

This page is to be completed and held at unit level, it is to be forwarded to the CJTF-XX PRCC / RC-E RCC when requested

LEFT HAND	CODE	PRINT CODE		CODE	RIGHT HAND
1. LITTLE FINGER		Arch	KK		10. LITTLE FINGER
		Tented Arch	LL		
		Finger Loop	MM		
		Thumb Loop	NN		
2. RING		Whorl	OO		9. RING
		Finger Missing	PP		
		Finger Mutilated	QQ		
		Questions/Uncertain	YY		
3. MIDDLE		PHOTOGRAPH (Front View):			8. MIDDLE
4. INDEX					7. INDEX
		PHOTOGRAPH (Profile View):			
5. THUMB					6. THUMB

CONFIDENTIAL
(When Completed)

Page 2 of 2

Rys. 2. Przykład wypełnionej deklaracji *ISOPREP* – strona 2.

Źródło: Zbiory własne. Autor otrzymał materiały szkoleniowe w postaci m.in. powyższego dokumentu podczas kursu instruktorskiego SERE.

Wnioski

W podsumowaniu powyższych rozważań należy wskazać, że obecność Polaków w Afganistanie, Iraku, państwach Afryki Północnej i w państwach upadłych[36], może skłonić różnego rodzaju ugrupowania terrorystyczne do porwań obywateli RP. Polacy mogą też stać się np. ofiarami katastrof komunikacyjnych lub wojen plemiennych. Dlatego też państwo polskie powinno zapewnić swoim obywatelom poczucie bezpieczeństwa, które z pewnością zostanie wzmocnione z chwilą utworzenia narodowego systemu odzyskiwania obywateli RP.

Według autora publikacji Polska jako jeden z większych krajów członkowskich NATO i UE jest w stanie udźwignąć koszty utworzenia i funkcjonowania Narodowego Systemu Odzyskiwania Obywateli RP. Mógłby on uzyskać pełną gotowość operacyjną już w okresie dwóch–trzech lat od chwili utworzenia.

Taki system pozwoli państwu polskiemu po pierwsze na natychmiastową reakcję w przypadku izolacji polskiego obywatela, po drugie – umożliwi skuteczne użycie własnej jednostki poszukiwawczo-ratowniczej pod jednolitym polskim dowództwem w dowolnym rejonie świata. Tego typu jednostka mogłaby być także wykorzystana na terenie naszego kraju w akcjach ratowniczych po wystąpieniu klęsk żywiołowych oraz do udzielania pomocy obywatelem państw członkowskich NATO i UE, jeżeli te państwa zwróciłyby się do Polski z prośbą o taką pomoc, w przypadku gdyby same nie były w stanie jej udzielić swoim obywatelom.

Bibliografia:

1. Dudkiewicz H., *Prawa międzynarodowe w kwestii państwa upadłego,* w: *Problem upadku państw w stosunkach międzynarodowych*, R. Kłosowicz (red.), Kraków 2012, Wydawnictwo Uniwersytetu Jagiellońskiego.
2. Falandys K., *The development process of the national polish citizens recovery system*, „Zeszyty Naukowe WSOWL" 2015, t. 47, nr 3.
3. Falandys K., *Uwarunkowania prawne determinujące kształt Narodowego Systemu Odzyskiwania Obywateli Rzeczypospolitej Polskiej,* „Rocznik Bezpieczeństwa Wewnętrznego" 2015, t. 9, nr 2.
4. Falandys K., *Zjawisko izolacji (bezprawnego przetrzymywania) – jego skala i regionalizacja*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13.
5. *Koncepcja i ogólne zasady funkcjonowania Narodowego Systemu Odzyskiwania Personelu Wojskowego*, Warszawa 2008, Ministerstwo Obrony Narodowej, Sztab Generalny WP.
6. *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r.* (Dz.U. Nr 78 poz. 483, ze zm.).
7. Kubiak K., *Przemoc na oceanach. Współczesne piractwo i terroryzm morski,* Warszawa 2009, Trio.
8. *NATO Joint Doctrine for Personnel Recovery*, AJP-3.3.9 (SD-8), MCASB, 2007.
9. *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 26 marca 2012 r. w sprawie ogłoszenia jednolitego tekstu ustawy o Radzie Ministrów* (Dz.U. z 2012 r. poz. 392).

[36] Państwo upadłe to według Huberta Dudkiewicza państwo, które w wyniku wewnętrznych konfliktów zupełnie i trwale utraciło władzę centralną. Zob. H. Dudkiewicz, *Prawa międzynarodowe w kwestii państwa upadłego*, w: *Problem upadku państw w stosunkach międzynarodowych*, R. Kłosowicz (red.), Kraków 2012, s. 67–86.

10. *Odzyskiwanie izolowanego personelu (DD/3.3.9)*, Warszawa 2010, Ministerstwo Obrony Narodowej, Sztab Generalny WP.
11. *Personnel Recovery,* Kalkar 2011, JAPCC.
12. *Połączona doktryna sojusznicza prowadzenie operacji ewakuacji personelu niewojskowego NATO*, AJP – 3.4.2, 2007.
13. *Rozporządzenie Prezesa Rady Ministrów z dnia 17 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra Spraw Zagranicznych* (Dz.U. z 2015 r. poz. 1899, ze zm.).
14. *Ustawa z dnia 4 września 1997 r. o działach administracji rządowej* (tekst jednolity: Dz.U. z 2016 r. poz. 543).

Źródła internetowe:

1. http://www.dodea.edu/
2. http://www.dziennikpolski24.pl/
3. http://www.polskieradio.pl/
4. http://www.sar.gov.pl/
5. http://www.swietapolska.com/

Abstrakt

W zaprezentowanym artykule zwrócono uwagę na konieczność utworzenia Narodowego Systemu Odzyskiwania Obywateli Rzeczypospolitej Polskiej oraz na problemy natury prawej, systemowej i logistycznej, które trzeba pokonać, aby taki system powstał. W tym celu zasugerowano utworzenie jednostki poszukiwawczo-ratowniczej przeznaczonej specjalnie do planowania i przeprowadzania operacji odzyskiwania obywateli naszego kraju oraz umiejscowienie jej w odpowiednich strukturach administracji państwowej. Zaakcentowano również potrzebę utworzenia bazy danych *ISOPREP*. Jednocześnie autor zaproponował definicję narodowego systemu odzyskiwania obywateli RP.

Słowa kluczowe: odzyskiwanie personelu, personel izolowany, jednostka poszukiwawczo-ratownicza, operacje poszukiwawczo-ratownicze, *ISOPREP*.

Abstract

In the article the author highlighted the need to establish a National Recovery System for the Citizens of the Republic of Poland together with appropriate law, system or logistics that must be overcome in order to achieve the goal. In the same order he suggested the creation of a special search and rescue unit, its location in the appropriate structures of state administration and the creation of a database called ISOPREP. At the same time the author proposed a definition of the national recovery system for Polish citizens.

Keywords: personnel recovery, isolated personnel, search and rescue unit, operations search and rescue, ISOPREP.

II
STUDIA I ANALIZY

Krzysztof Domeracki

Hezbollah oraz jego Aparat Militarny i Bezpieczeństwa

Na początku lat 80. ubiegłego wieku pojawił się na Bliskim Wschodzie nowy aktor niepaństwowy, który dwie dekady później stał się jednym z podmiotów oddziałujących na bezpieczeństwo międzynarodowe. Organizacja Hizb Allah (Hezbollah, Partia Boga) powstała w 1982 r. w wyniku przemian zachodzących w regionie[1], stając się siłą do dzisiaj dysponującą środkami i narzędziami pozwalającymi na kształtowanie sytuacji bezpieczeństwa, przede wszystkim w Libanie. Jak pokazały dotychczasowe doświadczenia, jest ona również podmiotem, który w dużym stopniu wpływa na bezpieczeństwo Bliskiego Wschodu.

W związku ze swoją aktywnością i udanymi operacjami skierowanymi głównie na cele izraelskie i amerykańskie nowo powstała organizacja posiadająca własne siły zbrojne stała się celem operacji wywiadowczych prowadzonych przede wszystkim przez Izrael i Stany Zjednoczone[2]. Zdając sobie z tego sprawę, Hezbollah i irańscy mocodawcy zaczęli rozwijać zdolności wywiadowcze i kontrwywiadowcze organizacji. Doświadczenia palestyńskie (szczególnie Fatahu) oraz wsparcie zewnętrzne (otrzymane przede wszystkim od irańskiego Pasdaranu) pozwoliło na stworzenie Aparatu Militarnego i Bezpieczeństwa, który funkcjonuje w strukturach Partii Boga i jest jedną z najlepiej strzeżonych tajemnic organizacji.

Autor w niniejszym opracowaniu przedstawił odpowiedzi na pytania:

1. Jak jest zorganizowana Partia Boga i jakie miejsce w jej strukturze zajmuje Aparat Militarny i Bezpieczeństwa?
2. Jak jest zorganizowany Aparat Militarny i Bezpieczeństwa organizacji Hezbollah, jakie są jego zadania oraz jaki wpływ może on wywierać na kształt organizacji?

Artykuł został podzielony na osiem części. W pierwszej autor krótko charakteryzuje organizację wraz z określeniem czynników determinujących jej powstanie. W kolejnych porusza zagadnienia związane ze strukturą oraz źródłami finansowania Partii Boga. W czwartej autor zawarł analizę funkcjonalną Aparatu Militarnego i Bezpieczeństwa wraz z określeniem ogólnych celów i zadań realizowanych przez poszczególne podmioty. Części piąta i szósta traktują odpowiednio o wywiadzie i kontrwywiadzie organizacji. Natomiast siódma dotyczy części militarnej Aparatu organizacji. Ostatnia zaś jest związana z określeniem wpływu Aparatu Militarnego i Bezpieczeństwa na kierunki działania Hezbollahu i jego przyszły kształt.

Praca, z uwagi na przedmiot i podmiot badań oraz związane z tym istotne ograniczenia dotyczące dostępu do informacji źródłowych, została oparta na opracowaniach naukowych, informacjach przekazywanych przez środki masowego przekazu, analizach i raportach.

[1] W dalszej części pracy określono czynniki wewnętrzne i zewnętrzne warunkujące powstanie organizacji.

[2] Izraelskie służby do czasu pojawienia się nowego ugrupowania były skupione przede wszystkim na rozpoznaniu zagrożeń związanych z terroryzmem palestyńskim.

Na potrzeby niniejszego artykułu posłużono się głównie metodami teoretycznymi[3]. Zastosowano przede wszystkim metody analizy oraz syntezy, a także wnioskowanie indukcyjnego enumeracyjnego i dedukcyjnego. Autor wykorzystał także elementy metody zbierania sądów (opinii)[4], w ramach których stosował technikę wywiadu eksperckiego.

Hezbollah – jeden z aktorów na Bliskim Wschodzie

Partia Boga, której członkowie są połączeni więzami rodzinnymi i religijnymi, jest jedną z najbardziej tajnych i zakonspirowanych organizacji na świecie. To nie tylko zwyczajna organizacja o charakterze paramilitarnym, lecz także – w opinii ekspertów ją badających – szeroko rozumiany ruch oporu (ang. *resistance movement*). W politycznym środowisku libańskim Partia Boga jest uważana za superpartię polityczną, z własnym zapleczem militarnym, której słabe libańskie struktury państwowe nie są w stanie się przeciwstawić.

Funkcjonowanie Hezbollahu jest oparte na trzech filarach[5]. Są to: ***wiara w Boga zgodnie z islamem***, ***dżihad*** oraz ***al-wali al-faqih***[6]. Organizacja działa w sferach[7]: politycznej (jako część Sojuszu 8 Marca), dżihadu[8], specjalnej – wywiadu i kontrwywiadu (także na rzecz innych podmiotów), społecznej (opieka zdrowotna, kultura) oraz ekonomicznej (zdobywanie środków na finansowanie działalności oraz wspieranie społeczności szyickiej).

Organizacja jako partia polityczna oraz lider koalicji 8 Marca jest podmiotem mającym możliwości wpływania na politykę wewnętrzną i zewnętrzną Libanu. Stąd też w materiałach dotyczących bezpieczeństwa w regionie konieczne wydaje się uwzględnianie tej organizacji jako jednego z podmiotów, który posiada możliwość oddziaływania na rozwój sytuacji na Bliskim Wschodzie, szczególnie w obszarze Lewantu.

Hezbollah powstał w wyniku wewnętrznych procesów zachodzących w Libanie. Katalizatorem była izraelska inwazja na Liban w 1978 r. i następnie w 1982 r. Był to czas, kiedy libańskie społeczeństwo było mocno podzielone. W sytuację w Libanie były zaangażowane szczególnie dwa państwa – Syria i Iran. Syria, chcąc osłabiać wpływy Iranu i zahamować eksport irańskiej rewolucji, wspierała konkurencyjną dla Hezbollahu partię Amal, z której wywodziło się wielu członków Partii Boga[9]. Obie organizacje, które są organizacjami szyickimi, walczyły o wpływy w szyickiej części libańskiego społeczeństwa. *Etap kończący otwartą walkę pomiędzy Amalem i Hezbollahem zakończył się w listopadzie 1990 r., kiedy osiągnięto porozumienie kończące działania wojenne pomiędzy obiema stronami. Syryjska interwencja była kluczowym bodźcem doprowadzającym te dwie partie do przerwania działań militarnych. Syryjski nacisk doprowadził również do współpracy pomiędzy Hezbollahem i Amalem i uformowaniem politycznego*

[3] M. Pelc, *Elementy metodologii badań naukowych*, Warszawa 2012, s. 67–78.

[4] Tamże, s. 59.

[5] Zob. N. Qassem, *Hizbullah. The story from within*, London 2005, s. 21–58.

[6] *Al-wali al-faqih* – duchowny uczony sprawujący przywództwo. Zob. *Słownik polityczny angielsko-perski, persko-angielski*, wyd. 2, Teheran 1996, s. 412 (w tekście odniesienie do najwyższego religijnego przywódcy Iranu).

[7] Podział dokonany przez autora na potrzeby niniejszego opracowania.

[8] W tym dżihad militarny, który został podzielony przez Naima Qassema na: *groundwork jihad* (czyli konfrontacja Muzułmanów z innymi. „święta wojna") i *defensive jihad* (obrona terytorium). Źródło: N. Qassem, *Hizbullah*…, s. 39.

[9] M.in.: Hussain Mussawi, Hassan Nasrallah, Naim Qassem. Do Hezbollahu trafiali również członkowie innych ugrupowań, m.in. z Hizb al-Dawa: Subhi al-Tufayli, Sayyid Abbas al-Mousawi czy też z Harakat Fatah Imad Mugniyah.

sojuszu – który przetrwał do dzisiaj[10]. Była to demonstracja siły Syrii w stosunku do Iranu potwierdzająca, że Liban jest nieodłączną częścią syryjskiej strefy wpływów. Amal zaś został politycznym współpracownikiem dobrze zorganizowanej i lepiej uzbrojonej organizacji Hezbollah[11].

Hezbollah to również „efekt ratyfikacji Manifestu Dziewięciu" przez różne organizacje i prowadzenie przez nie działalności pod jednym szyldem[12], a także wola i zaangażowanie Iranu, gdyż do Doliny Bekaa[13] popłynęły środki finansowe, uzbrojenie oraz irańscy instruktorzy (pochodzący z Korpusu Strażników Rewolucji Islamskiej, ang. *Islamic Revolutionary Guard Corps* – IRGC[14]). Korpus to produkt rewolucji islamskiej z 1979 r. Jednym z podmiotów wchodzących w jego skład są siły specjalne Al-Quds, które współpracują między innymi z Hezbollahem oraz innymi organizacjami szyickimi[15].

Za Rafałem Ożarowskim **czynniki determinujące powstanie organizacji** można podzielić następująco[16]:

1) czynniki wewnętrzne:
   a) aktywność bojowników palestyńskich i obecność OWP w Libanie przyczyniła się do wybuchu wojny domowej,
   b) rewitalizacja szyickiej społeczności w Libanie;
2) czynniki zewnętrzne:
   a) rewolucja islamska w Iranie z 1979 r.,
   b) inwazja Izraela na Liban w 1982 r.

Dodatkowo w ujęciu geostrategicznym i geopolitycznym było to stworzenie irańskiego ośrodka wpływu na sytuację bezpieczeństwa w regionie.

Partia Boga ukonstytuowała się na wzór „irańskiego mentora" oraz częściowo skorzystała z doświadczeń wyniesionych z funkcjonowania organizacji palestyńskich[17]. Uzbrojenie dla organizacji dostarcza Syria, która jest swoistego rodzaju łącznikiem pomiędzy Hezbollahem a Iranem[18]. Jednym z głównych celów utrzymywania tej organizacji w Libanie przez Iran i Syrię jest możliwość wywierania wpływu na sytuację w regionie oraz zachowanie stanu pozornego wrzenia w Libanie, co angażuje uwagę Izraela będącego wrogiem numer jeden dla muzułmańskiego świata.

Hezbollah oficjalnie określił swoją tożsamość jako militarne skrzydło Brygad Islamskiego Oporu[19] *w styczniu 1985 r., kiedy w gazecie As-Safir opublikował „List otwarty: program Hezbollahu"*[20]. Dzięki przemyślanej strategii oraz pomocy irańsko-syryjskiej organizacja stała się uosobieniem walki z okupantem oraz jedynym podmiotem niosącym pomoc biedniejszej, szyickiej części społeczeństwa libańskiego. Hezbollah jest dobrze zorganizowaną strukturą i jednocześnie swego rodzaju „państwem w pań-

[10] N. Qassem, *Hizbullah*…, s. 14.

[11] Hezbollah przewodzi parlamentarnej opozycji 8 Marca.

[12] N. Qassem, *Hizbullah*…, s. 20.

[13] Dolinę Bekaa zamieszkują przede wszystkim szyici, dlatego też w tym miejscu Hezbollah rozpoczął działalność.

[14] Nazwa nieformalna – Pasdaran.

[15] Zob. A.H. Cordesman, *Iran's Revolutionary Guards, the Al Quds Force, and Other Intelligence and Paramilitary Forces*, Washington 2007.

[16] R. Ożarowski, *Hezbollah w stosunkach międzynarodowych na Bliskim Wschodzie*, Gdańsk 2011, s. 28.

[17] Członkami Hezbollahu zostały również osoby mające doświadczenia zdobyte w palestyńskim Fatahu, w osławionej Force17 oraz libańskim Amalu.

[18] Zob. M. Bar-Zohar, N. Mishal, *Mossad,* Poznań 2012, s. 298.

[19] Ang. Islamic Resistance Brigades – arab. Muqawama al-Islamiyyah.

[20] J.L. Gleis, B. Berti, *Hezbollah and Hamas. A Comparative Study*, Baltimore 2012, s. 35.

stwie", gdyż (…) *dysponuje możliwościami politycznymi, gospodarczymi, militarnymi i informacyjnymi*[21]. Mając własne media, systemy łączności oraz rozbudowane struktury edukacyjno-kulturalne, pomocy społecznej i opieki medycznej, finansowe, polityczno-militarne, a także ds. zagranicznych, religijnych oraz aparat bezpieczeństwa, organizacja jest podmiotem, który nie może być pominięty przy podejmowaniu studiów nad bezpieczeństwem na Bliskim Wschodzie.

Przez wiele lat największe służby wywiadowcze świata nie były w stanie spenetrować tej organizacji. Jest ona świetnie zakonspirowana, niektórzy mogą mówić, że pod tym względem wykazuje skłonności paranoidalne. Nawet izraelski wywiad wojskowy twierdzi, że Hezbollah (…) *to organizacja terrorystyczna, której nie można skompromitować przy użyciu techniki. Supertajne komórki i szyfrowe sposoby komunikowania się mogłyby wzbudzić zazdrość najbardziej wyrafinowanych służb wywiadowczych. Organizacje terrorystyczne i szyickie układy terrorystyczne bazują na powiązaniach rodzinnych i religijnych. Pełnym członkiem takiej organizacji ktoś staje się z urodzenia i nawet najbardziej wyrafinowane służby wywiadowcze nie są w stanie sfałszować tej rzeczywistości*[22]. Ale służby zachodnie, szczególnie izraelskie, mają także swoje sukcesy w walce z tym głęboko zakonspirowanym wrogiem.

Można zatem stwierdzić, że powstanie Hezbollahu miało nie tylko doprowadzić do utworzenia sił, które mogły prowadzić operacje (akcje) o charakterze zbrojnym, lecz także – jak pokazała historia – stworzyć ruch zdolny zespolić część społeczeństwa libańskiego oraz utworzyć struktury niepaństwowe mogące oddziaływać na bezpieczeństwo wewnętrzne i zewnętrzne państwa, a także mające wpływ na bezpieczeństwo międzynarodowe. W ocenie Ahmada Nizara Hamzeha[23] (…) *z wielu grup islamskich, które powstały i zaczęły funkcjonować w świecie islamu od połowy lat 80 XX wieku, prawdopodobnie żadna nie miała tak dużego wpływu na Bliski Wchód i stosunki międzynarodowe jak Hezbollah – Partia Boga*. Przekształcenie Hezbollahu i rozszerzenie jego profilu działalności o zaangażowanie się na libańskiej scenie politycznej doprowadziły do zmiany zaklasyfikowania organizacji. Obecnie można ją zdefiniować jako „podmiot subpaństwowy"[24] i „transnarodowy"[25], który funkcjonuje w Libanie oraz poza jego granicami. Obecnie w skład rządu libańskiego wchodzi dwóch ministrów wywodzących się z Partii Boga[26].

Struktura Hezbollahu

Struktura organizacji jest swego rodzaju odwzorowaniem struktur Pasdaranu. Stanowi również mieszankę doświadczeń palestyńskich i tych wyniesionych z funkcjonowania partii Amal. Można ją określić jako hierarchiczny układ mgławicowy uwzględniający podział terytorialny Libanu. Na zamieszkałych przez szyitów terenach Libanu, tj.: w Dolinie Bekaa, Bejrucie oraz Południowym Libanie, Partia Boga zorganizowała swoje struktury.

[21] R. Ożarowski, *Hezbollah*…, s. 28.

[22] S.L. Katz, *Aman. Wywiad wojskowy Izraela*, Warszawa 1999, s. 334.

[23] Profesor Uniwersytetu Amerykańskiego w Bejrucie, badacz organizacji Hezbollah.

[24] Zob. R. Ożarowski, *Hezbollah*…, s. 25.

[25] Zob. M. Pietraś, K. Piórko, *Podmioty transnarodowe*, w: *Międzynarodowe stosunki polityczne*, M. Pietraś (red.), Lublin 2006, s. 140.

[26] Hussein Hajj Hassan – minister przemysłu oraz Muhammad Fneish – minister ds. młodzieży i sportu (zmiana po wyborze prezydenta w końcu 2016 r.).

Hezbollah nie jest zwykłą partią polityczną, dlatego też struktura organizacji nie odzwierciedla struktury typowych partii politycznych. Powstała on jako organizacja paramilitarna, która realizowała zadania zlecane przez swoich mocodawców. Działalność polityczną rozpoczęto ponad dekadę później. W ocenie A.N. Hamzeha (…) *w organizacji nie ma rozdzielenia funkcji wykonawczych i legislacyjnych*[27].

Struktura organizacyjna Hezbollahu[28] jest bardzo złożona i ulega ciągłym zmianom, które są determinowane zarówno przez czynniki wewnętrzne, jak i zewnętrzne, dlatego też trudne jest precyzyjne jej określenie. Koordynacja wszystkich procesów i zadań realizowanych przez poszczególne komórki organizacji jest dużym wyzwaniem dla kierownictwa Partii Boga, z tego względu istniejący system, bazujący na koncepcji *al-wali al-faqih*, jest jednym z elementów, który pozwala na utrzymanie reżimu decyzyjnego w organizacji. Dotyczy to również jej członków, którzy zostali wybrani do parlamentu oraz którzy zajmują stanowiska ministerialne. Wszystkie decyzje, które są przez nich podejmowane, muszą być zgodne z wolą i stanowiskiem Partii Boga (tj. Rady Szura). Z punktu widzenia funkcjonowania państwa libańskiego istnienie tego ugrupowania jest niekorzystnym zjawiskiem i świadczy o słabości struktur państwowych.

Źródła finansowania organizacji[29]

Niezbędne dla funkcjonowania organizacji jest zdobywanie środków finansowych na jej działalność. W przypadku Hezbollahu nie do końca są znane i potwierdzone wszystkie źródła finansowania jego działalności, dlatego też przedstawiony katalog jest otwarty i nie wyklucza się jego rozszerzenia.

Organizacja jest finansowana przede wszystkim przez Iran. Fundusze operacyjne są przekazywane przez Korpus Strażników Rewolucji Islamskiej oraz irański wywiad (Ministry of Intelligence and Security, MOIS[30]). Środki finansowe pochodzą również z sieci supermarketów, stacji paliw, sklepów i restauracji, a także firm budowlanych i agencji turystycznych, które są prowadzone przez Partię Boga. Część pieniędzy ugrupowanie inwestuje w różnego rodzaju przedsięwzięcia biznesowe. Dochód przynosi także działalność bankowa, w tym handel walutami. Ważną częścią przychodów są darowizny przekazywane przez osoby indywidualne, grupy społeczne, przedsiębiorstwa, banki oraz innych partnerów z Ameryki Północnej, Łacińskiej, Europy i Australii. Kolejnym źródłem są środki pochodzące ze zbiórek prowadzonych przez organizacje charytatywne, a także z podatków. Duża część dochodów Hezbollahu pochodzi z działalności przestępczej[31], m.in.: z obrotu narkotykami, diamentami[32], samochodami[33], handlu bronią.

---

[27] A.N. Hamzeh, *In the Path of Hizbullah*, New York 2004, s. 49.

[28] Szczegółowe zadania realizowane przez poszczególne komórki organizacji zostały opisane np. w publikacjach A.N. Hamzeha, M. Levitta, B. Bertiego, R. Ożarowskiego, C.A. Wege'a, a także F. Burtona, S. Stewarta, D. Leroya, M. Ranstorpa.

[29] Na podstawie A.N. Hamzeh, *In the Path*…, s. 62–65; zob. także: M. Levitt, *The global footprint of Lebanon's Party of God*, London 2013, rozdział IX.

[30] VAJA.

[31] Zob. C.B. Realuyo, *The Terror-Crime Nexus. Hezbollah's Global Facilitators*, PRISM 2014, t. 5, nr 1, s. 117–13; także: http://cco.ndu.edu/Portals/96/Documents/prism/prism_5-1/The_Terror_Crime_Nexus.pdf [dostęp: 18 I 2017].

[32] Zob. http://www.terroryzm.com/hezbollah-w-czarnej-afryce/ [dostęp: 8 XI 2015].

[33] Zob. http://www.treasury.gov/press-center/press-releases/Pages/jl1908.aspx [dostęp: 8 XI 2015].

Pieniądze są przechowywane w irańskich bankach (np. Saderat Bank w Teheranie), (…) *które w zależności od potrzeb transferowane są na konta w Libanie*[34]. Pomoc finansowa oficjalnie przekazywana Partii Boga przez irańskie instytucje jest szacowana na kwotę (…) *od min. 200 mln USD rocznie do powyżej 1 mld USD rocznie – nie wliczając przekazywanej pomocy wojskowej (uzbrojenie itp.)*[35].

Zbieranie środków finansowych przez Hezbollah ma charakter globalny dzięki temu, że komórki organizacji oraz podmioty od niej zależne funkcjonują w wielu krajach, zwłaszcza w miejscach, w których znajdują się diaspory libańskich szyitów. Operacje przeprowadzone przez to ugrupowanie w Afryce, mające na celu uzyskanie funduszy, bardzo dokładnie odtworzył Matthew Levitt w książce pt. *Hezbollah. The Global Footprint of Lebanon's Party of God*. Książka powstała na podstawie dokumentów źródłowych Centralnej Agencji Wywiadowczej i innych organów administracji USA.

Ugrupowanie – w związku z wprowadzeniem przez niektóre kraje sankcji wynikających z wpisania Hezbollahu na listy organizacji terrorystycznych – stworzyło system prania pieniędzy zdobytych z działalności przestępczej. Agendy rządowe USA[36] wykryły mechanizm, który miał na celu legalizację środków finansowych pochodzących z przemytu i obrotu narkotykami. Były one wykorzystywane w handlu używanymi samochodami kupowanymi w Stanach Zjednoczonych.

Proceder przemytu narkotyków został opisany m.in. w artykule pt. *Kartel Allaha*[37]. Na podstawie informacji zawartych w tej publikacji można wywnioskować, że to przedsięwzięcie odbywało się (i z dużym prawdopodobieństwem można stwierdzić, że odbywa się nadal) za wiedzą i wsparciem irańskich i syryjskich służb, a także prawdopodobnie przy aprobacie jordańskich służb[38] oraz innych organizacji niepaństwowych[39]. Główną rolę w działalności Hezbollahu odgrywali członkowie Aparatu Militarnego i Bezpieczeństwa, bez których wiedzy i zgody narkotyki nie mogłyby zostać przerzucone do Europy. Jednostki specjalne tego ugrupowania zajmowały się również ochroną takich ładunków. W 2016 r. Liga Państw Arabskich oraz Rada Państw Zatoki Perskiej uznały Partię Boga za organizację terrorystyczną, co prawdopodobnie utrudni jej działalność oraz ograniczy zdobywanie środków finansowych w regionie Bliskiego Wschodu (poza Libanem i Iranem).

Środki finansowe Hezbollahu pochodzą z różnych źródeł i z różnych stron świata. Taka dywersyfikacja powoduje, że w przyszłości ugrupowanie mogłoby się w pełni uniezależnić od finansowego wsparcia Iranu i stać się samodzielnym bytem. Jednak to nie finanse stanowią o możliwości zdobycia samodzielności strategicznej tej organizacji. Bez wsparcia Iranu nie jest możliwe funkcjonowanie Partii Boga w takim kształcie, jak obecnie. Z uwagi na to, że finansowanie organizacji nie jest problemem badawczym niniejszej pracy, podano w tym miejscu wyłącznie ogólne informacje, które pozwalają na przeanalizowanie działalności Aparatu Militarnego i Bezpieczeństwa oraz jego wpływu na kształt całej organizacji.

[34] A. N. Hamzeh, *In the Path*…, s. 62–65.

[35] J.L. Gleis, B. Berti, *Hezbollah and Hamas*…, s. 69.

[36] Więcej na www.treasury.gov.

[37] Patrz: https://www.wprost.pl/345568/Kartel-Allaha.

[38] Przez terytorium Jordanii prowadził szlak przerzutowy.

[39] Szerzej o współpracy w dalszej części artykułu dotyczącej funkcjonowania komórek operacyjnych i wywiadowczych poza granicami Libanu.

Aparat Militarny i Bezpieczeństwa

Partia Boga od początku istnienia prowadziła działalność militarną i nadal stanowi najważniejszy element funkcjonowania tej organizacji. Jak pokazał konflikt w Syrii, aktywność militarna Hezbollahu jest narzędziem irańskiej polityki bezpieczeństwa.

Aparat Militarny i Bezpieczeństwa stanowi trzon organizacji oraz wpływa na kształt i funkcjonowanie pozostałych jej komponentów, gdyż jego działalność jest istotna przede wszystkim dla realizacji irańskich interesów w regionie Bliskiego Wschodu. Jest też ogniwem spajającym szeroko rozumiany szyicki ruch oporu na Bliskim Wschodzie. Z uwagi na zmieniające się uwarunkowania bezpieczeństwa organizacja z biegiem czasu zaczęła rozwijać nowe zdolności. W jej strukturach powstały m.in. jednostki operatorów bezzałogowych aparatów latających oraz jednostki zajmujące się cyberbezpieczeństwem. W momencie konstytuowania się organizacji głównym celem działania Aparatu było zapewnienie bezpieczeństwa wewnętrznego organizacji, który został zbudowany (…) *na klanach Hamadi i Musawi*[40] i następnie rozwijany w wysoko zaawansowaną strukturę.

System bezpieczeństwa Hezbollahu można scharakteryzować następująco[41]:

1) decydent – Rada Szura z Sekretarzem Generalnym Organizacji i jego zastępcą kierującym pracami Aparatu Militarnego i Bezpieczeństwa[42], z zastrzeżeniem roli *al-wali al-faqih*,
2) organ doradczy – IRGC oraz irański wywiad,
3) organ sztabowy – Rada ds. Dżihadu[43],
4) podsystemy wykonawcze (operacyjne):
   a) obronne – Islamski Ruch Oporu oraz Specjalny Aparat Bezpieczeństwa:
      – ogniwa „obrony terytorialnej" – współpraca z organizacjami palestyńskimi, chrześcijańskimi i sunnickimi, w tym w ramach Libańskich Brygad Oporu,
      – ogniwa operacji zagranicznych,
      – ogniwa operacji na kierunkach strategicznych (Izrael, Syria, Irak, Strefa Gazy),
      – elementy operacyjnego przygotowania terytorium;
   b) ochronne – Organ Bezpieczeństwa oraz biuro ds. koordynacji:
      – ochrona zajmowanego terytorium i zapewnienie bezpieczeństwa oraz porządku publicznego,
      – ochrona fizyczna najważniejszych postaci organizacji oraz infrastruktury krytycznej,
      – wywiad, w tym elementy kontrwywiadu zagranicznego (współpraca z innymi organizacjami, m.in. wywiadami innych państw, w celu przygotowywania operacji bądź uzyskiwania informacji),
      – kontrwywiad;
5) podsystemy wsparcia:
   a) społeczne:

[40] C.A. Wege, *The Hizballah Security Apparatus* [online], http://www.terrorismanalysts.com/pt/index.php/pot/article/view/42/html [dostęp: 28 XII 2015].

[41] Specyfika funkcjonowania organizacji nie pozwala na jednoznaczny podział, gdyż IRGC ma swoich przedstawicieli w Radzie Szura oraz w innych komórkach organizacji.

[42] Wszystkie decyzje muszą być zatwierdzone przez *al-wali al-faqih* (duchowego przywódcę Islamskiej Republiki Iranu) i zgodne z jego wolą.

[43] Tej Rady nie należy uznawać za typowy organ sztabowy.

- ideologia i tożsamość (*panislamizm i arabsko-islamski nacjonalizm*[44]),
- media, propaganda, indoktrynacja,
- rekrutacja, edukacja i szkolenie członków organizacji,
- służba zdrowia i pomoc społeczna, szczególnie dla członków organizacji, męczenników i ich rodzin,
- potencjał demograficzny, o czym świadczy dwukrotne zwiększenie procentowego udziału społeczności szyickiej na przestrzeni około 70 lat (z 19,6 proc. w 1932 r. do 40 proc. w 2005 r.)[45];

b) gospodarcze:

- gromadzenie środków finansowych na działalność w kraju i poza granicami,
- logistyka,
- tworzenie podstaw egzystencji, szczególnie szyickiej części libańskiego społeczeństwa.

Aparat Militarny i Bezpieczeństwa nie jest samodzielnym bytem, który jest niezależny od całości działań w innych sferach, m.in. społecznej[46]. Podlega bezpośrednio Radzie ds. Dżihadu (Jihad Council). Po kilku dekadach funkcjonowania organizacji Aparat Militarny i Bezpieczeństwa stał się tak potężnym narzędziem, że irańscy mocodawcy zdecydowali o podporządkowaniu tego skrzydła organizacji Zastępcy Sekretarza Generalnego Naimowi Qassemowi[47]. Takie działanie miało prawdopodobnie na celu: zrównoważenie pozycji przywódcy ugrupowania Hassana Nasrallaha i jego kontrolowanie, decentralizację kierownictwa organizacji[48] oraz zwiększenie kontroli nad Aparatem przez IRGC.

W ocenie amerykańskiego naukowca Carla Anthony'ego Wege'a, badacza organizacji Hezbollah, sprawowanie administracyjnej kontroli nad skrzydłem militarnym oraz organem bezpieczeństwa jest problematyczne. Aparat został przekształcony z paramilitarnej bojówki w zaawansowaną specjalistyczną strukturę. Organizacja dzięki rozwiniętej infrastrukturze oraz obowiązującym wewnętrznym procedurom jest niezwykle trudna do spenetrowania przez wywiady państw trzecich. Struktura operacyjna części militarnej jest stworzona na bazie sekretnych komórek funkcjonujących na danym terytorium i prowadzących samodzielne operacje, które kierują się wytycznymi kierownictwa organizacji bez potrzeby wykorzystywania bieżącej łączności[49]. Płynność tej struktury, a w zasadzie mgławicowy układ, w dużym stopniu ogranicza możliwości zakłócania działań operacyjnych komórek przez czynniki zewnętrzne.

Przy tworzeniu Aparatu Militarnego i Bezpieczeństwa oraz jego poszczególnych komponentów wykorzystywano także doświadczenia palestyńskie. Jednym z takich rozwiązań było utworzenie przez Hezbollah Organizacji Islamskiego Dżihadu (JIO[50]) jako

---

[44] Zob. R. Ożarowski, *Hezbollah*…, s. 48.

[45] Zob. Y. Hazran, *The Shiite Community in Lebanon from marginalization to ascendancy,* „Middle East Brief" 2009, nr 37; także: http://www.brandeis.edu/crown/publications/meb/MEB 37.pdf, s. 3 [dostęp: 3 I 2016].

[46] Zob. M. Levitt, *Hizbollah and the Qods Force in Iran's Shadow War with the West*, „Policy Focus" 2013, nr 123, s. 13.

[47] Zob. J. Gleis, B. Berti, *Hezbollah and Hamas*…, s. 63–64 oraz R. Nahmias, *Report: Nasrallah replaced as head of Hizbullah military wing* [online], www.ynetnews.com/articles/0,7340,L-34825380,00.html [dostęp: 29 XII 2015].

[48] W przypadku zlikwidowania szefa część militarna organizacji w dalszym ciągu będzie miała swoje dowództwo.

[49] Zob. N. Qassem, *Hizbullah*…, s. 69–72.

[50] Ang. I*slamic Jihad Organization* (arab. Harakat al-Dżihad al-Islami). Organizacja znana jest też jako ESO (ang. External Security Organization).

odpowiednika palestyńskiego Czarnego Września. *Członkowie aparatu są specjalnie selekcjonowani oraz poddawani wielopoziomowemu szkoleniu*[51], a także wieloetapowej weryfikacji. Rekruci muszą przedstawiać (…) *specjalne list(-y) polecające od jednego z członków Hezbollahu wyższej rangi (duchownych) lub innych przedstawicieli, do których organizacja posiada zaufanie*[52]. Odrębną weryfikację prowadzi Organ Bezpieczeństwa – odpowiednik kontrwywiadu, który (…) *po zakończeniu postępowania sprawdzającego wydaje certyfikat bezpieczeństwa. Jest to niezbędne, aby rekrut został członkiem Partii Boga*[53].

Jak już wspomniano, organizacja dysponuje własnym potencjałem obronnym, ochronnym oraz społecznym, a także elementami gospodarczego potencjału bezpieczeństwa. Struktury Aparatu wchodzą w skład potencjału obronnego i ochronnego, do których należy zaliczyć również część niemilitarną struktury (np. komórka ds. zewnętrznych oraz biuro ds. koordynacji).

Aktywność oraz główne zadania całego Aparatu Militarnego i Bezpieczeństwa można podzielić następująco:

1) w sferze zewnętrznej (funkcje obrony i wsparcia):
   a) realizacja zadań stawianych przez Iran,
   b) obrona terytorium Libanu, szczególnie terenów zamieszkałych przez szyitów,
   c) ochrona organizacji,
   d) zapewnienie bezpiecznego funkcjonowania organizacji;
2) w sferze wewnętrznej (środek pomocy i przemocy):
   a) ochrona wewnętrzna organizacji,
   b) ochrona fizyczna kierownictwa organizacji i obiektów infrastruktury krytycznej,
   c) zapewnienie bezpieczeństwa i porządku publicznego na obszarach kontrolowanych przez organizację.

Aparat Militarny i Bezpieczeństwa oprócz działań militarnych ma również możliwości działania w wymiarze niemilitarnym. Można do nich zaliczyć działania o charakterze terrorystycznym, partyzanckim, a także kryminalnym. Aparatem militarnym kierował bezpośrednio Mustapha Badredine[54], a jego najbardziej tajną częścią – Talal Hamiyeh[55], natomiast Organem Bezpieczeństwa organizacji kierował Wafiq Safa. Aparat militarny jest nadzorowany przez irańskie resorty: obrony oraz wywiadu i bezpieczeństwa. Bezpośredni wpływ na kształt tej jednostki oraz realizowane przez nią zadania ma Pasdaran i funkcjonujące w ramach jego struktur jednostki specjalne: Qods Force i Unit 400 oraz MOIS (w sferze wywiadowczej). Na funkcjonowanie Aparatu wpływa również syryjska służba bezpieczeństwa[56], która dostarcza organizacji niezbędnych informacji.

Hezbollah ma dużo większe możliwości w sferach wywiadu i kontrwywiadu niż pozostałe organizacje tego typu, np. Al-Kaida. Jest to związane między innymi z możliwością kontaktu z irańskimi dyplomatami oraz dostępem do bezpiecznych środków

[51] W zakresach: militarnym i kulturowym. Rekrutacja i szkolenia członków są prowadzone w Skautach Mahdiego (czyli „młodzieżówce Hezbollahu", do której należą dzieci i młodzież w wieku 8–16 lat), w szkołach i na uniwersytetach, również wobec nauczycieli i wykładowców. Jest to także misja wszystkich ośrodków stworzonych wokół organizacji Hezbollah, których to jednym z zadań jest wspieranie procesu rekrutacji nowych członków. Zob. N. Qassem, *Hizbullah*…, s. 60–61.

[52] A.N. Hamzeh, *In the Path* …, s. 76.

[53] Tamże, s. 76.

[54] Szef Islamic Resistance, który zginął pod Damaszkiem w maju 2016 r.

[55] Zob. http://stop910.com/en/danger1.php i danger2 [dostęp: 2 IX 2014].

[56] W chwili obecnej wydaje się, że role mogły zostać odwrócone.

komunikacji. Organizacja może również korzystać z zasobów informacyjnych Libanu, zarówno dzięki ministrom[57] wywodzącym się z bloku 8 Marca i wchodzącym w skład rządu, jak i bezpośrednio dzięki Dyrekcji Generalnej Służby Bezpieczeństwa, z którą współpracują organy bezpieczeństwa Hezbollahu[58]. *W sferze zewnętrznej aparat bezpieczeństwa współpracuje z Departamentem Spraw Zewnętrznych Hezbollahu*[59].

Bez wątpienia utrzymywanie swojego skrzydła zbrojnego przez Hezbollah stanowi wyznacznik jego siły i określa pozycję w realiach międzynarodowych, szczególnie w konfrontacji z Izraelem. Zaplecze siły militarnej pozwala też na kreowanie swojego interesu na scenie politycznej Libanu[60], gdyż to ugrupowanie jest postrzegane jako superpartia, ale także – przez część społeczeństwa – jako jedyna siła, która może obronić i ochronić Liban przed zagrożeniami zewnętrznymi, zwłaszcza ze strony Izraela. Takie przeświadczenie istnieje po konflikcie, który miał miejsce w 2006 r. W tym miejscu można się jednak pokusić o stwierdzenie, że utrzymywanie przez organizację Hezbollah struktury militarnej i bezpieczeństwa jest również próbą osiągnięcia (…) *czterech efektów strategicznych*, tj. (...) *odstraszanie, przeciwzaskoczenie, uniemożliwienie wtargnięcia na własne terytorium, skuteczna odpowiedź w przypadku wtargnięcia na terytorium*[61].

Wywiad organizacji Hezbollah

Jeśli traktuje się proces zbierania i analizowania informacji jako „system nerwowy struktury rządzenia"[62], to należy uznać, że informacja jest tym cenniejsza, im jest bardziej tajna[63]. Informacja nabiera szczególnego znaczenia, zwłaszcza gdy dotyczy wroga bądź rywala. O tym, jak istotna jest informacja o przeciwniku i jak ważne jest jej zdobywanie przez wyszkolone osoby, pisał Sun Tzu już w VI w. p.n.e. Informacja jest tym bardziej cenna, im bardziej dotyczy nadchodzących zagrożeń – umożliwia wtedy m.in. przygotowania się do przeciwdziałania tym niekorzystnym zjawiskom lub reagowania na nie. Domeną wywiadu (…) *jest uzyskiwanie informacji, jej gromadzenie, przetwarzanie oraz przekazywanie decydentom*[64]. Procesy te są realizowane nie tylko przez instytucje państwowe, lecz także pozarządowe. Wszystkie wywiady mają jeden i ten sam cel – wyposażenie decydentów w wiedzę umożliwiającą podejmowanie przez nich jak najkorzystniejszych decyzji, które dotyczą funkcjonowania danej organizacji. *Termin „wywiad" rozumie się nawet szerzej, „jako proces, w którym społeczeństwo, struktura społeczna czy przemysłowa, czy nawet osoba prywatna zbiera informacje, przetwarza je*

[57] Między innymi minister spraw zagranicznych Gebran Bassil (maronita, Free Patriotic Movement); minister stanu Muhammad Fneish (szyita, Hezbollah); minister przemysłu Hussein Hajj Hassan (szyita, Hezbollah); minister finansów Ali Hasan Khalil (Amal); minister pracy i transportu Ghazi Zeaiter (szyita, Liberation and Development Bloc).

[58] Zob. http://www.washingtoninstitute.org/policy-analysis/view/lebanon-unstable-and-insecure [dostęp: 20 IV 2016].

[59] M. Levitt, *Hizbollah*…, s. 15.

[60] R. Ożarowski, *Hezbollah*…, s. 78.

[61] Zob. M. Fryc, *Polska strategia obronności wobec zagrożenia militarnego z elementami „wojny hybrydowej"*, w: „Bezpieczeństwo Narodowe" 2015 nr 1, s. 67.

[62] M. Herman, *Potęga wywiadu*, Warszawa 2002, s. 11.

[63] Tę tezę można postawić chociażby po analizie polskich regulacji prawnych w tym zakresie.

[64] Według słownika terminów AON wywiad to (…) *działania ukierunkowane na legalne i nielegalne zbieranie oraz opracowywanie wiadomości dotyczących państw obcych, a szczególnie ich kondycji gospodarczej i stanu bezpieczeństwa*, zob. *Słownik terminów z zakresu bezpieczeństwa Akademii Obrony Narodowej*, Warszawa 2012 r., s. 150.

i ocenia". Przechowuje i wykorzystuje w swoich działaniach[65]. Wywiad to (…) *najbardziej tajemnicza działalność struktur danej organizacji często wiąże się z nielegalnym zdobywaniem informacji o przedmiocie zainteresowania*[66].

Każda struktura zajmująca się wywiadem, aby zdobyć informacje interesujące dla decydentów, musi stosować kombinację różnego rodzaju metod operacyjnych. Ich dobór jest uzależniony od wielu czynników. Jednym z najważniejszych sposobów, który wykorzystuje człowieka jako najsłabsze ogniwo systemu bezpieczeństwa, jest posługiwanie się szeroko rozumianymi źródłami osobowymi (HUMINT).

Hezbollah jest jedną z niewielu organizacji, która ma możliwości, struktury oraz wykwalifikowane kadry wywiadowcze. Członkowie organizacji prowadzą operacje na całym świecie, również we współpracy z komórkami wywiadowczymi innych podmiotów, w tym także państwowych. Współpraca logistyczna i operacyjna jest budowana przede wszystkim na diasporach: libańskiej, arabskiej (np. irackiej, syryjskiej), muzułmańskiej, a także dzięki realizacji wspólnych interesów (np. działalność w Ameryce Południowej, współpraca z Al-Kaidą w Afryce). Działalność wywiadowcza jest prowadzona na wielu poziomach przez różne komórki organizacji (w tym również bojowe, np. IJO).

Autorzy ośrodka STRATFOR po przeanalizowaniu działalności Partii Boga w 2007 r. dostrzegli funkcjonowanie w ramach jej struktury aparatu wywiadowczego, który jest czynny w USA[67]. Analizie została poddana siatka, której udało się spenetrować Federalne Biuro Śledcze (FBI), Centralną Agencję Wywiadowczą (CIA) oraz Korpus Marynarki Wojennej USA. Hezbollah zdołał umieścić w CIA Nadę Nadim Prouty (Nada Nadim Al Aouar), która legalnie wjechała na terytorium USA, następnie uzyskała obywatelstwo amerykańskie dzięki zawarciu małżeństwa z obywatelem USA odbywającym służbę m.in. w piechocie morskiej podczas operacji Pustynna Burza. Pracę rozpoczęła w FBI, następnie przeniosła się do CIA. Po rozwodzie wyszła za mąż za członka służby zagranicznej USA, który był skierowany do pracy w Islamabadzie oraz w Kairze. Do Nady doprowadziło prawdopodobnie śledztwo prowadzone wobec jej siostry Elfat Al Aouar i jej męża (członka komórki Hezbollahu zajmującej się finansami) oraz Ruli Nadim Al Aouar[68]. Warto odnotować, że koleżanka Nady – Samar Spinelli służyła w marynarce wojennej USA w stopniu kapitana (dwukrotnie pełniła służbę w Iraku).

Ulokowanie agentów w najczulszym miejscu systemu bezpieczeństwa, jakim są służby specjalne, może przynosić wiele korzyści – poczynając od poznania metod rekrutacji, szkolenia przez zdobycie informacji na temat lokalizacji stacji wywiadowczych czy funkcjonariuszy i agentów działających w innych krajach, po kierunki działań infiltrowanych agencji wywiadowczych. Tego typu informacje są niezwykle cennym „towarem" i mogą być wymieniane z największymi rywalami Stanów Zjednoczonych, np. z Rosją, Chinami, w zamian za wsparcie Iranu oraz Hezbollahu[69].

---

[65] M. Herman, *Potęga wywiadu*…, s. 11.

[66] Szerzej na temat terminu w y w i a d zob. S. Zalewski, *Służby specjalne w państwie demokratycznym*, Warszawa 2002, s. 14.

[67] Zob. F. Burton, S. Stewart, *Hezbollah: Signs a sophisticated intelligence apparatus*, Austin 2007.

[68] Zob. C.A. Wege, *The Hizballah Security Apparatus*…

[69] Opisana operacja jest przykładem działania w sferze wywiadu. Hezbollah wielokrotnie plasował i prawdopodobnie dalej umieszcza (pozyskuje) swoich agentów na kierunkach strategicznych, przede wszystkim na terenie Izraela, zob. np.: T. Otłowski, *Hezbollah 1982–2010: od „pasów szahida" po rakiety balistyczne* [online], http://www.geopolityka.org/analizy/500-hezbollah-1982-2010-od-'pasow-szahida'-po-rakiety-balistyczne [dostęp: 14 V 2016] i D. Brenner, *Officer who aided Hezbollah released for health reasons* [online], http://www.israelhayom.com/site/newsletter_article.php?id=3918 [dostęp: 14 V 2016].

Partia Boga jest jedną z nielicznych organizacji, która jest zdolna do prowadzenia operacji wywiadowczych na świecie z wykorzystaniem praktycznie wszystkich metod i źródeł wywiadowczych (w tym HUMINT, SIGINT[70], IMINT[71], MASINT[72]) lub ma do nich dostęp przez wywiad irański, syryjski i północnokoreański, a także specjalną jednostkę Federalnej Służby Bezpieczeństwa Federacji Rosyjskiej[73]. Ponadto (…) *dowódcy komórek oraz operatorzy wywiadu*, w tym zajmujący się wywiadem elektronicznym i walką elektroniczną, (…) *organizacji Hezbollahu są szkoleni w irańskich, syryjskich i północnokoreańskich ośrodkach szkoleniowych sił specjalnych i wywiadu*[74].

Jeden z badaczy Hezbollahu, były pracownik FBI, do głównych zadań jednostki wywiadu zagranicznego tej organizacji zaliczył[75]: (…) *szpiegostwo; kontrwywiad; infiltrowanie środowisk diaspory libańskiej, szyickiej i muzułmańskiej; infiltrowanie organizacji ekstremistycznych, środowisk biznesowych i sieci przestępczych; organizowanie i wsparcie innych komórek Partii Boga w organizacji zamachów*. Celem działania wywiadu zagranicznego jest także wsparcie jednostek operujących poza granicami. Wywiad organizacji ściśle współpracuje z komórką ds. działań zewnętrznych, która zajmuje się m.in. gromadzeniem i dystrybucją środków finansowych oraz działaniami propagandowymi.

Głównymi kierunkami aktywności wywiadu Hezbollahu są kraje rywalizujące i wrogie Iranowi (przede wszystkim Izrael, Stany Zjednoczone, Arabia Saudyjska) oraz te, w których znajdują się diaspory: libańska, szyicka oraz inne, określane ogólnie jako arabskie i szerzej – muzułmańskie (na mapie zaznaczono wykryte komórki Hezbollahu). Tajlandia, państwa zachodnioafrykańskie (np. Senegal, Wybrzeże Kości Słoniowej, Angola, Nigeria, Somalia), państwa Ameryk[76] oraz Australia są traktowane przede wszystkim jako miejsca rekrutacji bojowników, zbierania informacji, a także gromadzenia funduszy na działalność Hezbollahu, np. podczas prowadzenia działań przestępczych. Podobnie traktowana jest Polska[77]. W Afryce Hezbollah współpracuje z różnymi grupami[78].

[70] Ang. *Signals Intelligence* – wywiad sygnałów – rodzaj działalności wywiadowczej (rozpoznawczej) prowadzonej w środowisku promieniowania elektromagnetycznego, między innymi w telekomunikacji, teleinformatyce (przyp. red.).

[71] Ang. *Imagery Intelligence* – rozpoznanie obrazowe, umożliwiające wytwarzanie danych na podstawie zobrazowania pochodzącego ze zdjęć fotograficznych (PHOTINT), radiolokatorów, przyrządów elektrooptycznych pracujących w podczerwieni i termowizyjnych oraz innych urządzeń (przyp. red.).

[72] Ang. *Measurement and Signature Intelligence* – rozpoznanie pomiarowe i sygnaturowe (przyp. red.).

[73] Zob. M. Rudner, *Hizbullah: An Organizational and Operational Profile*, "International Journal of Intelligence and Counterintelligence" 2010, nr 2.

[74] Zob. C.A. Wege, *The Hizballah-North Korean Nexus*, „Small Wars Journal" [online] z 23 stycznia 2011 r. [dostęp: 28 XII 2015]; Y. Denoël, *Sekretne wojny Mossadu*, Warszawa 2013.

[75] Zob. M. Levitt, *Hizbollah*…, s. 15.

[76] Amerykańskie cele są atakowane głównie poza terytorium USA, które jest wykorzystywane jako miejsce zbierania funduszy i danych wywiadowczych. Najważniejszym celem ataków jest Izrael.

[77] Zob. m.in. B. Weinthal, *A False Distinction: The Division of Hezbollah into Political and Military Wings*, „Friends of Israel Initiative" [online], 2013, nr 14, http://www.friendsofisraelinitiative.org/uploads/papers/pdf/FOI_Paper14.pdf. Sprawcy, którzy przeprowadzili atak na autobus z izraelskimi turystami w Burgas, przedostali się do Bułgarii m.in. przez Polskę.

[78] Przy obrocie narkotykami i diamentami grupa współpracuje m.in. z Al-Kaidą.

Mapa. Miejsca aktywności organizacji Hezbollah na świecie.

Źródło: Opracowanie własne na podstawie danych zawartych w literaturze przedmiotu badań. Podkład: Mapa Visibone Country Chart.

Hezbollah utworzył międzynarodową sieć komórek działających w wielu państwach świata. *Analitycy oceniają liczebność tej sieci na około 15 tys. osób*[79]. Obecność organizacji w Ameryce Południowej[80] jest związana przede wszystkim z bliskimi relacjami Iranu z krajami tego regionu, np. Nikaraguą, Boliwią i Wenezuelą[81]. Żołnierze i funkcjonariusze Qods Force oraz irańskiego wywiadu – którzy w tym regionie działają pod przykryciem dyplomatycznym, w biznesie, centrach kulturowych oraz w fundacjach prowadzących działalność charytatywną – blisko współpracują z członkami Partii Boga. Rezultatem tego są m.in. działania, których celem stała się izraelska ambasada w Buenos Aires[82]. Analizowane ugrupowanie operuje także w TBA (*tri-border area*, tzw. Trójkącie Trzech Granic)[83] z uwagi na to, że jest to region zamieszkały przez libańską diasporę (Libańczycy to najbardziej liczna w tym regionie grupa imigrantów arabskich), Chińczyków oraz Rosjan.

Hezbollah utworzył także sieć komórek operacyjnych oraz logistyczno-finansowych w Europie. Czynnikiem umożliwiającym działalność operacyjną na terenie Unii Europejskiej jest m.in. swoboda przepływu osób i kapitału. Dopiero uznanie przez Unię Europejską militarnego skrzydła Partii Boga za terrorystyczne[84], spowodowało, że działalność w tym regionie była utrudniona, co zmusiło organizację do przeprowadzenia zmian.

[79] M. Rudner, *Hizbullah*…, s. 237.

[80] Hezbollah zbierał rocznie około 50 mln dolarów, tamże, s. 240.

[81] W Wenezueli IRGC prawdopodobnie zajmuje się szkoleniem wenezuelskiej armii oraz kolumbijskich rewolucyjnych sił zbrojnych z prowadzenia działań nieregularnych.

[82] Zob. S. Stewart, *Hezbollah, Radical but Rational* [online], http://www.worldsecuritynetwork.com/Terrorism-Broader-Middle-East-United-States-Iran-Israel-Palestine/Stewart-Scott/Hezbollah-Radical-but-Rational [dostęp: 10 I 2016].

[83] Argentyna, Paragwaj, Brazylia.

[84] http://eu-un.europa.eu/articles/en/article_13820_en.htm [dostęp: 24 I 2016].

Po wykryciu w jednostce 910 (Unit 910 – IJO) agenta pracującego dla izraelskiego wywiadu cywilnego, przeprowadzono zmiany w funkcjonowaniu organizacji. Utworzono wówczas jednostkę 133 (Unit 133), do której zadań należy m.in.: prowadzenie operacji specjalnych, wywiad (szczególnie HUMINT), ochrona przemytu narkotyków, wyspecjalizowanych urządzeń oraz materiałów wybuchowych i uzbrojenia. *Jednostka operuje na terenie Europy, a także w Izraelu, na Zachodnim Brzegu i Jordanii*[85]*. Natomiast w Kanadzie głównymi zadaniami komórek operacyjnych organizacji są: zbieranie środków finansowych, zakupy i dostawy uzbrojenia, materiałów podwójnego zastosowania, w tym z terenu USA, oraz rekrutacja nowych członków i uzyskiwanie kanadyjskich dokumentów podróży*[86].

Bardzo ważnym elementem potencjału wywiadowczego organizacji są informacje pochodzące od wywiadów irańskiego, syryjskiego, północnokoreańskiego oraz rosyjskiego. W 2006 r. podczas konfliktu z Izraelem organizacja otrzymywała tego rodzaju dane z dwóch rosyjsko-syryjskich stacji wywiadowczych. Jedną tego typu stację zdobyli bojownicy walczący przeciwko siłom wiernym Baszarowi al-Asadowi w południowej Syrii, niedaleko bazy wojskowej na górze Tel al-Hara w okolicach Wzgórz Golan[87]. Prawdopodobnie Rosjanie dzielili się również danymi wywiadowczymi zebranymi na Morzu Śródziemnym przez siły marynarki wojennej. Stacje zbudowane w okolicach wzgórz znajdujących się niedaleko miast Hara, Nawa i Jaba wykryto po zajęciu Centrum S[88] w al-Hara, w którym znajdowała się mapa z oznaczonymi pozostałymi centrami[89]. Na mapie zaznaczono sieć stacji usytuowanych od Jordanii przez Syrię, Liban i następnie dalej w kierunku Cypru. Te stacje prawdopodobnie prowadziły wywiad radioelektroniczny z kierunków: Jordania, Arabia Saudyjska, Izrael i Egipt.

Wynika z tego, że zadań Hezbollahu realizowanym w Syrii jest m.in. ochrona tego typu instalacji. Obecnie ugrupowanie jest jednym z podmiotów, który w warunkach syryjskich może zapewnić bezpieczeństwo rosyjsko-syryjskim instalacjom, dzięki czemu Iran może otrzymywać dane wywiadowcze zbierane przez te stacje.

Na aktywność komórek wywiadowczych Partii Boga na Bliskim Wschodzie zwracają uwagę również służby kontrwywiadowcze państw arabskich. W Kuwejcie w 2015 r. dokonano aresztowań kilkudziesięciu osób za działalność szpiegowską na rzecz Iranu oraz Hezbollahu, a także za przemyt uzbrojenia, w tym materiałów wybuchowych[90]. W Bahrajnie zlikwidowano komórkę (Brygada Al Ashtar) działającą na rzecz tych dwóch podmiotów, która planowała dokonania zamachów w tym królestwie[91].

Istotne jest również funkcjonowanie komórki ds. bezpieczeństwa strategicznego, gdyż działania tej jednostki dotyczą obszaru Bliskiego Wschodu i Afryki północnej i polegają na monitorowaniu teatru działań, a przede wszystkim – ruchów wojsk amerykańskich i izraelskich[92]

[85] Zob. http://www.israeldefence.com/ oraz https://stop910.com/.

[86] M. Rudner, *Hizbullah*…, s. 239.

[87] http://www.telegraph.co.uk/news/worldnews/europe/russia/11148857/Russian-spy-base-in-Syria-used-to-monitor-rebels-and-Israel-seized.html [dostęp: 26 I 2016].

[88] Rosyjsko-syryjska baza wywiadowcza.

[89] Zob. http://www.telegraph.co.uk/news/worldnews/europe/russia/11148857/Russian-spy-base-in-Syria-used-to-monitor-rebels-and-Israel-seized.html [dostęp: 26 I 2016].

[90] Zob. http://www.albawaba.com/news/kuwait-arrests-24-people-having-links-iran-hezbollah-738450 oraz http://www.albawaba.com/news/kuwait-busts-%E2%80%98terror%E2%80%99-cell-linked-hezbollah-seizes-arms-cache-730860 [dostęp: 24 I 2016].

[91] http://www.middleeasteye.net/news/bahrain-arrests-terror-cell-alleged-links-hezbollah-and-revolutionary-guard-2132070689 [dostęp: 24 I 2016].

[92] www.saidonline.com/newsapp.php?go=fullnewsid=44083, al-ǧumhuriya [dostęp: 20 XI 2016].

Zdolności wywiadowcze organizacji rozwijają się od wielu lat pod okiem przede wszystkim irańskich instruktorów, ale także – jak już wcześniej wspomniano – syryjskich, północnokoreańskich oraz rosyjskich. Nacisk na rozwój wywiadu położono w czasie, kiedy izraelskie i amerykańskie służby zorientowały się, że na terenie Bliskiego Wschodu powstał gracz, który będzie mógł wpływać na sytuację bezpieczeństwa.

Poniżej przedstawiono cele działalności wywiadu Hezbollahu, które można podzielić na[93]:

- **cele strategiczne**:
  - uzyskiwanie informacji wywiadowczych na potrzeby wywiadu irańskiego, w tym ochrona i osłona interesów irańskich na całym świecie,
  - rozpoznawanie zagrożeń bezpieczeństwa organizacji, szczególnie ze strony Izraela, Stanów Zjednoczonych i innych państw oraz organizacji niepaństwowych,
  - rozpoznawanie zagrożeń zewnętrznych i wewnętrznych bezpieczeństwa szyickiej społeczności Libanu;
- **cele operacyjne (taktyczne):**
  - rozpoznawanie i identyfikacja celów ataków wymierzonych głównie w interesy izraelskie i amerykańskie na całym świecie,
  - uzyskiwanie i gromadzenie informacji wywiadowczych na terenach objętych konfliktami zbrojnymi, które znajdują się w kręgu zainteresowania Iranu,
  - udział w operacjach uzyskiwania i gromadzenia środków finansowych na potrzeby działalności organizacji,
  - osłona kontrwywiadowcza baz, firm i podmiotów zlokalizowanych poza granicami Libanu i Iranu, związanych przede wszystkim z Iranem, a także organizacji i struktur sprzymierzonych,
  - prowadzenie kontrwywiadu zagranicznego (w ograniczonym zakresie).

Dzięki wykorzystywaniu większości metod i źródeł wywiadowczych Hezbollah jest potężnym narzędziem, które mogłoby obecnie funkcjonować samodzielnie. Jednak utrata ideologicznego i politycznego wsparcia Iranu mogłaby oznaczać dla organizacji koniec działalności. Do komórek wywiadowczych kierowani są najlepsi rekruci weryfikowani przez irański wywiad oraz IRGC.

Kontrwywiad organizacji Hezbollah

Kontrwywiad to działania mające na celu (…) *udaremnienie wysiłków wrogich służb wywiadowczych w penetrowaniu lub dekonspirowaniu własnej służby wywiadowczej i realizowanych operacji* [94]. Można go też rozumieć jako (…) *identyfikacja i neutralizacja zagrożeń związanych z działalnością obcych wywiadów oraz manipulacją w celu osiągnięcia określonych korzyści* [95]. Działania kontrwywiadu w ujęciu ogólnym skupiają się na czterech obszarach zainteresowań, którymi są: (…) *działalność organizacji wywiadowczych państw obcych, skrajne organizacje nielegalne rozwijające działalność w kraju – ekstremiści, zagraniczne i krajowe organizacje terrorystyczne, działania eko-*

[93] Podział na strategiczne i taktyczne źródła informacji wywiadowczej został przedstawiony przez M. Hermana, zob. tenże, *Potęga wywiadu*…, s. 130.

[94] Zob. R. Kessler, *CIA od środka,* Warszawa 1994, s. 295.

[95] C.A. Wege, *Hezbollah's Counterintelligence Apparatus, International Journal of Intelligence and Counterintelligence*, „Routledge" [online] z 29 sierpnia 2012 r., s. 771 [dostęp: 14 V 2016].

nomiczne zagrażające bezpieczeństwu lub funkcjonowaniu państwa (organizacji). Przy czym szczególnego wyodrębnienia wymaga kontrwywiad wojskowy [96].

Równolegle do możliwości wywiadowczych i militarnych Hezbollah rozwijał zdolności związane z zapewnieniem bezpieczeństwa funkcjonowania organizacji, w tym ochrony jej kierownictwa i używanej przez nią obiektów oraz instalacji.

Po zorientowaniu się przez wywiady Izraela oraz państw zachodnich, że w Libanie i poza nim funkcjonuje nowa organizacja[97] rozpoczęły się operacje skierowane przeciwko Partii Boga. Iran, chcąc ochronić swoje „dzieło", zaczął rozwijać zdolności wywiadowcze i kontrwywiadowcze Hezbollahu przez modyfikowanie obu obszarów funkcjonowania kontrwywiadu, tj.: pasywny i aktywny (lub też defensywny i ofensywny)[98].

Domeną kontrwywiadu pasywnego są zadania związane przede wszystkim z zabezpieczeniem zasobów organizacji, w tym informacyjnych. Natomiast domeną kontrwywiadu o charakterze aktywnym jest dążenie do rozpoznania działalności obcych służb wywiadowczych, obiektów ich zainteresowania oraz stosowanych przez nie metod. Kontrwywiadem – zarówno pasywnym, jak i aktywnym – w Hezbollahu zajmuje się Organ Bezpieczeństwa (Security Organ). Do jego zadań[99] można zaliczyć: przeciwdziałanie infiltracji ugrupowania, zwalczanie szpiegostwa, ochronę informacji, przeciwdziałanie infiltracji sieci teleinformatycznych i zakłócaniu jej pracy, a także zadania z zakresu ochrony fizycznej osób i mienia (ochrona najważniejszych osób oraz istotnych obiektów i instalacji należących do organizacji).

Hezbollah w zakresie kontrwywiadu współpracuje przede wszystkim z wywiadem irańskim, syryjskim, ale także ze służbami północnokoreańskimi, (…) *które znacznie zwiększyły możliwości organizacji, w szczególności w zakresie wywiadu radioelektronicznego*[100]. Między Organem Bezpieczeństwa organizacji a libańską Dyrekcją Generalną Urzędu Bezpieczeństwa oraz Armią Libańską (ang. Lebanese Armed Forces – LAF) również została nawiązana współpraca[101], szczególnie w zakresie zapewnienia bezpieczeństwa państwa przed zagrożeniami płynącymi z sąsiedniej Syrii.

Komórki kontrwywiadu Hezbollahu współpracowały i prawdopodobnie współpracują z Federalną Służbą Bezpieczeństwa. Przykładem tej współpracy jest np. szeroko zakrojona operacja kontrwywiadowcza z 2009 r., która umożliwiła wykrycie siatki izraelskiej działającej w strukturach Aparatu Militarnego i Bezpieczeństwa[102]. Hezbollah prowadził również operację z użyciem podwójnego agenta, co w 1997 r. zakończyło się śmiercią 12 izraelskich żołnierzy sił specjalnych marynarki wojennej. Kolejnym sukcesem służb specjalnych organizacji było zidentyfikowanie działającego pod „fałszywą flagą" pułkownika izraelskiego wywiadu cywilnego Elhana Tannenbauma[103]. Hezbollah

[96] Zob. S. Zalewski, *Służby specjalne…*, s. 15.

[97] Wysiłki były dotychczas skupione na działalności Organizacji Wyzwolenia Palestyny, która była spenetrowana przez izraelskie służby.

[98] Zob. M. Minkina, *Sztuka wywiadu w państwie współczesnym*, seria: „Gry wywiadów", Warszawa 2014; B. Piasecki, *Kontrwywiad ofensywny jako element systemu bezpieczeństwa państwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10.

[99] Katalog określony m.in. na podstawie: B. Berti, *Hizb Allah's Counterintelligence War*, „CTC Sentinel" 2012, nr 2, także online:: http://www.dtic.mil/dtic/tr/fulltext/u2/a556873.pdf, s. 8; J.L. Gleis, B. Berti, *Hezbollah and Hamas…*; A.N. Hamzeh, *In the Path….*

[100] Zob. C.A. Wege, *The Hizballah – North Korea Nexus…*, s. 5.

[101] Zob. J. Salhani, *Distinction between the Lebanese Army and Hizbullah Fading,* Liban 2015.

[102] M. Rudner, *Hizbullah...*, s. 236.

[103] Zob. C. Jones, *A Reach Greater than the Grasp: Israeli Intelligence and the Conflict in South Lebanon 1990–2000*, „Intelligence and National Security" 2001, nr 3, s. 12.

wykrył również siatkę CIA działającą w Bejrucie – zidentyfikował funkcjonariuszy wywiadu i prowadzonych przez nich libańskich agentów, których miejscem spotkań była restauracja Pizza Hut w Bejrucie[104].

W 2015 r. kontrwywiad Hezbollahu zdemaskował w najbliższym otoczeniu zastępcy sekretarza generalnego organizacji N. Qasema oraz ważnego szyickiego duchownego w Libanie Muhammada Yazbeka, a także w Centralnej Jednostce Bezpieczeństwa (Unit 1000)[105] agentów prowadzonych przez CIA[106]. Wydarzeniem, które jednak miało największy wpływ na funkcjonowanie całego aparatu bezpieczeństwa, było wykrycie agenta Mossadu – Muhammada Shawraby – w Jednostce 910 (External Security Organization) zajmującej się operacjami zagranicznymi[107]. To zdarzenie spowodowało znaczne zmiany w funkcjonowaniu tej jednostki specjalnej – została powołana do życia Jednostka nr 133. Kolejnym sukcesem kontrwywiadu było schwytanie w 1984 r. Williama Buckleya, szefa rezydentury CIA w Bejrucie. Był on starannie wybranym celem. Całą operację Hezbollah przeprowadził przy współpracy z irańskim wywiadem. Informacje, które pozwoliły na rozpracowanie W. Buckleya, zostały zebrane podczas ataku na amerykańską ambasadę w Teheranie w 1979 r.[108]

Wsparcie państw, o których była już mowa, pozwoliło Hezbollahowi na rozwinięcie najlepszego w Libanie aparatu kontrwywiadowczego. Organizacja ma również dostęp do danych libańskiej Dyrekcji Generalnej Urzędu Bezpieczeństwa[109]. Dzięki urzędnikom piastującym stanowiska ministerialne, a pochodzącym z bloku 8 Marca, Hezbollah może zdobywać różnego rodzaju informacje umożliwiające funkcjonowanie Aparatu, i szerzej – całej organizacji.

Wraz z rozwojem Hezbollahu, a także wzrostem możliwości kontrwywiadowczych organizacja, przy wsparciu Iranu oraz Korei Północnej, rozwinęła zdolności w zakresie SIGINT[110]. Zaczęto wykorzystywać cyberprzestrzeń, w której głównym celem była przede wszystkim ochrona interesów irańskich oraz własnych[111]. W ośrodkach Korei Północnej szkolono wyselekcjonowanych członków Partii Boga z wywiadu, kontrwywiadu, (…) *w tym w zakresie SIGINT, budując potencjał organizacji*[112]. Natomiast Iran utworzył na południowych przedmieściach Bejrutu *Cyber War-Room*[113] w kwaterze Organu Bezpieczeństwa organizacji, z którego były prowadzone m.in. ataki na amerykańskie banki oraz saudyjskie i katarskie przedsiębiorstwa przemysłu petrochemicznego,

[104] Zob. J.R. Schindler, *The Counterintelligence Imperative*, „The National Interest" [online] z 29 listopada 2011 r., http://nationalinterest.org [dostęp: 20 III 2014].

[105] Zob. *Hezbollah arrests CIA infiltrator*, „Now" [online] z 24 września 2015 r., https://now.mmedia.me/lb/en/NewsReports/565961-hezbollah-arrests-cia-infiltrator [dostęp: 3 I 2016]; *Hezbollah intensifies purge*, „Intelligence Online" [online] z 4 listopada 2015 r., http://www.intelligenceonline.com/governmentintelligence/2015/11/04/hezbollahintensifiespurge,108109751-ART [dostęp: 3 I 2016]. UNIT 1000 zajmuje się ochroną kwatery głównej Hezbollahu oraz najważniejszych obiektów należących do organizacji.

[106] Zob. *US Spies uncovered in sensitive Hizballah positions*, *claim sources* [online], Al-Araby Al-Jadeed/The New Arab, https://www.alaraby.co.uk/english/politics/2015/9/25/us-spies-uncovered-in-sensitive-hizballah-positions-claim-sources [dostęp: 25 IX 2015].

[107] Muhammad Shawraba – szef ESO/910, zob. *Hezbollah Admits 'Mistakes' after Alleged Israeli Spy Expose* [online], http://www.israelnationalnews.com/News/News.aspx/189541#.VzdoRy_VzIU [dostęp: 14 V 2016].

[108] M. Levitt, *The Global Footprint*…, s. 38.

[109] C.A. Wege, *Hizballah's Counterinteligence Apparatus*…, s. 775.

[110] M. Minkina, *Gry wywiadów*…, s. 177.

[111] Zob. https://counterjihadreport.com/tag/wafiq-safa/ oraz https://www.recordedfuture.com/wafiq-safa-and-irans-cyber-outpost-in-lebanon/ [dostęp: 15 V 2016].

[112] C.A. Wege, *The Hizballah-North Korean Nexus*…, s. 5.

[113] Jednostka ds. cyberprzestrzeni.

a także z którego są kontrolowane działania bezzałogowych aparatów latających (UAV, tzw. drony)[114]. Partia Boga (…) *w 2000 r. za pomocą DDoS zaatakowała internetowe giganty – Yahoo, Amazon, CNN, eBay. Wskutek tych ataków na jakiś czas te serwisy zostały zablokowane. Amerykańscy eksperci twierdzili, że ataki te były testem skuteczności* [115].

Podsumowując, można stwierdzić, że głównymi celami kontrwywiadu Hezbollahu są:

- ochrona zasobów informacyjnych organizacji,
- rozpoznanie i neutralizacja aktywności obcych służb specjalnych na terenie Libanu[116]; szczególnie amerykańskich, izraelskich i saudyjskich,
- zapobieganie i wykrywanie infiltracji Libanu oraz jej neutralizacja, zwłaszcza na terenach zamieszkałych przez szyitów, przez inne państwa i organizacje niepaństwowe,
- przeciwdziałanie infiltracji i zakłócaniu pracy sieci teleinformatycznych organizacji,
- prowadzenie wywiadu radioelektronicznego,
- zapewnienie bezpieczeństwa najważniejszym osobom i głównym instalacjom (infrastruktura krytyczna organizacji), w tym ich ochrona fizyczna,
- zapewnienie, we współpracy z innymi komórkami organizacji, bezpieczeństwa i porządku publicznego na terenach zasiedlonych przez szyitów.

Organ Bezpieczeństwa realizuje również działania, które można uznać za elementy obrony przeciwdywersyjnej i kontrwywiadu wojskowego. Z punktu widzenia działania służb rosyjskich czy irańskich kontrwywiad Hezbollahu może służyć strategicznym celom związanym z rozpoznaniem działalności (np. stosowanych metod operacyjnych, kierunków zainteresowań) służb specjalnych innych państw, szczególnie amerykańskich (wykorzystanie Hezbollahu do prowadzenia działań w zakresie kontrwywiadu zagranicznego na terytorium Libanu). Prawdopodobnie zajmuje się także koordynacją działań prowadzonych przez afiliowane grupy palestyńskie.

Hezbollah jest jedną z nielicznych organizacji, które mają swoje struktury wywiadowcze i kontrwywiadowcze oraz zdolności operowania w zakresie wywiadu i kontrwywiadu. Te możliwości powstały głównie dzięki woli i zaangażowania Iranu. Kontrwywiad Hezbollahu ma niczym nieograniczone możliwości operowania na terytorium Libanu i prawdopodobnie jest jedynym podmiotem, który może zapewnić osłonę kontrwywiadowczą dla tego państwa[117].

Aparat wojskowy organizacji Hezbollah

Jak już wspomniano, Hezbollah rozwija swoje militarne zdolności od początku swojego istnienia. Wzorce czerpie bezpośrednio od założycieli – IRGC, a także czę-

[114] Zob. https://counterjihadreport.com/tag/wafiq-safa/ [dostęp: 15 V 2016].

[115] „E-Terroryzm.pl, Wydanie Specjalne nr II", Rzeszów 2013, s. 20.

[116] Zadania realizowane przy współpracy z libańskimi służbami specjalnymi i wojskiem, a także przy wsparciu Iranu, Rosji i Korei Północnej.

[117] W związku z zaangażowaniem się Hezbollahu w konflikt syryjski po stronie reżimu Baszara al-Asada pojawiło się nowe zagrożenie dla tej organizacji związane z działalnością grup powiązanych z Arabią Saudyjską i saudyjskim wywiadem. Na południowych przedmieściach Bejrutu w Harat Hreik, miejsca połączonego z Hezbollahem, kontrwywiad organizacji wykrył oraz przekazał LAF i libańskiej służbie bezpieczeństwa informacje o penetrowaniu przez komórki ISIS południowych przedmieść Bejrutu, które działają na rzecz saudyjskiego wywiadu. Zob. H. Shaaban, *Security bodies: no ISIS cell in Beirut's southern suburbs*, „The Daily Star" z 11 lutego 2014 r. Komórki ISIS działające na zlecenie saudyjskiego wywiadu pod przykrywką prowadzenia działalności gospodarczej zbierały informacje wywiadowcze. Kamuflażem były piekarnie w Harat Hreik i Bir al-Abed.

ściowo od ugrupowań palestyńskich, których bojownicy wraz z upływem czasu zasilali nowy ruch. Duży wpływ na to miało szkolenie kadr dowódczych w Iranie, Syrii czy Korei Północnej. Nie pominięto przy tym także przygotowania operacyjnego terytorium, na którym Hezbollah funkcjonuje[118].

System militarny organizacji składa się z:

- podsystemu operacyjnego (w jego skład wchodzą jednostki bojowe, rezerwy kadrowe oraz infrastruktura obronna),
- podsystemu wsparcia (tj. przygotowanie bojowników, organizowanie zaplecza logistycznego, w tym uzyskiwanie środków walki),
- podsystemu wsparcia społecznego (zalicza się do niego terytorium wraz ze społecznością szyicką, ośrodki gospodarcze prowadzone przez organizacje itp.).

Ugrupowanie niejednokrotnie demonstrowało swoją siłę i możliwości działania. Zastępca sekretarza generalnego organizacji uważa, że głównym źródłem sukcesów odnoszonych przez Hezbollah na polu walki jest tajność. Jest to oczywiste działanie ze strony organizacji, gdyż w przypadku otwartego konfliktu na szeroką skalę prawdopodobnie by ona nie przetrwała, co pokazała już wojna w 2006 r. (operacja „Wolność dla Samira Kuntara i jego braci").

Po przeanalizowaniu aktywności militarnej Hezbollahu można pokusić się o tezę, że organizacja kieruje się zasadami określonymi przez Sun Tzu i w tym celu stosuje: rozpoznanie, fortel, zaskoczenie, manewr, działania pośrednie i presję psychologiczną. Hezbollah nie ma samodzielności strategicznej do prowadzenia działań wojennych na pełną skalę (chociażby z uwagi na brak wojsk lotniczych, wojsk pancerno-zmechanizowanych itp.). Organizacja dysponuje przygotowanymi operacyjnie terenami, na których funkcjonują jej komórki. Nie dysponuje i nie rozwija jednak nowych rodzajów wojsk, np. pancernych. Za koniecznością utrzymania takiego stanu rzeczy przemawia możliwość wykrycia i neutralizacji tych rodzajów sił, co powodowałoby niemożliwość realizacji nadrzędnego celu, jakim jest zachowanie tajności działań.

Część militarna organizacji (…) *nie jest typową zhierarchizowaną organizacją wojskową*[119]. Jest ona oparta na mgławicowej strukturze – poszczególne komórki są samodzielne operacyjnie i taktycznie. Nie ma tutaj pośrednich struktur dowodzenia. Obecnie cały Aparat Militarny i Bezpieczeństwa jest bezpośrednio podporządkowany zastępcy sekretarza generalnego Partii i Radzie ds. Dżihadu. Taka organizacja struktur ma na celu zminimalizowanie strat własnych w przypadku wykrycia przez wroga jednej z komórek. Proces informacyjno-decyzyjny odbywa się za pośrednictwem (…) *dowódców polowych sektorowych i regionalnych, przy czym komendanci regionalni są zazwyczaj członkami Sztabu Wojskowego, w skład którego wchodzi także przedstawiciel IRGC* [120].

Rdzeniem części militarnej Hezbollahu jest Islamski Ruch Oporu, który można podzielić na dwie części: operacyjną (bojową) oraz wsparcia bojowego (logistyka, rekrutacja). Funkcjonowanie tego Aparatu jest niezwykle trudne do wykrycia, gdyż zgodnie z założeniami (…) *bojownicy prowadzą zwykłe życie (są farmerami, prowadzą własne drobne przedsiębiorstwa itp.). Podczas prowadzenia działań bojowych nie są informowani o założeniach taktyczno-operacyjnych i strategicznych, ani o czasie trwania działań* [121].

[118] Hezbollah ma własną infrastrukturę obronną (militarną oraz pozamilitarną) na terenach zamieszkałych przez szyicką część społeczeństwa.

[119] Zob. J.L. Gleis, B. Berti, *Hezbollah and Hamas*…

[120] A.N. Hamzeh, *In the Path*..., s. 71.

[121] Tamże, s. 72.

Wraz z upływem czasu oraz kumulowaniem doświadczeń historycznych, a także ewolucją priorytetów irańskiej polityki zagranicznej i jednocześnie zmianą metod działania Izraela, Hezbollah zaczął rozwijać inne struktury militarne, uwzględniając przy tym czynnik geograficzny. Organizacja zaczęła rozwijać jednostki morskie, jednostki operatorów UAV oraz prawdopodobnie jednostki rakietowe[122]. Bojownicy są szkoleni w obozach w Libanie, Iranie (Teheran, Isfahan, Maszhad, Ahvaz), Iraku, Syrii a takżew Korei Północnej.

Niezależnie od wymienionych komórek do części militarnej można zaliczyć również jednostki: 1800 i 3800. Pierwsza powstała w 2001 r. i operuje na terenie Izraela oraz Zachodniego Brzegu. Do jej zadań należy między innymi (…) *prowadzenie operacji przeciwko Izraelowi oraz współpraca i współdziałanie z organizacjami palestyńskimi, w tym szkolenie i rekrutacja Palestyńczyków, włączając w to Palestyński Islamski Dżihad oraz Hamas*[123]. Druga jednostka odpowiada za przygotowanie szyitów walczących przeciwko USA w Iraku i Jemenie (obecnie również przeciwko grupom sunnickim powiązanym z Al-Kaidą i ISIS), w tym ich uzbrojenie i wyszkolenie[124]. Działania obu tych jednostek szerzej przeanalizował we wspomnianej już publikacji M. Levitt.

Globalizacja i związany z nią rozwój nowoczesnych technologii spowodował, że do celów militarnych zaczęto powszechnie wykorzystywać drony. Hezbollah utworzył tego rodzaju jednostkę dzięki wsparciu IRGC. *Baza została usytuowana w okolicach Hermel w Południowym Libanie*, gdzie funkcjonuje (…) *30 operatorów przeszkolonych w obozie szkoleniowym w pobliżu Isfahanu*[125]. Do głównych zadań jednostki należy przede wszystkim prowadzenie operacji przeciwko Izraelowi oraz przeciwnikom zaangażowanym w konflikt w Syrii.

W obliczu rosnącego obecnie zagrożenia ze strony grup sunnickich w ramach Aparatu powstała również Brygada Libańskiego Ruchu Oporu[126]. Należą do niej m.in. chrześcijanie zamieszkali Dolinę Bekaa[127], a także sunnici. Hebollah koordynował aktywność grup palestyńskich oraz wspomnianej Brygady, których jednym z zadań było zapewnienie ochrony granicy Libanu.

Hezbollah przez trzy dekady rozwinął wszystkie sfery swojego funkcjonowania. Dla zobrazowania, jak rozwinęły się możliwości militarne organizacji, warto przytoczyć słowa szefa Biura Badań i Analiz wywiadu wojskowego izraelskich sił zbrojnych wypowiedziane podczas wystapienia w Knesecie: *Hezbollah posiada arsenał składający się z tysięcy rakiet różnych typów i zasięgów, włączając w to rakiety na paliwo stałe i pociski*

[122] http://english.aawsat.com [dostęp: 10 III 2016]. W Hezbollahu działa jednostka komandosów wykorzystująca do swoich działań szybkie łodzie wyprodukowane przez Chińczyków. Organizacja posiada również sieć magazynów zbrojeniowych.

[123] J.L. Gleis, B. Berti, *Hezbollah and Hamas*…, s. 65.

[124] Zob. *New Hezbollah Unit Training Shiite Guerrillas Across Mideast* [online], www.algemeiner.com, 2010 [dostęp: 29 XI 2015].

[125] Zob. A. Rosen, *Here'e Hezbollah's game-changing secret drone base* [online], http://www.businessinsider.com/hezbollahs-secret-drone-base-2015-4 [dostęp: 29 XI 2015]; M. Hoening, *Hezbollah and the Use of Drones as a Weapon of Terrorism* [online], https://fas.org/wp-content/uploads/2014/06/Hezbollah-Drones-Spring-2014.pdf; także materiał filmowy z przeprowadzonych operacji udostępniony przez telewizję Al-Manar, zob. https://www.youtube.com/watch?v=agzxU4Nr4Bw [dostęp: 29 XI 2015].

[126] Idea sięga lat 90. XX w. Wówczas do brygad przyjmowano wszystkich chętnych Arabów, którzy stawiali sobie za cel walkę z Izraelem. W skład brygad wchodzili szyici, sunnici i chrześcijanie.

[127] Zob. http://www.al-monitor.com/pulse/originals/2014/08/hezbollah-resistance-arsal-counter-islamic-state-attacks.html#ixzz3KTWUBiTN [dostęp: 1 VIII 2014].

precyzyjnego rażenia (…) *Hezbollah z 2006 r. różni się od Hezbollahu z 2010 r. w zakresie zdolności militarnych, które wzrosły znacząco* [128].

Wpływ funkcjonowania Aparatu Militarnego i Bezpieczeństwa na działanie organizacji Hezbollah oraz jej przyszły kształt

Hezbollah powstał z nadania Iranu i do dnia dzisiejszego stanowi jeden z elementów strategii działania tego państwa w stosunkach międzynarodowych[129]. Początkowo był on stworzony do działań o charakterze zbrojnym (nieregularnym). Ponieważ głównymi celami działania tej organizacji było, według A.N. Hamzeha, wyeliminowanie obcych wojsk i wpływów z Libanu, a także przejęcie władzy w Libanie, militarne skrzydło stanowiło trzon funkcjonowania całej struktury Hezbollahu[130]. Ponadto to ugrupowanie kontrolowało i dalej kontroluje organizacje palestyńskie, które jednocześnie stanowiły jej część[131].

Wpływy Partii Boga znacznie się rozszerzają z uwagi na stale rosnącą liczbę szyitów w Libanie[132]. Czynnik demograficzny może zatem zadecydować i o kształcie państwa libańskiego w przyszłości, i o możliwościach połączenia struktur Hezbollahu ze strukturami państwowymi. Paradoksalnie takie rozwiązanie mogłoby ustabilizować sytuację w Libanie, ale jednocześnie rozpalić wewnętrzny konflikt na tle wyznaniowym.

Hezbollah nie jest sygnatariuszem jakiejkolwiek konwencji międzynarodowej, wobec czego należy postrzegać to ugrupowanie jako narzędzie wykorzystywane przez Iran do realizacji swoich celów i interesów. Dzięki organizacji ten kraj może oddziaływać na sfery, na które władze państwowe nie mają wpływu. Jest to również niezwykle korzystne dla Federacji Rosyjskiej, dla której Bliski Wschód, a szczególnie Zatoka Perska, jest jednym ze strategicznych kierunków i – jak to określił Zbigniew Brzeziński w *Planie gry* – jednym z elementów (…) *trzyzębnego strategicznego apetytu*[133]. Toteż możliwość wpływania na sytuację bezpieczeństwa przez wykorzystanie działań Hezbollahu jest jednym z elementów maskowania aktywności Federacji Rosyjskiej na tym kierunku. Można pokusić się również o stwierdzenie, że Iran otrzymał system S-300 między innymi jako nagrodę za współdziałanie z wojskami rosyjskimi w Syrii i Iraku, w tym za ochronę m.in. stacji wywiadu wojskowego GRU i innych instalacji rosyjskich rozmieszczonych w Syrii. Natomiast czynnikiem, który miał ograniczyć wpływy Hezbollahu (cel taktyczny) i Iranu (cel strategiczny) w Libanie, był program dofinansowania libańskiej armii przez Arabię Saudyjską.

Aparat Militarny i Bezpieczeństwa oraz cała organizacja Hezbollah (w opinii niektórych naukowców nie jest możliwe oddzielenie części wojskowej od politycznej, gdyż obie są ze sobą powiązane i się przenikają) wywiera potężny wpływ na politykę zagraniczną Libanu. Władze libańskie nie mają siły ograniczyć tego wpływu, a w świetle rosnącej liczby szyitów i ich dominacji w strukturze społecznej – wpływ Partii Boga

[128] A. Meranda, *Military Intelligence: Hezbollah Scuds tip of iceberg*, Ynet News Online (Israel) z 4 maja 2010 r., http://www.ynetnews.com/articles/0,7340,L-3884753,00.html [dostęp: 19 V 2015].

[129] R. Ożarowski, *Hezbollah*…, s. 13

[130] A.N. Hamzeh, *In the Path*..., s. 80–108.

[131] Np. Organizacja Sprawiedliwości Rewolucyjnej, Organizacja Uciśnionych na Ziemi, Muzułmański Dżihad dla Wyzwolenia Palestyny. Szerzej: R. Ożarowski, *Hezbollah*…, s. 44.

[132] Około 30% libańskich żołnierzy to szyici. Zastępca Dyrektora Generalnej Służby Bezpieczeństwa to również szyita.

[133] Zob. Z. Brzeziński, *Plan gry,* Warszawa 1990, s. 36.

będzie się zapewne zwiększał. Aparat prawdopodobnie będzie nadal utrzymywał swoje miejsce w organizacji oraz będzie realizował zadania stawiane przede wszystkim przez Iran. Prawdopodobnie nie będzie mógł oddziaływać na zmiany struktur organizacji, gdyż są one kontrolowane przez *al-wali al-faqih*, a sam Aparat został sprowadzony do roli wykonawcy założeń i zadań stawianych przez mocodawcę.

Służba w jednostkach Aparatu Militarnego i Bezpieczeństwa oraz przynależność do Hezbollahu jest w środowisku szyickim prestiżem, wiąże się również z realnymi korzyściami, w tym finansowymi. Stwarza również perspektywy „pracy" poza granicami Libanu (patrz mapa), zdobycia wykształcenia, a przede wszystkim możliwość utrzymania rodziny i zapewnienia jej bezpieczeństwa oraz opieki medycznej. Nierzadko jest to jedyne rozwiązanie dla osób zamieszkujących tereny południowego i wschodniego Libanu. Jednak aby przetrwać i funkcjonować, Aparat Militarny i Bezpieczeństwa, jak również cała organizacja, musi wytworzyć *raison d'etre*, a także być związana z imperialnymi ambicjami Iranu oraz aspiracjami społecznymi w Libanie[134].

Działalność Hezbollahu będzie prawdopodobnie rozwijana i wspierana przez inne podmioty dopóty, dopóki będzie się wpisywała w ich politykę zagraniczną i bezpieczeństwa. Jak długo organizacja będzie zakłócała realizację przez Stany Zjednoczone swoich interesów w regionie, tak długo będzie wspierana przez Federację Rosyjską, Chińską Republikę Ludową oraz Koreańską Republikę Ludowo-Demokratyczną. Szczególnie dotyczy to Aparatu Militarnego i Bezpieczeństwa, który jest bezcennym ośrodkiem oddziaływania na podmioty państwowe w stosunkach międzynarodowych.

Podsumowanie

Artykuł może być przyczynkiem do szerszego i bardziej szczegółowego opracowania dotyczącego Aparatu Militarnego i Bezpieczeństwa Hezbollahu. W kolejnych pracach warto skupić się także na potencjalnym lub rzeczywistym „wykorzystywaniu" tej organizacji do celów politycznych (strategicznych) przez mocarstwa zaangażowane w regionie, tj. USA, Federację Rosyjską, Francję, Chiny i Wielką Brytanię, gdyż pomimo wpisania ugrupowania na listę organizacji terrorystycznych, w mediach pojawiały się wzmianki świadczące o takiej (pośredniej) współpracy. Przykładem może być chociażby ostrzeżenie Hezbollahu – przekazane przez CIA via libańskie służby bezpieczeństwa – o możliwości zorganizowania ataku terrorystycznego przez inne grupy na cele zlokalizowane w południowych, szyickich, przedmieściach Bejrutu.

Partii Boga nie należy rozpatrywać wyłącznie jako islamskiej milicji czy ugrupowania prowadzącego działania o charakterze terrorystycznym. Jest to złożony podmiot, który od wielu lat jest obecny we wszystkich sferach życia w Libanie, ale także – w pewnym sensie –jest czynnikiem stabilizującym sytuację w tym kraju. Znaczenie organizacji oraz jej odbiór, szczególnie w środowisku libańskich szyitów oraz chrześcijan, zmienił się wraz z otwartą konfrontacją z salafickimi organizacjami w Syrii, które dążą do przeniesienia konfliktu na tereny Libanu, a zwłaszcza w miejsca zamieszkałe głównie przez szyitów.

Funkcjonowanie potężnej organizacji w Libanie jest rezultatem słabych struktur państwowych, które nie są w stanie kontrolować swojego terytorium. Tę tezę potwierdza m.in. wypowiedź premiera Izraela Binjamina Netanjahu, który twierdzi, że (…) *obecnie*

[134] C.A. Wege, *The Hizballah Security Apparatus*..., s. 4.

Partia Boga stała się prawdziwą i główną libańską siłą militarną. Armia jest dobrze wyszkolona i posiada coraz lepsze uzbrojenie. Hezbollah oraz libański rząd przenikają się wzajemnie. Jeżeli doszłoby do ataku na Izrael, odpowiedzialność ponoszą wszyscy[135]. Organizacja stworzyła globalną sieć, która jest aktywna na wszystkich kontynentach, i w przeciwieństwie do organizacji typu mgławicowego (Al-Kaida), jest kontrolowana i zarządzana z Libanu. Swoją działalność prowadzi głównie w środowiskach libańskich i muzułmańskich (głównie szyickich).

Prezentowany w mediach obraz rzeczywistości pozwalał wywnioskować, że możliwość oddziaływania Iranu na Hezbollah była ograniczona. Kierownictwo organizacji wielokrotnie starało się przekonać libańskie społeczeństwo, że jest ona niezależnym graczem o zabarwieniu nacjonalistycznym[136], a nie religijną marionetką w syryjskich i irańskich rękach. Ostatnie wydarzenia na Bliskim Wschodzie (od 2011 r.) oraz irańskie poczucie zagrożenia związanego z sytuacją w Syrii spowodowało, że Hezbollah powrócił do realizacji „priorytetów irańskich", wykorzystując nadbudowę ideologiczną związaną z religią[137].

Liban jest jedną z „szachownic"[138], na której rozgrywa się gra (walka) o pozycję regionalnego supermocarstwa. Udział w niej biorą Iran i Arabia Saudyjska[139]. Otwarty konflikt pomiędzy tymi państwami prawdopodobnie nie jest możliwy z uwagi na globalne uwarunkowania oraz zaangażowanie w regionie przede wszystkim USA, Rosji i Turcji. Stąd też sytuację w Libanie, Jemenie oraz w Syrii można określić jako „*proxy war*" (wojnę zastępczą – przyp. red.). Zaangażowanie w sprawę syryjską stawia jednak organizację ponownie w sytuacji bycia irańskim narzędziem w walce o wpływy w regionie Bliskiego Wschodu. A funkcjonowanie silnego Hezbollahu oraz prorosyjskiego Iranu jest niezwykle istotne z punktu widzenia strategii rosyjskiej[140].

Bibliografia:

1. *As–Safir: How did the Resistance Infiltrate CIA's Secret Structure*, S.T. Moughnieh (red. tł.) [program telewizyjny], Bejrut: Al-Manar [wyemitowano: 23 XII 2011].
2. Avon D., Khatchadourian A.T, *Hezbollah. A History of the „Party of God"*, London 2012, Harvard University Press.
3. Bahr-Zohar M., Mishal N., *Mossad*, Poznań 2012, Rebis.
4. Berti B., Gleis J.L., *Hezbollah and Hamas. A comparative study*, Baltimore 2012, The John Hopkins University Press.
5. Berti B., *Hizb Allah's Counterintelligence War*, „CTC Sentinel" 2012 nr 5, Combating Terrorism Center at West Point.

[135] http://www.psz.pl/tekst-25798/Netanyahu-Hezbollah-to-glowna-sila-Libanu; K. Domeracki, *Netanyahu: Hezbollah to główna siła Libanu* [online], www.psz.pl. Portal Spraw Zagranicznych [dostęp: 8 XII 2009].

[136] Szkolenie członków Hezbollahu jest oparte na trzech filarach: patriotyzmie, religii, szkoleniu militarnemu. Źródło: http://news.bbc.co.uk/2/hi/middle_east/8076820.stm [dostęp: 12 VI 2013].

[137] Podstawą działalności organizacji jest połączenie dwóch ideologii – panislamizmu oraz arabsko-islamskiego nacjonalizmu.

[138] Pozostałe to m.in. Jemen oraz Irak.

[139] Pozycja Egiptu w regionie uległa pogorszeniu, Syria i Irak stanęły w obliczu wojny domowej – na bliskowschodniej szachownicy pozostały wyłącznie Iran i Arabia Saudyjska. Ostatnio obserwuje się także wzrost zaangażowania w regionie Turcji, która, próbując wykorzystać irańsko-saudyjską rywalizację, stara się poszerzyć strefę wpływów.

[140] Zob. Z. Brzeziński, *Plan gry*...

6. Brzeziński Z., *Plan gry*, Warszawa 1990, Nowe Wydawnictwo Polskie.
7. Brzeziński Z., *The Grand Chessboard*, Washington 1997, Basic Books.
8. Burton F., Stewart S., *Hezbollah: Signs of Sophisticated Intelligence Apparatus* [online], https://www.stratfor.com/weekly/hezbollah_signs_sophisticated_intelligence_apparatus z 12 XII 2007 r. [dostęp: 14 V 2016].
9. Cohler S., *Hezbollah: Analysis of violence*, American Diplomacy [online] z marca 2011 r., www.unc.edu, [dostęp: 14 V 2016].
10. Cordesman A.H., *Iran's Revolutionary Guards, the Al Quds Force, and Other Intelligence and Paramilitary Forces*, Washington 2007, Center for Strategic and International Studies.
11. Denoël Y., *Sekretne wojny Mossadu*, Warszawa 2013, Czarna Owca.
12. Domeracki K., *Hezbollah i jego zaangażowanie w Syrii*, w: *Wiedza Obronna*, Warszawa 2013, Towarzystwo Wiedzy Obronnej.
13. Domeracki K., *Syria – kolejna próba sił światowych mocarstw?*, „Zeszyty Doktoranckie Wydziału Bezpieczeństwa Narodowego Akademii Obrony Narodowej" 2012, nr 4.
14. Domeracki K., *The Middle East Geopolitical Mosaic*, Warszawa 2012, Art Ideas.
15. „E-Terroryzm. Wydanie specjalne", Rzeszów 2013, Instytut Studiów nad Terroryzmem, Wyższa Szkoła Informatyki i Zarządzania.
16. Hamzeh A.N., *In the path of Hizbullah*, New York 2004, Syracuse University Press.
17. Herman M., *Potęga wywiadu*, Warszawa 2002, Bellona.
18. Katz S., *Aman. Wywiad wojskowy Izraela*, Warszawa 1999, Bellona.
19. Koziej S., *Teoria sztuki wojennej*, Warszawa 2011, Bellona.
20. Levitt M., *Hizballah and the Qods Force in Iran's Shadow War with the West*, „Policy Focus" 2013, nr 123.
21. Levitt M., *If you don't understand our commitment to Iran, you don't understand Hezbollah*, „Weekly Standard" z 13 lutego 2014.
22. Levitt M., *The global footprint of Lebanon's Party of God*, London 2013, Hurst&Company.
23. Levitt M., *Hizb Allah Resurrected: The Party of God's Return to Tradecraft*, „CTC Sentinel" 2013, nr 4, Combating Terrorism Center at West Point.
24. Minkina M., *Sztuka wywiadu w państwie współczesnym,* seria: *Gry wywiadów*, Warszawa 2014, Bellona–Rytm.
25. Ożarowski R., *Hezbollah w stosunkach międzynarodowych na Bliskim Wschodzie*, Gdańsk 2011, Wydawnictwo Uniwersytetu Gdańskiego.
26. Pelc M., *Elementy metodologii badań naukowych*, Warszawa 2012, Akademia Obrony Narodowej.
27. Pelc M., *Wybrane problemy metodologiczne wojskowych badań naukowych*, Warszawa 1998, Akademia Obrony Narodowej.
28. Piasecki B., *Kontrwywiad ofensywny jako element systemu bezpieczeństwa państwa*, „Przegląd Bezpieczeństwa Wewnętrznego" 2014, nr 10.
29. Qassem N., *Hizbullah. The story from within*, London 2005, SAQI.
30. Rudner M., *Hizbullah: An Organizational and Operational Profile*, „International Journal of Intelligence and Counterintelligence" 2010, nr 2.
31. Schindler J.R., *The Counterintelligence Imperative*, "The National Interest" [online] z 29 listopada 2011 r., nationalinterest.org [dostęp: 20 III 2014].
32. Stewart S., *Hezbollah. Radical but Rational* [online], 2010, worldsecuritynetwork.com [dostęp: 20 III 2014].

33. Sun Zi, *Sztuka wojenna*, Ożarów Mazowiecki 2012, Olesiejuk.
34. Wege C.A., *The Hizballah Security Apparatus*, „Perspectives on Terrorism" [online] 2008, nr 7; www. terrorismanalysts.com [dostęp: 28 XII 2015].
35. Wege C.A., *The Hizballah-North Korean Nexus*, „Small Wars Journal" [online] z 23 stycznia 2011 r.; smallwarsjournal.com/blog/journal/docs-temp/654-wege.pdf [dostęp: 28 XII 2015].
36. Wege C.A., *Hizballah's Counterintelligence Apparatus*, „International Journal of Intelligence and Counterintelligence" z 29 lutego 2012 r., Routledge.
37. *Who's watching the spies?*, Born H., Johnson L.K., Leigh I. (red.), Washington 2005, Potomac Books.
38. Zalewski S., *Służby specjalne w państwie demokratycznym*, Warszawa 2002, Akademia Obrony Narodowej.
39. Żebrowski A., *Wywiad i kontrwywiad XXI wieku*, Lublin 2010, Wyższa Szkoła Ekonomii i Innowacji w Lublinie.

Strony internetowe:

1. www.alahednews.com.lb.
2. www.aljazeera.com.
3. www.almanar.com.lb.
4. www.alnour.com.lb.
5. www.buisnessinsider.com.
6. www.dailystar.com.lb.
7. www.haaretz.com.
8. www.israeldefence.com.
9. www.fas.org.
10. www.lebanonwire.com.
11. www.moqawama.org.
12. www.presstv.ir.
13. www.saltspringnews.com.
14. www.stop910.com.
15. www.stratfor.com.
16. www.trackingterrorism.org.
17. www.terrorismanalysts.com.
18. www.worldjewishdaily.com.

Abstrakt

Artykuł stanowi analizę struktury organizacji Hezbollah oraz funkcjonowania jednego z jej najbardziej zakonspirowanych elementów – Aparatu Militarnego i Bezpieczeństwa. Zawiera także między innymi analizę funkcjonowania wywiadu i kontrwywiadu organizacji. W pracy określono znaczenie Aparatu Militarnego i Bezpieczeństwa oraz jego wpływ na kształt organizacji.

Słowa kluczowe: Hezbollah, Partia Boga, wywiad, kontrwywiad, aparat bezpieczeństwa.

Abstract

The paper analyses the structure of Hezbollah and its Military and Security Apparatus, which is the most covert element of the Party of God. The author focuses on Apparatus functioning and attempts to describe its modus operandi. The paper also contains information about a few selected intelligence and counterintelligence operations as well as the attempt to determine the significance of the Apparatus and its influence on Hezbollah.

Keywords: Hezbollah, Party of God, intelligence, counterintelligence, Military and Security Apparatus.

Anna Łasińska

Analiza nieorganicznych i organicznych pozostałości po wystrzale z broni palnej

Wstęp

W kryminalistyce analiza pozostałości powystrzałowych (ang. *gunshut residue,* GSR) jest metodą badań często stosowaną w celu wyjaśniania okoliczności zdarzeń z użyciem broni palnej. Badania pozostałości po wystrzale z broni palnej są prowadzone na polskim rynku kryminalistycznym już od 1998 r. W tym procesie cząsteczki GSR są wykrywane na wskazanych obiektach, takich jak ręce podejrzanego, ubranie, skóra osoby oddającej strzał z broni palnej oraz w otoczeniu domniemanego zdarzenia. Obecność GSR na osobie podejrzanej jest istotnym wskaźnikiem oceny jej zeznania.

Robin Mejia zadał w swojej publikacji kilka pytań na temat wykorzystywania metod badań do analizy pozostałości powystrzałowych: *Która metoda jest najbardziej efektywna*? *W jaki sposób zmniejszyć ilość fałszywych negatywnych lub fałszywych pozytywnych wyników*? *Czy aktualnie możliwe jest stwierdzenie z całą pewnością, że dana osoba oddała strzał z broni palnej*? Istnieje wiele pytań, na które odpowiedź jest bardzo trudna, niejednoznaczna, a wręcz niemożliwa[1].

Aleksandar Ivanović podkreślił, że w ciągu 10 lat swojej intensywnej pracy jako biegły sądowy nadal nie jest w stanie znaleźć na tyle dobrej metody, aby na jej podstawie z całą pewnością stwierdzić, że podejrzany oddał strzał z broni palnej, mimo że wiadomo na sto procent, iż strzelił on z tej broni[2].

Obecnie identyfikacji cząstek powystrzałowych nie nadaje się znamion pewności, lecz dużego prawdopodobieństwa, podobnie zresztą jak w przypadku badań fizykochemicznych wszelkich innych mikrośladów. Niemniej jednak nadal cząstkom trójskładnikowym, zwłaszcza licznie występującym w danym materiale, jest przyporządkowana najwyższa wartość dowodowa. Ustalenie obecności metalicznych cząstek powystrzałowych w materiale pobranym z rąk lub odzieży osoby podejrzanej pozwala stwierdzić z bardzo dużym lub dużym prawdopodobieństwem, że strzelała ona, dotykała broni, z której strzelano, lub jakiegokolwiek zanieczyszczonego pozostałościami powystrzałowymi przedmiotu, lub też znajdowała się w pobliżu, gdy oddano strzał z broni palnej.

Pozostałości powystrzałowe, znane również jako pozostałości powystrzałowe z łuski (ang. *cartridge discharge residue,* CDR) lub pozostałości powystrzałowe z broni palnej (ang. *firearms discharge residue,* FDR), to mikrocząstki powstałe podczas oddawania strzału. W skład pozostałości powystrzałowych wchodzą: niespalone lub częściowo spalone cząsteczki prochu, cząsteczki pochodzące ze spłonki amunicji, pozostałości smarów oraz metale z łuski i użytej broni. Nieorganiczne pozostałości powystrzałowe – azotany, azotyny, cząstki metaliczne – pochodzą właśnie ze spłonki i materiału miotającego oraz z innych źródeł: łuski, płaszcza pocisku, lufy broni. Typowe cząstki GSR mają kształt sferyczny

[1] R. Mejia, *Why we cannot rely on firearms forensics*, „New Scientist" 2005, nr 2527, s. 6.

[2] A. Ivanović, *Is there a way to precisely identify that the suspect fired from the firearm?*, „Forensic Science International" [online] 2003; nr 136 (Supplement 1), s. 158–159, http://www.fsijournal.org/article/S0379-0738(15)00108-5/references.

o rozmiarach rzędu mikrometrów. Są one złożone z odpowiednich metali ciężkich, takich jak: ołów + bar + antymon, tytan + cynk oraz związków strontu[3]. Jako małe, lecz ciężkie drobiny mogą zostać przemieszczone na większe odległości, np. w przypadku pistoletu lub rewolweru kaliber 0.38 tego rodzaju ślady można znaleźć do około 1 m od wylotu lufy[4].

Charakterystycznych, typowych i unikalnych cząsteczek pozostałości nie można się jednak spodziewać w coraz częściej wykorzystywanej czystej, nietoksycznej amunicji, wolnej od ołowiu.

Instytut Wojskowy, Instytut Kryminalistyki oraz departamenty Policji Stanowej w Rio de Janeiro i Sao Paulo w Brazylii od początku XXI wieku prowadzą badania nad nietoksyczną amunicją[5]. Brazylijski rynek broni palnej i amunicji różni się od innych krajów tym, że jest zdominowany przez dwie fabryki broni: strzeleckiej i lekkiej (Industria de Material Belico Brasil, IMBEL i Forjas Taurus SA) oraz tylko jednego producenta amunicji (Companhia Brasileira de Cartuchos, CBC). Ogromna liczba broni i amunicji o różnej konstrukcji jest codziennie zatrzymywana przez organy ścigania, ale w więcej niż w 90% przypadków stosowano oryginalną lub przerobioną amunicję firmy CBC. Przeanalizowano kilka rodzajów nietoksycznej amunicji, pochodzącej z tych firm, wystrzelonej z broni palnej różnego kalibru[6]. Na podstawie analizy EDS (ang. *Energy Dispersive Spektrometry*[7]) w prochu amunicji stwierdzono obecność miedzi (Cu) i cynku (Zn). Przeprowadzono analizę SEM (z wykorzystaniem skaningowego mikroskopu elektronowego SEM) dwóch generacji amunicji, która miała na celu ujawnienie morfologii i składu pozostałości wytworzonych w wyniku spalenia mieszanin. Obserwowano zróżnicowaną wielkość sferoidalnych cząsteczek pomiędzy 0,5 a 20 µm. W przypadku amunicji produkowanej od 1998 do 2002 r. badania prochu wykazały obecność prawie wyłącznie strontu (Sr). Źródłem tego pierwiastka może być deklarowana przez producenta obecność azotanu strontu [$Sr(NO_3)_2$]. Ślady sodu (Na) i potasu (K) często były ujawniane w próbkach pobranych z rąk strzelającego, tak jak i ślady żelaza (Fe). W amunicji kolejnej generacji, produkowanej od 2002 r., stront (Sr) nie był wykrywalny, obserwowano natomiast obecność głównie glinu (Al), krzemu (Si) i potasu (K). Pierwiastki te były obecne w więcej niż 90% cząstek analizowanych w różnych proporcjach. Inne, które wykryto za pomocą mikroanalizatora EDS, to wapń (Ca), siarka (S), sód (Na), magnez (Mg) i chlor (Cl). W próbkach pobranych z lufy lub z ręki strzelającego również wykryto sód (Na), chlor (Cl) i magnez (Mg), ale zwykle jako składnik drugorzędny[8].

W 2011 r. Ingrid T. Weber i inni jako pierwsi zastosowali wysoko fotoluminescencyjne związki chemiczne typu metal – kompleks organiczny w celu znakowania amunicji. Testy przeprowadzono na kompleksach zawierających jony europu (Eu^{3+}) i terbu (Tb) oraz pirydyny (C_5H_5N) i kwasu dikarboksylowego. Wykazano, że znaczniki były

[3] O. Dalby, D. Butler, J. Birkett, *Analysis of gunshot residue and associated materials – a review*, „Journal of Forensic Science" 2010, nr 4, s. 924; L. Gunaratnan, K. Himberg, *The identification of gunshot residue particles from lead free Sintox ammunition*, „Journal of Forensic Science" 1994, nr 39, s. 532; P. Collins i in., *Glass-containing gunshot residue particles: a new type of highly characteristic particle?*, „Journal of Forensic Science" 2003, nr 48, s. 538; *Guide for primer gunshot residue analysis by scanning electron microscopy/energy dispersive X-ray spectrometry* [online], http://www.swggsr.org/documents.html 2011 [dostęp: 1 IX 2016].

[4] H. Meng, B. Caddy, *Gunshot residue analysis – a review*, „Journal of Forensic Science" 1997, nr 42, s. 553.

[5] A. Martiny i in., *SEM/EDS analysis and characterization of gunshot residues from Brazilian lead-free ammunition*, „*Forensic Science International"* 2008, nr 177, s. e9.

[6] Tamże.

[7] Metodą energodyspersyjna spektrometrii rentgenowskiej.

[8] Tamże.

widoczne przy stężeniu około 5% wagowych[9]. W 2012 r. ta sama grupa przeprowadziła testy z wykorzystaniem jonów iterbu (Yb) i terbu (Tb) w kompleksie z pirydyną i kwasem dikarboksylowym[10].

W celu wizualizacyjnej identyfikacji pozostałości powystrzałowych Caline A. Destefani i inni również zastosowali optyczne znaczniki oparte na wysoko fotoluminescencyjnych związkach chemicznych typu metal – kompleks organiczny[11]. W wyniku reakcji jonów europu (Eu^{3+}) z kwasem pikrynowym ($C_6H_3N_3O_7$) i kaprolaktamem metylowym otrzymano znacznik $[Eu(PIC)_3(NMK)_3]$ dający zabarwienie żółte przy emisji o długości 254 nm i czerwone o długości 369 nm. Badania przeprowadzono na konwencjonalnej amunicji typu .38 CBC dostępnej na terenie Ameryki Południowej. Znacznik dodawano do prochu w pięciu różnych stężeniach: 2 mg, 5 mg, 10 mg, 25 mg i 50 mg. Amunicja była ponownie składana. Pozostałości uzyskiwano po wystrzeleniu amunicji z rewolweru Taurus kaliber .38 z odległości 50 cm do tarczy zrobionej z czarnej odzieży. Przed każdym strzałem broń była czyszczona. Analizę wykonywano przy użyciu następujących instrumentów: spektrometru osłabionego całkowitego wewnętrznego odbicia (ATR) w podczerwieni (FTIR-ATR), termograwimetru sprzężonego z różnicową analizą termiczną (TG/DTA) w zakresie temperatur od 25°C do 1000°C, analizatora cyklotronowego rezonansu jonów z fourierowską transformacją ze spektrometrią mas i jonizacją przez elektrorozpylanie (ESI(±)-FT-ICR MS), analizatora cyklotronowego rezonansu jonów z fourierowską transformacją z tandemem spektrometrii mas i jonizacją przez elektrorozpylanie (ESI(±)-FT-ICR MS/MS) oraz spektrofluorometru sprzężonego z lampą ksenonową w zakresie wzbudzenia od 500 do 750 nm w temperaturze pokojowej. Testy wykazały obecność znaczników w pozostałościach powystrzałowych na strzelcu i broni przy stężeniu 25 mg i 50 mg znacznika w prochu. Znaczniki były widoczne nawet po upływie czterech miesięcy od momentu wystrzału.

W 2014 r. I.T. Weber i inni przeprowadzili badania ze znakowaną amunicją nietoksyczną, bezołowiową[12]. Ocenili wpływ znaczników na prędkość pocisków w funkcji ich procentowej zawartości w prochu, możliwości zebrania luminescencyjnych pozostałości powystrzałowych (LGSR), czas, po jakim można zebrać LGSR po umyciu rąk, przenoszenie LGSR na obiekty dotykane przez strzelca, rozproszenie w miejscu symulowanego zdarzenia i na symulowanym poszkodowanym. Zaobserwowano, że zawartość znaczników powyżej 10% wagowych powoduje zmniejszenie prędkości pocisku. Natomiast dodanie znacznika w ilości 2% wagowych minimalizuje efekt spowalniania i pozwala na ujawnienie, zebranie i analizę LGSR. Podczas testów na symulowanym miejscu zdarzenia LGSR ujawniono w odległości do 9,4 m od strzelca i bez problemu znaleziono je na poszkodowanym. Pozostałości LGSR na rękach mytych wielokrotnie (ponad 16 razy) były obecne nawet po 9 godzinach. Pozostałości tego typu mogą być analizowane przy użyciu spektroskopii Ramana oraz SEM/EDS.

[9] I.T. Weber i in., *High photoluminescent metal-organic framework as optical markers for the identification of gunshot residues*, „Analytical Chemistry" 2011, nr 83, s. 4720.

[10] I.T. Weber i in., *Up-conversion properties of lanthanide-organic framework and how to track ammunitions using these materials*, „RSC Advances" 2012, nr 2, s. 3083.

[11] C.A. Destefani i in., *Europium-organic complex as luminescent marker for the visual identification of gunshot residue and characterization by electrospray ionization FT-ICR mass spectrometry*, „Microchemical Journal" 2014, nr 116, s. 216.

[12] I.T. Weber i in., *Use of luminescent gunshot residues markers in forensic context*, „Forensic Science International" 2014, nr 244, s. 276.

Obecnie w niektórych krajach europejskich amunicja używana przez policję jest znakowana specyficznymi, nieorganicznymi pierwiastkami. Znaczniki dodawane do amunicji powodują wzrost formowania się charakterystycznych cząsteczek podczas wystrzału. Przykładem tego jest amunicja produkowana przez RUAG Ammotec AG, która zawiera GdTiZn (mieszanina nieorganiczna gadolinu, tytanu i cynku) i może też zawierać śladowe ilości wapnia (Ca) oraz siarki (S), natomiast amunicja produkowana przez MEN GmbH zawiera w swoim składzie GaCuSn (mieszanina nieorganiczna galu, miedzi i cyny), a także śladowe ilości potasu (K) i siarki (S).

Tym śladom towarzyszą zwykle inne, niecharakterystyczne pozostałości, np. drobiny mosiądzu, stali, kamienia do zapalniczek, siarki i inne. W tym wypadku pomocna będzie analiza organicznych składników pozostałości powystrzałowych OGSR (ang. *organic gunshut residua*).

Organiczne GSR (OGRS) pochodzą głównie z materiału miotającego i smarów używanych do konserwacji broni, występują w postaci niespalonych lub częściowo spalonych cząstek prochu oraz produktów ich przemiany, a także w postaci węglowodorów.

Materiał miotający używany do produkcowania amunicji jest znany jako proch bezdymny. Jest on nisko wybuchowy, szybkość reakcji przebiega na tyle powoli, że pozwala na użycie go jako materiału miotającego dla pocisków. Prochy bezdymne są jednobazowe (nitroceluloza), dwubazowe (nitroceluloza, nitrogliceryna) lub trójbazowe (nitroceluloza, nitrogliceryna, nitroguanidyna). Do produkcji materiału miotającego zwykle wykorzystuje się jeden albo więcej stabilizatorów w zależności od ich struktury chemicznej, co zapobiega spontanicznemu, egzotermicznemu, katalityczno-kwasowemu rozkładowi nitrocelulozy, nitrogliceryny i estrów kwasu azotowego. Difenyloamina (DPA) reaguje z tlenkami azotu tworzonymi przez powolny rozkład nitrocelulozy (NC) i w ten sposób zamienia się na odpowiednie N-nitrozo i nitro-pochodne. Difenyloamina jest czystym stabilizatorem, który, jak inne substancje, takie jak: metylo- i etylocentrality, może dawać efekt stabilizujący i efekt żelowania, co z kolei upraszcza produkcję prochów bezdymnych. Difenyloamina jest stabilizatorem najczęściej stosowanym do prochów jednobazowych, natomiast etylocentrality do prochów dwubazowych, jako substancje żelujące nitroglicerynę. Zwykle materiał miotający zawiera DPA razem z etylocentralitem. W chińskiej amunicji często etylocentralit zastępuje się metylocentralitem. Akardyt II jest używany najczęściej jako stabilizator w prochach dwubazowych. W materiale miotającym typowej, konwencjonalnej amunicji znajduje się najczęściej nitroceluloza[13]. Inne substancje są wprowadzane do składu materiału miotającego w konkretnym celu, np. dinitrotolueny są używane jako modyfikatory szybkości spalania, a ftalany jako plastyfikatory. Inne związki stosowane jako stabilizatory to mocznik i difenyloamina, wyższe alkohole, kamfora, węglowodory, wazeliny. Czystymi stabilizatorami są głównie difenyloamina i akardit I. Stabilizatory wywołujące efekt żelowania to: centralit I, centralit II, centralit III, akardit II akardit III, ethylphenylurethane, methylphenylurethane i diphenylurethane.

Obecnie są prowadzone również badania nad zachowaniem się prochu podczas procesu starzenia i oceną prawdopodobnej jego trwałości na podstawie m.in. analiz difenyloaminy, metylocentalitów, etylocentralitów oraz innych stabilizatorów i ich produktów rozkładu. Mechanizm starzenia prowadzi do formowania się różnych produktów reakcji. Okazuje się, że występowanie pochodnych DPA w starzonym prochu zależy od temperatury, w której jest prowadzony ten proces[14].

[13] D. Laza i in., *Development of a quantitative LC-MS/MS method for the analysis of common propellant powder stabilizers in gunshot residua*, „Journal of Forensic Science" 2007, nr 52, s. 842.

[14] Tamże.

Zakres podłoży, z których można zebrać GSR, jest dość szeroki. Są to: skóra, pojazdy (siedzenia, drzwi, okna, sufit, kierownica itd.), miejsce zdarzenia, drzwi, okna, części ciała, odzież i inne powierzchnie, które stanowiły tarczę.

Należy podkreślić, że o ile typowe GSR obecne na przykład na rękach można zebrać maksymalnie po ośmiu godzinach (w Niemczech – do czterech – sześciu godzin), o tyle OGSR utrzymują się dłużej. Nieorganiczne GSR są przenoszone znacznie łatwiej niż organiczne GSR. Mikroślady w postaci nieorganicznych GSR mogą pochodzić z kontaminacji, natomiast OGSR mogą pomóc w odróżnianiu ich pochodzenia. James Arndt i inni podjęli badania nad „wytrwałością" organicznych pozostałości powystrzałowych na dłoniach strzelca[15]. Stwierdzono, że maksymalny czas, po jakim jest możliwe zebranie OGSR, to około 24 godziny. Nie obserwowano przy tym przenoszenia się OGSR na inne obiekty. Umycie rąk mydłem lub innymi środkami czyszczącymi powoduje całkowite pozbycie się organicznych pozostałości ze skóry dłoni.

Techniczno-analityczna strona badań GSR jest ustandaryzowana i oparta na zaakceptowanych standardach międzynarodowych. Jedynie interpretacja wyników analizy jest w mniejszym stopniu zdefiniowana (biegły interpretuje te wyniki na swój sposób, indywidualnie). Interpretacja wyników nie jest podyktowana żadnymi standardami międzynarodowymi, wpływają na nią natomiast liczne paradygmaty – m.in.: rodzaj zdarzenia, miejsce i sposób pobrania, zabezpieczenia mikrośladów, pogoda (czy padał deszcz, czy wiał wiatr), ubiór (czy osoba, która użyła broni, miała rękawiczki, czapkę) – które mają wpływ na obecność lub brak cząstek GSR na danej osobie, nie mówiąc już o ilości cząstek. Końcowe wnioski, jakie stawia biegły, w ścisły sposób zależą od niego samego.

Problematycznym aspektem badawczym jest istnienie cząstek, które są podobne pod względem struktury i składu pierwiastkowego, a nie pochodzą z broni palnej[16]. Znalezienie źródła cząstek niepochodzących z broni palnej i potwierdzenie tego mogłoby spowodować, że obecnie wykorzystywana metoda byłaby całkowicie nieprawidłowa. Takie źródła nie zostały jednak jeszcze potwierdzone. Na przykład klocki hamulcowe albo elementy sprzęgła samochodowego mogą wytwarzać cząstki o podobnym składzie pierwiastkowym, ale o innym kształcie[17]. Również resztki z zapłonnika poduszki powietrznej w samochodzie mogą być źródłem wielu różnych cząstek, które dają się odróżnić od cząstek GSR[18].

Badania na obecność pozostałości GSR i OGSR są prowadzone wieloma metodami, m.in.: testy barwne, spektroskopia Raman, spektroskopia w podczerwieni (ATR-FTIR), hybrydowa spektrometria mas sprzężona z plazmą wzbudzaną indukcyjnie

[15] J. Arndt i in., *Preliminary evolution of the persistence of organic gunshot residua*, „Forensic Science International" 2012, nr 222, s. 137.

[16] P.V. Mosher i in., *Gunshot residue-similar particles produced by fireworks*, „Canadian Society of Forensic Science" 1998, nr 31, s. 157; K.L Kosanke, R.C. Dujay, B.J. Kosanke, *Characterization of pyrotechnic reaction residue particles by SEM/EDS*, „Journal of Forensic Science" 2003, nr 48, s. 531; ciż sami, *Pyrotechnic reaction residue particles*, „Journal of Forensic Science" 2006, nr 51, s. 296; F.S. Romolo, P. Margot, *Identification of gunshot residue: a critical review*, „Forensic Science International" 2000, nr 119, s. 195.

[17] C. Torre i in., *Brake linings: a source of non-GSR particles containing lead, barium and antimony*, „Journal of Forensic Science" 2002, nr 47, s. 494; B. Cardinetti i in., *X-ray mapping technique: a preliminary study in discriminating gunshot residue particles from aggregates of environmental occupation origin*, „Forensic Science International" 2004, nr 143, s. 1; B. Burnett, *Errors in gunshot residue assessment by scanning electron microscopy elemental analysis in criminal cases: III. Friction-brake particles assigned as highly specific gunshot residue particles* [online], http://www.meixatech.com/articles.html [dostęp: 1 IX 2016].

[18] R.E. Berk, *Automated SEM/EDS analysis of airbag residue. II: Airbag residue as a source of percussion primer residue particles*, „Journal of Forensic Science" 2009, nr 54, s. 69.

(MC-ICP-MS), spektrometria fluorescencji rentgenowskiej (XRF), neutronowa analiza aktywacyjna (NAA), atomowa spektroskopia absorpcyjna (AAS), atomowa spektrometria emisyjna ze wzbudzeniem plazmowym (ICP-AES), chromatografia gazowa z analizą energii cieplnej (GC-TEA), chromatografia gazowa ze spektrometrią mas (GC-MS), wysokoprężna chromatografia cieczowa (HPLC), wysokociśnieniowa chromatografia cieczowa z detekcją elektrochemiczną (HPLC-PMDE), chromatografia cieczowa z tandemową spektrometrią mas (LC-MS/MS), wysokociśnieniowa chromatografia cieczowa z jonizacją pod ciśnieniem atmosferycznym i spektrometrią mas (HPLC-API-MS), elektroforeza kapilarna (CE), spektrometria mas sprzężona z czasem przelotu jonów wtórnych ToF-SIMS, laserowa ablacja sprzężona ze spektrometrią mas z plazmą wzbudzaną indukcyjnie (LA-ICP-MS), chromatografia cieczowa sprzężona z kwadrupolowym czasem przelotu (LC-QTOF), mikroskopia konfokalna oraz najpowszechniej stosowana metoda skaningowej mikroskopii elektronowej z mikroanalizą rentgenowską (SEM/EDS). Większość z tych metod jest w stanie potwierdzić obecność specyficznych składników (metali) w pozostałościach.

Mikroskopia elektronowa SEM w połączeniu z mikroanalizą rentgenowską jest metodą wykorzystywaną rutynowo do badań broni palnej i amunicji w wielu laboratoriach kryminalistycznych na całym świecie. Mikroskopy elektronowe do badań kryminalistycznych są wyposażone w dodatkowe oprogramowanie umożliwiające analizę cząsteczek pozostałości po wystrzale z broni palnej[19]. Ślady po wystrzale z broni palnej zazwyczaj zabezpiecza się na stoliku mikroskopowym. Pakiet do analizy GSR pozwala na automatyczną klasyfikację cząstek GSR większych od np. 0,5 μm i innych cząstek wskaźnikowych, np. duże ilości ołowiu (Pb). Wynikiem analizy GSR jest automatycznie generowany raport z badań, który zawiera liczbę znalezionych cząsteczek z uwzględnieniem zdefiniowanych klas[20].

Lis G.A. Melo i inni zaproponowali analizę pozostałości GSR metodą transmisyjnej mikroskopii elektronowej TEM ze względu na obecność sub- i mikrocząsteczek, średnicy rzędu 2–10 nm, tzn. poniżej poziomu detekcji automatycznego wyszukiwania w mikroskopie SEM[21]. Wykazano, że w amunicji firmy CBC cząsteczki te składają się głównie z tlenku ołowiu. Za pomocą metody dyfrakcji elektronów stwierdzono, że są to krystaliczne nanocząsteczki, które tworzą aglomeraty wewnątrz większych cząstek GSR. Wbrew powszechnej wiedzy o amorficznej strukturze mikrometrycznych cząstek GSR okazało się, że nanocząstki GSR wykazują bardziej krystaliczną strukturę[22]. Dzięki analizie EDX stwierdzono również obecność dużej liczby cząsteczek zawierających jedynie ołów i antymon (PbSb). Interesującym spostrzeżeniem było to, że bar nie był obecny w nanocząsteczkach GSR.

Spektroskopia Ramana jest jedną z metod alternatywnych do analizy organicznych GSR, najczęściej pozostałości pochodzących z nietoksycznej amunicji, tzn. wolnej od ołowiu[23]. Analiza metodą spektroskopii Ramana jest stosowana do identyfikacji nie-

[19] H. Krüsemann, *SEMs and forensic science*, „Problems of Forensic Sciences" 2001, nr 47, s. 110.

[20] A. Filewicz, *Kryminalistyczne badania pozostałości po wystrzale z broni palnej (GSR)*, Warszawa 2001, s. 85.

[21] L.G.A. Melo i in., *Nano characterization of gunshot residues from Brazilian ammunition*, „*Forensic Science International"* 2014, nr 240, s. 69.

[22] O. Dalby, D. Butler, J. Birkett, *Analysis of gunshot residue*…, s. 924; F.S. Romolo, P. Margot, *Identification of gunshot residue*…, s. 195; *Standard Guide for Gunshot Residue Analysis by Scanning Electron Microscopy / Energy-Dispersive Spectroscopy* ASTM E 1588-10 (norma ASTM 1588 wersja 10 – przyp. red.), s. 17.

[23] M. Lopez-Lopez i in., *Analysis of macroscopic gunshot residues by Raman spectroscopy to assess*

spalonego i częściowo spalonego prochu. Obecnie ta metoda może być uzupełnieniem i potwierdzeniem informacji uzyskanych po analizie SEM/EDS. Maria Lopez-Lopez i inni badali efekt pamięci broni, który odgrywa istotną rolę w łączeniu znalezionych GSR z wystrzeloną amunicją[24]. Wykonano około 20 strzałów z odległości około 30 cm do tarczy papierowej, używając tej samej broni i dwóch różnych typów amunicji. Analiza widmowa wykazała obecność difenyloaminy i jej pochodnych w jednym rodzaju amunicji (SB-T 93+), a w drugim (SB 96+) obecność centralitu etylowego. Pozostałości GSR w obu amunicjach były ujawnione w badaniu na obecność pasma difenyloaminy (1342 cm^{-1}) w widmie Ramana. Gdy nie strzelano amunicją typu SB 96+, to nie było pozostałości GSR, które świadczyłyby o użyciu tej amunicji. Po wykonaniu od jednego do dziesięciu strzałów okazało się, że od 1,5 do 6%. analizowanych cząstek odpowiadało amunicji typu SB 96+, co świadczyły o występowaniu efektu pamięci broni.

Podjęto również próbę analizy organicznych pozostałości powystrzałowych techniką spektroskopii w podczerwieni (FTIR)[25]. Metoda jest nieniszcząca i szybka. Początkowe badania pozostałości powystrzałowych za pomocą FTIR były związane z analizą jakościową składu chemicznego oraz określeniem odległości strzału. Justin Bueno i inni[26] wykorzystali do badań spektrometrię osłabionego całkowitego odbicia w podczerwieni (ATR – FTIR). Widma w poczerwieni analizowano w zakresie 1800–600 cm^{-1} dla pojedynczych cząstek pozostałości GSR. W trybie ATR rozdzielczość spektralna wynosiła 4 cm^{-1}. Analiza wykazała obecność pasm rozciągających asymetrycznych i symetrycznych NO_2 oraz pasma rozciągającego NO w 1629 cm^{-1}, 1270 cm^{-1} i 816 cm^{-1}. Te pasma są charakterystyczne dla nitrocelulozy. Na podstawie różnicy pomiędzy uzyskanymi widmami z pozostałości GSR próbowano określić kaliber użytej amunicji. Jednak różnorodność składu pozostałości pozwala jedynie na spekulacje związane z przyporządkowaniem cech charakterystycznych cząstek GSR do kalibru amunicji.

Alternatywnymi i uzupełniającymi technikami badań organicznych GSR są metody chromatograficzne[27].

Désiré Laza i inni zastosowali metodę chromatografii cieczowej sprzężonej z tandemem spektrometrii mas (LC-MS/MS) do analizy organicznych składników z pozostałości materiału miotającego[28]. Metoda pozwala na analizę stabilizatorów zawartych w mieszaninie materiału miotającego (akardyt II, etylcentralit, difenyloamina, metylocentralit,

the weapon memory effect, „Forensic Science International" 2013, nr 231, s. 1; J. Bueno, V. Sikirzhytski, I.K. Lednev, *Raman spectroscopic analysis of gunshot residua offering great potential for caliber differentiation*, „Analytical Chemistry" 2012, nr 84, s. 4334; M. Lopez-Lopez, J.J. Delgado, C. Garcia-Ruiz, *Ammunition identification by means of the organic analysis of gunshot residues using Raman spectroscopy*, „Analytical Chemistry", 2012, nr 84, s. 3581.

[24] M. Lopez-Lopez i in., *Analysis of macroscopic gunshot residues by Raman spectroscopy*…, s. 1.

[25] J. Bueno, V. Sikirzhytski, I. K. Lednev, *Attenuated total reflectance FT-IR Spectroscopy for gunshot residue analysis: potential for ammunition determination*, „Analytical Chemistry" 2013, nr 85, s. 7287; ciż sami, J. Bueno, I. K. Lednev, *Attenuated total reflectance FT-IR imaging for rapid and automated detection of gunshot residue*, „Analytical Chemistry" 2014, nr 86, s. 3389.

[26] J. Bueno i in., *Attenuated total reflectance FT-IR Spectroscopy for gunshot residue analysis*…, s. 7287.

[27] O. Dalby, D. Butler, J. Birkett, *Analysis of gunshot residue*…, s. 924; D. Laza i in., *Development of a quantitative LC-MS/MS method*…, s. 842; S. Benito i in., *Characterization of organic gunshot residues in lead-free ammunition using a new sample collection device for liquid chromatography-quadrupole time-of-flight mass spectrometry*, „Forensic Science International" 2015, nr 246, s. 79; R.V. Taudte i in., *Detection of gunshot residues using mass spectrometry*, „BioMed Research International" 2014, s. 1; J. Wade Moran i in., *Skin permeation of organic gunshot residua: implications for sampling and analysis*, „Analytical Chemistry" 2014, nr 86, s. 6071.

[28] D. Laza i in., *Development of a quantitative LC-MS/MS method*…, s. 842.

N-nitrosodifenyloamina, 2-nitrodifenyloamina i 4-nitrodifenyloamina). Analizowano pozostałości powystrzałowe zebrane z dłoni strzelca za pomocą jednorazowych wymazówek. Do badań wykorzystano amunicję typu *lead free*, tzn. niezawierającą ołowiu, oraz amunicję typu *without heavy metals*, tzn. niezawierającą ciężkich metali. Wyniki wykazały, że w materiale miotającym zwykle używa się etylcentrality oraz difenyloaminę jako stabilizatorów. Difenyloamina została wykryta wraz z pochodnymi azotanowymi. Autorzy twierdzą, że metoda LC-MS/MS może być stosowana rutynowo w wykrywaniu pozostałości powystrzałowych. Badania wymagają uzupełnienia w postaci analizy pozostałości na osobach, które nie użyły broni, ale były w pobliżu miejsca zdarzenia.

Sandra Benito i inni w celu scharakteryzowania organicznych pozostałości powystrzałowych w amunicji typu *lead free* zastosowali metodę chromatografii cieczowej z kwadrupolowym detektorem mas sprzężonym z analizatorem czasu przelotu (LC-Q-TOF)[29]. Zidentyfikowano 18 składników prochu w pozostałościach powystrzałowych. Były nimi: dodatki w postaci plastyfikatora ftalanu dietylu (DEP), stabilizatorów, takich jak centrality EC i MC oraz produkty rozkładu difenyloaminy (DPA). Ftalan dietylu nie jest charakterystycznym związkiem dla pozostałości powystrzałowych, gdyż może on pochodzić z elementów plastikowych, kosmetyków, pestycydów. Ujawnienie produktów rozpadu DPA i centraliów w pozostałościach powystrzałowych daje większe prawdopodobieństwo, że te związki pochodzą właśnie z wystrzelonej amunicji. Centrality są stosowane wyłącznie do prochów, ich używanie jest ograniczone jedynie do amunicji. Wobec powyższego ujawnienie wymienionych składników i ich pochodnych pozwala na identyfikacje GSR, szczególnie gdy została użyta amunicja typu *lead free* czy *non-toxic*. Wiadomo również że taka amunicja generuje pozostałości nieorganiczne, które nie są typowe w rutynowych badaniach GSR. Według autorów zastosowana przez nich technika, ze względu na szeroki zakres możliwości analitycznych, a także na jej szybkość i precyzyjność, jest istotnym atrybutem w analizie organicznych GSR w stosunku do innych publikowanych metod. LC-QTOF daje możliwość dokładnego pomiaru masy fragmentów jonów. Pozwala jednocześnie na pracę w trybie tandemu MS/MS.

Skuteczność metody, a zwłaszcza zastosowanie tandemu MS/MS, zostało potwierdzone również w publikacji R.V. Taudte i in.[30] Czułą techniką pod względem wykrywalności związków chemicznych jest detektor mas z potrójnym kwadrupolem, która pozwala na analizę małych ilości materiału w zakresie nano- i pikogramów. Optymalne wyniki badań można również uzyskać przy wykorzystaniu technik jonizacji: EI (elektronowa – przyp. red.), ESI (elektrorozpylanie – przyp. red.) czy APCI (chemiczna pod ciśnieniem atmosferycznym – przyp. red.), które pozwalają na identyfikację składników organicznych GSR.

Techniki chromatograficzne mają przede wszystkim na celu ujawnianie materiału miotającego, z uwzględnieniem zmiany ich formuły podczas produkowania amunicji. Pozwalają na pracę z niewielką koncentracją OGSR. Obecnie są prowadzone badania nad przenikalnością skóry, przenoszeniem, procesem starzenia, koncentracją w skórze i na innych podłożach, a także oddziaływaniem na pozostałości GSR pochodzące ze spłonki.

Badania z wykorzystaniem szybkich kamer mogą dostarczyć dodatkowych informacji związanych z dynamicznym efektem obserwowanym podczas wystrzału. Dzięki nim można zaobserwować zróżnicowanie formowania się kształtu chmury dymu

[29] S. Benito i in., *Characterization of organic gunshot residues in lead-free ammunition*..., s. 79.
[30] R.V. Taudte i in., *Detection of gunshot residues using*…, s. 1.

w zależności od rodzaju broni palnej, a tym samym na zróżnicowanie rozkładu cząstek GSR. Ma to istotny wpływ w formułowaniu i interpretacji wyników analizy badań GSR i nie zawsze jest w pełni uwzględniane w raportach kryminalistycznych. Hans Ditrich w swojej publikacji przestawił wyniki badań z obserwacji powstawania chmury dymu i efektów z tym związanych po oddaniu strzału z różnych typów broni (pistolety, rewolwery, strzelby)[31]. Testowe strzały z wyżej wymienionych typów broni zostały sfilmowane za pomocą wysoko wyspecjalizowanego aparatu cyfrowego z prędkością 3000, 6000, 10 000 klatek na sekundę. Uzyskane zdjęcia zostały przeanalizowane z wykorzystaniem standardowego oprogramowania graficznego ImageJ. Okazało się, że formowanie mgiełki po wystrzale, a tym samym rozkład cząsteczek dymu, zależy od specjalnej konstrukcji broni. We wszystkich badanych pistoletach pierwszy strumień gazu i cząsteczek jest emitowany z lufy i tworzy najpierw stożek, który zostaje w pewnym momencie zaburzony i w obwodzie tworzy się wir. Kąt stożka zależy od długości lufy, kalibru i prędkości strumienia oraz typu amunicji. Następnie wir tworzy pierścień, który przekształca się w kulista chmurę dymu i cząstek, w wyniku wewnętrznych turbulencji. W tym czasie mniejszy strumień gazu i spalonych cząstek przenika chmurę wraz z pociskiem. Większość cząstek emitowanych z lufy jest skierowanych od strzelca. Tylko niewielka część osiądzie na rękach strzelca, co zależy od kombinacji broni i amunicji. Również inne możliwe źródła pozostałości po wystrzale zdecydowanie różnią się od budowy broni. Takimi źródłami są głównie mechanizm wyrzucania łuski z pistoletu, wycięcie na spuście lub szczelina między bębnem a lufą w rewolwerze.

Bez względu na to, jakie metody są stosowane do analizy GSR, możliwe są cztery rodzaje wyników:

1) cząstki GSR są obecne w próbce i są wykrywalne podczas analizy,
2) brakuje cząstek GSR i tym samym nie zostaną wykryte żadne cząstki.

Mimo że powyższe warunki są dość jednoznaczne, nie ma konkretnych wymagań co do prawidłowego wnioskowania wyniku (SWGGSR 2011). Pozostałe dwie możliwości są problematyczne:

3) cząstki GSR są nieobecne, ale wyniki analizy wskazują na ich obecność (wynik fałszywy, pozytywny),
4) cząstki GSR są obecne, ale podczas analizy ich nie wykryto (wynik fałszywy, negatywny).

Wysiłek ośrodków badawczych jest ukierunkowany na zapewnienie wysokiego poziomu precyzji w wykrywaniu cząsteczek GSR. Systematycznie ulepsza się sprzęt analityczny, stale udoskonala badania porównawcze. Stosuje się również środki przeciw zanieczyszczaniu próbek, kontaminacji, obsłudze niewłaściwych urządzeń lub błędnej interpretacji danej cząstki. Procedury pobierania próbek oraz procedury kalibracji urządzeń są skomplikowane, co wymaga zatrudniania odpowiedniego personelu i jego szkolenie. Sporadyczne niejasności powodują żywe dyskusje na temat pochodzenia wykrytych cząstek, czy pochodzą one z klocków hamulcowych, czy z materiałów pirotechnicznych itp. Niestety, wielokrotnie stwierdzono, że obecnie podejmuje się mniej wysiłku, aby wyniki analizy poddać krytycznej ocenie.

W artykule przedstawiono rezultaty pilotażowych badań metodą skaningowej mikroskopii elektronowej sprzężonej z mikroanalizą rentgenowską oraz spektroskopii Ramana składu chemicznego i cech morfologicznych cząstek rozproszonych na baweł-

[31] H. Ditrich, *Distribution of gunshot residua – the influence of weapon type*, „Forensic Science International" 2012, nr 220, s. 85

nianej tkaninie po użyciu broni palnej. Celem badań jest opracowanie metodyki analizy chemicznej cząstek powystrzałowych pochodzących z amunicji zawierającej ołów oraz amunicji bezołowiowej, a także opracowanie procedur badawczych ujawniania pozostałości po użyciu z broni palnej i w przyszłości wdrożenie do rutynowej praktyki opiniodawczej w Biurze Badań Kryminalistycznych ABW, w tym typowanie rodzaju materiałów dowodowych i materiału porównawczego. Wskazane jest także opracowanie własnych kryteriów interpretacji wyników badań pozostałości powystrzałowych w celu powiązania osoby podejrzanej z użyciem broni palnej.

Metody badawcze

Skaningowa mikroskopia elektronowa (SEM)

Istotą mikroskopii skaningowej SEM jest skanowanie powierzchni próbki nanometrową wiązką elektronów uformowaną przez układ elektronooptyczny mikroskopu. Taką wiązkę formuje układ magnetycznych soczewek elektronowych. Próbki są skanowane wiązką elektronów odchyloną przez cewki. Odchylenie wiązki tworzącej obraz na monitorze jest zsynchronizowane z odchyleniem wiązki skanującej próbkę. Sygnał z powierzchni próbki (najczęściej elektrony wtórne lub odbite) dociera do detektora. Sygnał wychodzący z detektora steruje jasnością obrazu wyświetlanego na monitorze. Powiększenie mikroskopu skaningowego wynika z relacji wielkości obszarów skanowanych na próbce i na monitorze.

Mikroanaliza rentgenowska (EDS)

Metoda mikroanalizy rentgenowskiej polega na wzbudzaniu charakterystycznego promieniowania rentgenowskiego przez silnie zogniskowaną wiązkę elektronów, o średnicy zazwyczaj rzędu 1 μm. Mikroanalizator rentgenowski, zwany też mikrosondą elektronową, służy do analizowania promieniowania charakterystycznego, co pozwala na określenie składu chemicznego w danym mikroobszarze. Do detekcji promieniowania w mikroanalizie rentgenowskiej zastosowano spektrometr mierzący energię promieniowania rentgenowskiego (ang. Energy Dispersive Spektrometry, EDS). Analiza składu chemicznego EDS pozwala wykrywać pierwiastki przy zawartości około 0,1% wagowych oraz uzyskiwać wyniki ilościowe przy zastosowaniu odpowiedniej kalibracji. Każde zarejestrowane widmo odzwierciedla dwa podstawowe typy promieniowania rentgenowskiego, tj. promieniowanie charakterystyczne i promieniowanie tła. W analizie ilościowej promieniowanie tła jest odejmowane od widma. Widmo jest wyskalowane na osi odciętych w keV, a na osi rzędnych w liczbie impulsów lub liczbie impulsów na sekundę. Linie spektralne są widoczne jako piki przewyższające tło. Mikroanaliza jakościowa polega na uzyskaniu czytelnego spektrum promieniowania rentgenowskiego z wybranego fragmentu próbki. W analizie ilościowej stężenie pierwiastków oblicza się na podstawie proporcjonalnej zależności natężenia charakterystycznego promieniowania rentgenowskiego od zawartości pierwiastków w analizowanej objętości. Przeliczenie intensywności pików na zawartość procentową pierwiastków, dokonywane przez oprogramowanie mikroanalizatora, należy jednak traktować jedynie jako szacunkową ocenę, jeśli nie przeprowadza się dokładnej kalibracji za pomocą odpowiednich wzorców.

W stosowanej bezwzorcowej analizie ilościowej wykorzystuje się korekcję macierzową ZAF i normalizację do 100% stężenia pierwiastków zidentyfikowanych. W praktyce obserwuje się duży rozrzut wyników mikroanalizy[32].

Spektroskopia ramanowska

Metody spektroskopowe można podzielić ogólnie na emisyjne i absorpcyjne. Metody emisyjne to takie, w których o budowie i składzie próbki wnioskuje się na podstawie analizy promieniowania emitowanego przez substancję badaną. W praktyce jednak częściej stosuje się metody absorpcyjne, które polegają na analizie promieniowania pochłanianego z przepuszczanej przez próbkę wiązki promieniowania elektromagnetycznego. Przewaga metod absorpcyjnych bierze się stąd, że odpowiednio wysokie natężenie promieniowania emitowanego występuje dopiero w podwyższonej temperaturze, ale podgrzewanie polimerów może skończyć się destrukcją związku chemicznego. Metodą pośrednią między spektroskopią emisyjną i absorpcyjną jest spektroskopia rozpraszania, zwłaszcza spektroskopia „ramanowska" badająca rozpraszanie monochromatycznej wiązki przez badaną substancję[33].

Spektroskopia absorpcyjna w podczerwieni (IR) razem ze spektroskopią Ramana dają informację o widmie oscylacyjno-rotacyjnym cząsteczki w podstawowym stanie elektronowym. Są to metody uzupełniające się. Decydujący wpływ na postać widm ciał stałych i cieczy mają wzbudzenia oscylacyjne, których energia jest o 1–2 rzędy większa od energii wzbudzeń rotacyjnych. Rotacje molekuł ciał stałych i cieczy są hamowane wskutek oddziaływań międzycząsteczkowych, a wzbudzenia rotacyjne powodują jedynie zwiększenie szerokości pasm absorpcyjnych. Z tego powodu widma ciał stałych i cieczy noszą nazwę **widm oscylacyjnych**. W fazie gazowej molekuły rotują stosunkowo swobodnie, dzięki czemu w widmie gazu można zaobserwować oddzielne przejścia oscylacyjno-rotacyjne, a odpowiednie widma noszą nazwę **widm oscylacyjno-rotacyjnych**. Liczba rodzajów drgań, ich częstość i amplituda ściśle charakteryzują cząsteczkę. Jeżeli drganie cząsteczki powoduje zmianę jej elektrycznego momentu dipolowego, to drganie jest aktywne w widmie IR. Jeżeli drganie cząsteczki powoduje zmianę jej polaryzowalności, jest ono aktywne w widmie Ramana. W przypadku występowania w cząsteczce środka symetrii, drganie aktywne w widmie IR jest nieaktywne w widmie Ramana, i odwrotnie (tzw. zakaz alternatywny). W cząsteczkach, które nie mają środka symetrii, występują drgania ujawniające się w obu widmach. Bardzo często widma IR i ramanowskie różnią się natężeniem pasm odpowiadających poszczególnym drganiom, np. grupy funkcyjne silnie polarne są lepiej widoczne w widmie IR, podczas gdy wiązania podwójne i potrójne oraz drgania szkieletu węglowego cząsteczki są lepiej widoczne w widmie Ramana. Drgania w pełni symetryczne są zazwyczaj lepiej widoczne w widmie Ramana[34].

Spektroskopia ramanowska bada zmiany częstotliwości światła rozproszonego przez molekuły. Jeśli częstość padającego światła jest υ_0, a częstość światła rozproszonego jest υ_r, to wtedy przesunięcie częstości $\upsilon_r - \upsilon_0 = \Delta\upsilon$ stanowi częstość Ramana. Zbiór częstości Ramana tworzy widmo Ramana. Przesunięcie częstości $\Delta\upsilon$ jest równoważne zmianie energii $\Delta\upsilon \times h$. Zamiast częstości υ podawana jest zwykle odpowiadająca jej liczba falowa[35].

[32] A. Szummer, *Podstawy ilościowej mikroanalizy rentgenowskiej*, Warszawa 1994, s. 244.
[33] J. Sadlej, *Spektroskopia molekularna*, Warszawa 2002, s. 132.
[34] H. Barańska, A. Łabudziński, J. Terpiński, *Laserowa spektroskopia ramanowska*, Warszawa 1981, s. 5.
[35] H.A. Szymański, *Raman spectroscopy*, New York 1967, s. 198.

Spektroskopia ramanowska umożliwia określenie składu chemicznego, formy krystalicznej, stopnia uporządkowania, rozkładu przestrzennego naprężeń oraz oddziaływań międzycząsteczkowych w badanym materiale.

Widma absorpcyjne w podczerwieni i widma Ramana mogą być wykorzystywane do identyfikowania nieznanych substancji, wykrywania w cząsteczce określonych grup atomów lub rodzajów wiązań chemicznych, ustalania struktury geometrycznej cząsteczek oraz do analizy drgań cząsteczki. Natężenie pasm w widmie podczerwieni oraz Ramana można przewidywać na podstawie reguł empirycznych. Istnieje jednak wiele wyjątków, np. grupie C≡N odpowiada bardzo intensywne pasmo w widmie Ramana, a niekiedy bardzo słabe w widmie podczerwieni. Pasma odpowiadające drganiom rozciągającym wiązania C–H grup alifatycznych są intensywne w widmie Ramana, natomiast mało intensywne w widmie podczerwieni. Natężenie tych pasm jest proporcjonalne do liczby wiązań C–H w danej cząsteczce. Z kolei pasma odpowiadające drganiom zginającym wiązania C–H mają średnie natężenie w widmie podczerwieni, są natomiast słabe w widmie Ramana[36].

Część eksperymentalna

Przygotowanie materiału do badań obejmowało wybór amunicji, broni oraz pobranie reprezentatywnej próbki mikrośladów i ich skoncentrowania na niewielkiej powierzchni próbnika przez wielokrotne przyłożenie stolika mikroskopowego pokrytego materiałem przylepnym do interesującej powierzchni fragmentu odzieży stanowiącej tarczę. Następnie porównano uzyskane wyniki ze składem materiału spłonkowego wyjętego z łusek oraz składem drobin zebranych z denka odzyskanych pocisków. Kolejnym etapem badań było określenie składu chemicznego organicznych pozostałości przez zeskrobanie drobin z okolic miejsca wlotowego pocisku.

Do badań wykorzystano dwa rodzaje amunicji: S&B 9×19 mm Luger oraz G.F.L. 9×19 mm Fiocchi. Strzały oddano z pistoletów GLOCK oraz Walter. Każda z wybranej broni była używana do jednego rodzaju amunicji w celu zminimalizowania kontaminacji. Strzały oddano do specjalnie przygotowanych tarcz z tektury obłożonej bawełnianym materiałem. Odległości strzałów wyznaczono dla każdego rodzaju broni na 10, 20, 30, 50 oraz 100 cm. Dla amunicji G.F.L. 9×19 mm Fiocchi wykonano dodatkowo strzały z odległości 5 cm i 70 cm. Próbki do badań pobrano ze spłonki łusek po oddaniu strzału oraz z denka odzyskanych pocisków. Stanowiły one materiał porównawczy. Następnie za pomocą specjalnych podstawek mikroskopowych z przyklejoną dwustronną węglową folią adhezyjną zabezpieczono mikroślady z obszarów wszystkich przestrzelin w odległości około 5 cm od miejsca otworu wlotowego pocisku.

Badania fizykochemiczne zgromadzonych próbek przeprowadzono przy użyciu skaningowego mikroskopu elektronowego (SEM) sprzężonego z mikroanalizatorem rentgenowskim (EDS), dodatkowo wyposażonego w specjalne oprogramowanie do badań pozostałości po wystrzale (GSR) – Inka (wersja 5 zgodna z normą ASTM E 1588 wersja 10).

Proces pomiarowy polegał na obserwowaniu obrazu z wykorzystaniem detekcji elektronów wstecznie rozproszonych, w celu ustalenia położenia cząstek o interesującej średniej wartości liczby atomowej, zebrania widma rentgenowskiego i obserwowania

[36] H. Barańska, A. Łabudziński, J. Terpiński, *Laserowa spektroskopia*…, s. 12.

obrazu dla każdej indywidualnej cząstki. Lokalizację interesujących cząstek o kulistym kształcie i wielkości większej od 1,0 μm oraz zebranie widm rentgenowskich przeprowadzono za pomocą oprogramowania do automatycznego „przeszukiwania" powierzchni stolika z naniesionymi mikrośladami. Program ten wyszukuje cząstki o określonych cechach i analizuje kolejno prostokątne obszary, na które została podzielona powierzchnia stolika mikroskopowego. Liczba i wielkość pól jest zależna od ustalonego powiększenia. Program wymaga zdefiniowania przez operatora następujących parametrów pomiaru: położenia stolika z materiałem dowodowym oraz standardu kobalt–złoto (służącego do określenia zakresu sygnału rejestrowanego przez detektor BSE w mikroskopie elektronowym), ustalenia zbioru spodziewanych klas chemicznych cząstek, wyznaczenia górnej i dolnej granicy rozmiarów cząstek oraz maksymalnej ich liczby w analizowanym polu. Po wykonaniu automatycznego „przeszukiwania" przeprowadzono manualne potwierdzenie klasy chemicznej ustalonej dla każdej z cząstek na podstawie otrzymanego widma rentgenowskiego oraz dokonano obserwacji zapisanego obrazu cząstki w celu zbadania jej morfologii.

Przed badaniami SEM/EDS próbki umieszczano w komorze próżniowej mikroskopu elektronowego na stoliku goniometrycznym. Jednorazowo na stoliku umieszczano maksymalnie do sześciu aluminiowych podstawek z przyklejonymi próbkami pozostałości powystrzałowych. Oddzielnie wykonywano badania pozostałości zebranych z amunicji bezołowiowej i oddzielnie pozostałości zebranych z amunicji ołowiowej. Osobno też wykonano badania materiału porównawczego w postaci pozostałości zebranych ze spłonki łusek i pocisków.

Badania (SEM/EDS) zostały wykonane z zachowaniem następujących stałych warunków pracy:

- próżni,
- napięcia przyspieszającego wiązkę elektronów w SEM – 20 kV,
- odległości roboczej – 15 mm,
- detektora mikroskopu elektronowego – BSE (detektor elektronów odbitych),
- detektora sondy elektronowej – typu SDD o powierzchni okienka 50 mm^2,
- minimalnej wielkości poszukiwanej cząstki – 1,0 μm,

Badania organicznych składników pozostałości powystrzałowych przeprowadzono metodą spektroskopii Ramana. Materiał do badań wymagał odpowiedniego przygotowania. Drobiny pozostałości powystrzałowych (resztki niespalonego prochu) widoczne gołym okiem zeskrobano z powierzchni tarcz na specjalne płytki aluminiowe. Ze względu na ograniczenia czasowe i przeprowadzenie badań poza BBK ABW analizę wykonano tylko dla jednej wybranej odległości strzału. Próbki pobrano z materiału tarcz ustawionych w odległości 20 cm od strzelca.

W analizie zastosowano pobudzenie niskoenergetyczną linią 532 nm oraz 785 nm lasera czerwonego. Zaopatrzony w filtry polaryzacyjne spektrometr umożliwia pomiar stopnia depolaryzacji pasm, co znacznie ułatwia identyfikację drgań charakterystycznych. Spektrometr jest sprzężony z układem mikroskopowym, który pozwala na zbieranie widm ramanowskich z objętości próbki około 1 $μm^3$. Cenną modyfikacją spektroskopii ramanowskiej jest spektrometria mikroramanowska. Spektrometria mikroramanowska to połączenie spektrometrii Ramana i mikroskopii optycznej. Na ekranie monitora jest widoczny obraz mikroskopowy (przy odpowiednim powiększeniu) badanej powierzchni preparatu. Typowe urządzenie do przesuwania preparatu pod mikroskopem pozwala wybrać odpowiednie miejsce do analizy za pomocą spektrometrii ramanowskiej. Dzię-

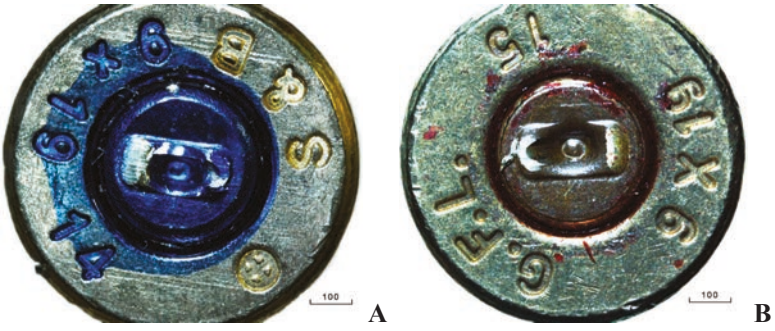
ki sprzężeniu spektrometru ramanowskiego z mikroskopem wyposażonym w przesuw skanujący jest możliwe zebranie widm z kilku punktów powierzchni górnej lub dolnej próbki i sporządzenie map na podstawie wielkości wybranej do porównywania widm.

Procedura wyznaczania intensywności pasm jest bardzo ważnym elementem prawidłowego stworzenia obrazu mikroramanowskiego. W tym celu zaznaczono obszar składający się z kilkunastu punktów położonych w linii prostej, z których były zbierane widma. Wyznaczone wartości stosunku intensywności pasm są przedstawione w postaci mapki składającej się z kolorowych kwadracików. Skala w postaci tęczy barw przyporządkowuje kolory wartościom mapowanej wielkości, podając jednocześnie zakres jej zmienności wyznaczanej w badanym obszarze. Jest to obrazowa postać funkcji określonej w punktach pomiaru, która za pomocą programu OMNIC For Nicolet Almega (Thermo Electron Corporation 2004) wykorzystującego odpowiedni wielomian może być aproksymowana[37] funkcją określoną we wszystkich punktach obszaru, przedstawioną w postaci gładkiego rozkładu barw na mapie. Spektroskopia mikro-Ramana jest uważana za metodę nieniszczącą substancję podczas jej badania, która pozwala na uzyskanie informacji o składzie chemicznym próbki w mikroskali.

Wyniki i dyskusja

Badania SEM/EDS

Badaniom z wykorzystaniem metody SEM/EDS zostały poddane mikrodrobiny pozostałości po wystrzale z broni palnej. W celu określenia wydajności oraz przydatności materiału porównawczego przeprowadzono na wstępie oględziny łusek oraz pocisków po oddaniu strzałów (zdj. 1).



A B

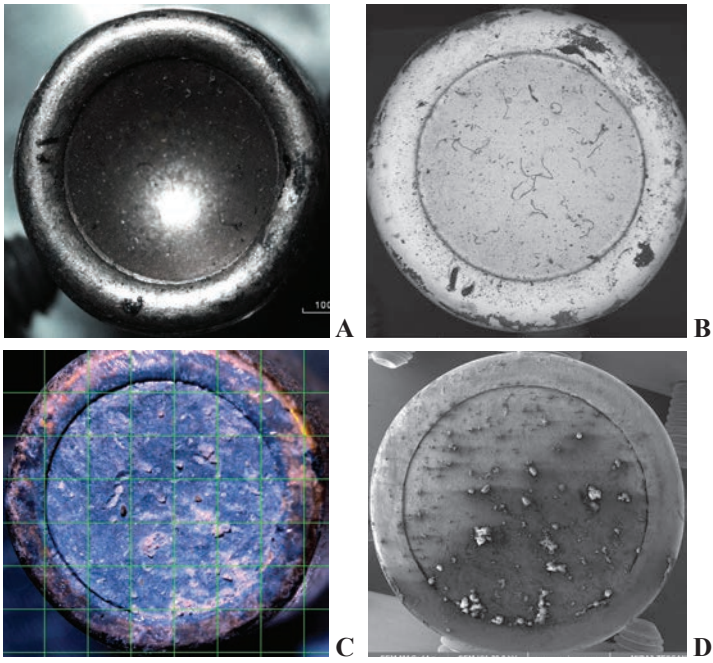
Zdj. 1. Denko łusek z amunicji S&B 9×19 mm Luger (A) oraz G.F.L. 9×19 mm Fiocchi (B) wykonane za pomocą stereomikroskopu[38].

Próbki mikrodrobin pozostałości GSR zostały pobrane za pomocą drewnianych wykałaczek z wnętrza łusek, ze spłonki. Następnie mikrodrobiny przyklejono do powierzchni okrągłych aluminiowych podstawek mikroskopowych za pomocą przewodzących węglowych adhezyjnych folii. Badano morfologię mikrodrobin z danej spłonki.

[37] Aproksymacja – proces określania rozwiązań przybliżonych na podstawie rozwiązań znanych, które są bliskie rozwiązaniom dokładnym w ściśle sprecyzowanym sensie (przyp. red.).

[38] Wszystkie materiały ilustracyjne i tabele zostały opracowane przez autorkę tekstu.

Scharakteryzowano klasy pod względem składu pierwiastkowego i liczby zidentyfikowanych cząstek w danej klasie. W przypadku pocisków wykonano próby pomiarów SEM/EDS bezpośrednio z powierzchni denka odzyskanych pocisków (zdj. 2). Pociski wkładano w specjalny aluminiowy uchwyt stosowany do badań materiałów o większych gabarytach. Na stoliku goniometrycznym, we wnętrzu mikroskopu elektronowego, pocisk w pozycji pionowej był utrzymywany za pomocą nakrętek wychodzących z nagwintowanych otworów aluminiowego uchwytu. Ta metoda pozwala jedynie na analizę płaskich równych powierzchni. Dlatego wykonanie pomiarów bezpośrednio z powierzchni denka za pomocą automatycznego „przeszukiwania" było możliwe jedynie dla pocisku pochodzącego z amunicji S&B 9×19 mm Luger. W przypadku denka pocisku pochodzącego z amunicji G.F.L. 9×19 mm Fiocchi nie było możliwe wykonanie bezpośredniej analizy ze względu na jego kształt. Denko pocisku było zaokrąglone, co jest widoczne na zdj. 2 A jako zagłębienie.



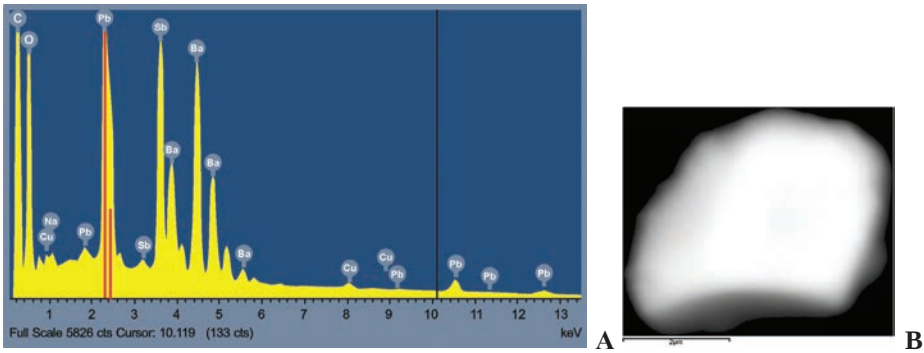
Zdj. 2. Powierzchnie denek pocisków wykonane za pomocą stereomikroskopu: G.F.L. 9×19 mm Fiocchi (A) i S&B 9×19 mm Luger (C) oraz mikroskopu SEM: G.F.L. 9×19 mm Fiocchi (B) i S&B 9×19 mm Luger (D).

W celu pozyskania materiału do badań pobrano mikrodrobiny z powierzchni denka pocisku za pomocą drewnianej wykałaczki. Podobnie jak dla pozostałości GSR pozyskanych z łusek zbadano morfologię mikrodrobin z denka pocisków, scharakteryzowano klasy pod względem składu pierwiastkowego i liczbę zidentyfikowanych cząstek w danej klasie. Wyniki uzyskane z automatycznego „przeszukiwania" oraz po manualnej korekcji wykonanej na podstawie oceny morfologii mikrodrobin zebranych z obu typów amunicji zestawiono w tabeli 1.

Tab. 1. Mikrodrobiny zebrane ze spłonki i z denka pocisku amunicji S&B 9×19 mm Luger i G.F.L. 9×19 mm Fiocchi.

Klasy	**Rodzaj klasy**	**Liczba cząstek charakterystycznych, zgodnych i środowiskowych w mikrodrobinach pobranych ze spłonki łuski**		**Liczba cząstek charakterystycznych, zgodnych i środowiskowych w mikrodrobinach pobranych z denka pocisku**	
		9×19 mm S&B	**9×19 mm G.F.L.**	**9×19 mm S&B**	**9×19 mm G.F.L.**
Pb Sn Sb Ba	charakterystyczne	0	0	0	0
Pb Sb Ba	**charakterystyczne**	**1967**	**0**	**81**	**0**
Ba Ca Si	zgodne Pb Sb Ba	8	0	4	0
Sb Ba	zgodne Pb Sb Ba	6635	0	1	0
Pb Sb	zgodne Pb Sb Ba	159	0	379	0
Ba Al	zgodne Pb Sb Ba	2	0	3	0
Pb Ba	zgodne Pb Sb Ba	6	0	347	0
Pb	zgodne Pb Sb Ba	145	0	30147	0
Sb	zgodne Pb Sb Ba	0	0	0	0
Ba	zgodne Pb Sb Ba	1	0	0	0
Pb Ca	zgodne Pb Sb Ba	7	0	505	0
Pb Cl	zgodne Pb Sb Ba	21	0	0	0
S Sb	zgodne Pb Sb Ba	0	0	0	0
Pb Sn Sb	zgodne Pb Sb Ba	0	0	0	0
Zr O	**lead-free/ non-toxic** (bezołowiowe/ nietoksyczne)	**0**	**725**	**0**	**0**
K Si Al	środowiskowe	0	1020	0	4
Cu Zn	środowiskowe	80	12	1066	558
Fe	środowiskowe	77	14	22	4
Cu	środowiskowe	78	32	115	58887
Zn	środowiskowe	5	1	0	0
Ba SO_4	środowiskowe	717	0	52	5
Pb Sn	środowiskowe	0	0	0	0
K Cl	środowiskowe	8	6	0	1
Ti	środowiskowe	4	0	1	0
Si	środowiskowe	55	40	2780	0
AlSi	środowiskowe	29	1	0	0

W mikrodrobinach zebranych z wnętrza łuski pochodzącej z amunicji S&B 9×19 mm Luger stwierdzono obecność takich cząsteczek, których skład pierwiastkowy oraz kształt świadczyły o tym, że są to charakterystyczne i zgodne cząsteczki pozostałości po wystrzale z broni palnej, o następujących składach pierwiastkowych: PbSbBa, SbBa, PbSb, BaAl, PbBa, Pb, PbCa, PbCl (zdj. 3 i tab. 2) Jest to amunicja typu SINTOX.



Zdj. 3. Widmo EDS składu pierwiastkowego pojedynczej mikrodrobiny GSR wydłubanej ze spłonki amunicji S&B 9×19 mm Luger (A), zdjęcie SEM cząsteczki charakterystycznej pozostałości GSR na powierzchni stolika mikroskopowego (B).

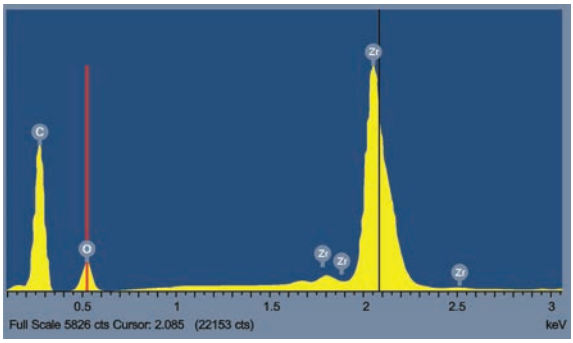
Tab. 2. Pierwiastki wchodzące w skład pojedynczej mikrodrobiny GSR wraz z zawartością (procent wag.) poszczególnych pierwiastków.

Pierwiastek	Procent wagowy	Błąd pomiaru
Ba	22,44 22,44	0,21
Sb	25,02	0,18
Pb	16,71	0,26
O	15,40	0,20
S	7,55	0,09
Cu	0,97	0,09

Mikrodrobiny spłonkowe o średnicach od kilku do kilkunastu mikrometrów miały w większości nieregularne kształty. Drobiny pobrano z wnętrza łuski. Charakteryzują się one nieco odmiennym kształtem i wielkościami w stosunku do cząsteczek, które zostały wyrzucone po oddaniu strzału. Obserwuje się znacznie mniejszą liczbę cząsteczek o regularnych i kulistych kształtach.

Podobny wynik został uzyskany po analizie powierzchni denka odzyskanego pocisku po wystrzeleniu amunicji S&B 9×19 mm Luger. Na podstawie zebranych danych (tab. 1) widać, że liczba pozyskanych cząstek charakterystycznych z łuski jest znacznie większa niż w materiale denka pocisku.

W mikrodrobinach pobranych z wnętrza łuski pochodzącej z amunicji G.F.L. 9×19 mm Fiocchi nie stwierdzono obecności charakterystycznych i zgodnych cząstek typowych dla pozostałości powystrzałowych. Zidentyfikowano natomiast liczne mikrodrobiny o średnicy kilku mikrometrów zawierające tlenek cyrkonu oraz liczne drobiny zawierające glin (Al), krzem (Si) oraz potas (K) (zdj. 4 i tab. 3).



A

B

Zdj. 4. Widmo EDS składu pierwiastkowego pojedynczej mikrodrobiny GSR wydłubanej ze spłonki amunicji G.F.L. 9×19 mm Fiocchi (A), zdjęcie SEM cząsteczki charakterystycznej pozostałości GSR na powierzchni stolika mikroskopowego (B).

Tab. 3. Pierwiastki wchodzące w skład pojedynczej mikrodrobiny GSR wraz z zawartością (procent wag.) poszczególnych pierwiastków.

Pierwiastek	Procent wagowy	Błąd pomiaru
Zr	69,07	0,35
O	24,74	0,27
Si	0,34	0,06
Na	0,28	0,04

Analiza powierzchni denka odzyskanego pocisku z amunicji G.F.L. 9×19 mm Fiocchi nie wykazała obecności tlenku cyrkonu w mikrodrobinach. Głównym składnikiem pocisku jest miedź.

Wydaje się więc, że najbardziej wydajnym materiałem porównawczym jest łuska. Jednak w przypadku badań typowej amunicji zarówno jeden, jak i drugi element amunicji może być dobrym materiałem porównawczym. W amunicji bezołowiowej rodzaj wyrzucanych cząsteczek jest nietypowy, dlatego może stanowić problem w identyfikacji mikrośladów za pomocą rutynowo wykorzystywanej techniki SEM/EDS. Prawdopodobnie nastąpiła kontaminacja (zanieczyszczenie) metalami, z których pocisk jest wykonany. Sygnał od cząstek tlenku cyrkonu na powierzchni dna pocisku mógł ulec zagłuszeniu.

Drugim etapem badań była analiza nieorganicznych pozostałości powystrzałowych uzyskanych z amunicji S&B 9×19 mm Luger oraz G.F.L. 9×19 mm Fiocchi i osadzonych na powierzchni materiału bawełnianego. Mikroślady pobrano w promieniu około 5 cm wokół przestrzeliny. Z uwagi na obecność metali powierzchni stolików z naniesionymi pozostałościami powystrzałowymi nie pokryto przewodzącą warstewką węgla. W przypadku badań materiałów nieprzewodzących napylone warstwy odgrywają rolę nie tylko przewodnika prądu elektrycznego, lecz także zabezpieczają badaną próbkę przed termicznym oddziaływaniem wiązki elektronowej. Program do automatycznej identyfikacji śladów powystrzałowych wyszukał cząstki o określonych cechach. Zgodność składu pierwiastkowego każdej cząstki, ustalonego na postawie zarejestrowanego dla tej cząstki widma rentgenowskiego z przypisaną jej przez program klasą chemiczną, była sprawdzana i korygowana przez operatora.

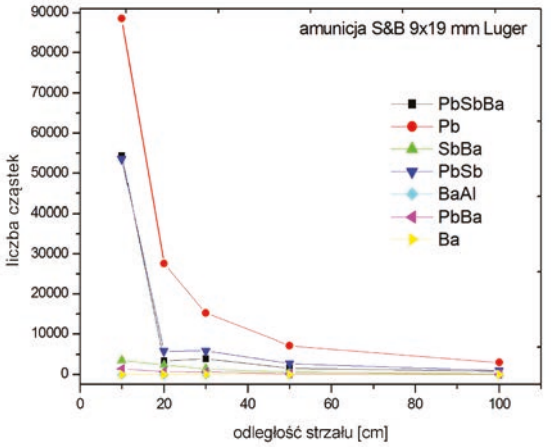
W tabeli 4 przedstawiono wyniki uzyskane po oddaniu strzału amunicją S&B 9×19 mm Luger z różnej odległości do tarcz wykonanych z materiału bawełnianego. Na bada-

nym materiale stwierdzono obecność cząstek metalicznych o składzie i morfologii typowej dla śladów powystrzałowych. Ujawniono wśród nich – w zależności od odległości – od kilkuset do kilkudziesięciu tysięcy charakterystycznych cząstek trójskładnikowych Pb-Sb-Ba oraz od kilkuset do kilkudziesięciu tysięcy dwu- i jednoskładnikowych cząstek zgodnych.

Tab. 4. Mikrodrobiny zebrane z powierzchni tarczy z okolic przestrzeliny, strzały z różnych odległości amunicją S&B 9×19 mm Luger.

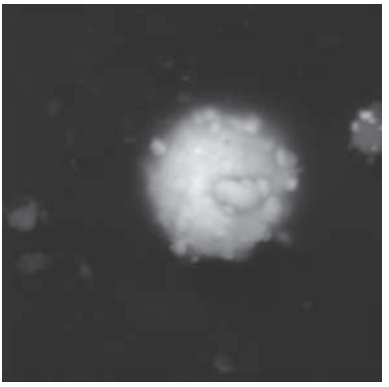
Klasy	Rodzaj klasy	Liczba cząstek w zależności od odległości od tarczy				
		10 cm	20 cm	30 cm	50 cm	100 cm
Pb Sn Sb Ba	charakterystyczne	0	0	0	0	0
Pb Sb Ba	**charakterystyczne**	**54305**	**3433**	**3909**	**1523**	**802**
Ba Ca Si	zgodne Pb Sb Ba	5	16	21	4	5
Sb Ba	zgodne Pb Sb Ba	3545	2357	1432	573	247
Pb Sb	zgodne Pb Sb Ba	53540	5838	5873	2745	961
Ba Al	zgodne Pb Sb Ba	0	6	5	4	1
Pb Ba	zgodne Pb Sb Ba	1410	742	616	226	136
Pb	zgodne Pb Sb Ba	88575	27664	15302	7153	2985
Sb	zgodne Pb Sb Ba	0	0	0	0	0
Ba	zgodne Pb Sb Ba	0	13	15	4	2
Pb Sn Ca Ba Si	zgodne Pb Sb Ba	0	0	0	0	0
Pb Ca Ba Si	zgodne Pb Sb Ba	2	11	4	1	2
Pb Ca	zgodne Pb Sb Ba	186	514	251	157	59
Pb Cl	zgodne Pb Sb Ba	4	6	4	5	0
S Sb	zgodne Pb Sb Ba	0	0	0	0	0
Pb Sn Sb	zgodne Pb Sb Ba	0	0	0	0	0
Ti Zn Gd	lead-free / non-toxic (bezołowiowe/ nietoksyczne)	0	0	0	0	0
Cu Sn Ga	lead-free / non-toxic (bezołowiowe/ nietoksyczne)	0	0	0	0	0
Zr	lead-free / non-toxic (bezołowiowe/ nietoksyczne)	0	0	0	0	0
K Si Al	środowiskowe	2	9	11	1	0
Cu Zn	środowiskowe	3	23	14	11	8
Sn	środowiskowe	0	0	0	0	0
Fe	środowiskowe	3	47	64	51	160
Cu	środowiskowe	6	38	35	9	17
Zn	środowiskowe	1	8	8	10	13
Bi	środowiskowe	0	0	6	59	3
Ba SO_4	środowiskowe	343	1168	909	291	106
Pb Sn	środowiskowe	0	0	0	0	0
K Cl	środowiskowe	0	11	4	8	4
Ti	środowiskowe	1	11	4	3	4
Si	środowiskowe	11	47	28	12	0
Al Si	środowiskowe	19	15	12	3	2

Najwięcej cząstek charakterystycznych i zgodnych zidentyfikowano na powierzchni tarczy, do której oddano strzał z odległości 10 cm. Nie zaobserwowano dwuskładnikowych cząstek zgodnych o składzie pierwiastkowym BaAl. Zarejestrowano największą liczbę cząstek ołowiu oraz dwuskładnikowych cząstek typu PbSb. Podobną tendencję (dominacja cząstek zgodnych o składzie Pb oraz PbSb oraz znikoma liczba lub brak cząstek o składzie BaAl) obserwowano na stolikach z mikrośladami zebranymi z tarcz, do których oddano strzał z większych odległości (wykres 1).



Wykres 1. Zależności liczby cząstek charakterystycznych i zgodnych od odległości strzału.

W miarę zwiększania dystansu strzelca od tarczy zmniejsza się ilość mikrośladów zebranych na stolikach. Najmniejszą liczbę cząstek charakterystycznych i zgodnych ujawniono na stoliku z mikrośladami uzyskanymi po wystrzale z odległości 1 m. Typowy kształt cząstki charakterystycznej przedstawia (zdj. 5).



Zdj. 5. Zdjęcie SEM cząsteczki charakterystycznej pozostałości po wystrzale z broni palnej na powierzchni stolika mikroskopowego.

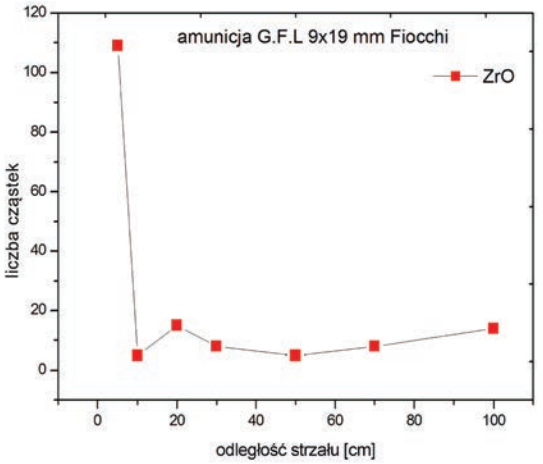
We wszystkich zbadanych próbkach tym śladom towarzyszyły inne niecharakterystyczne pozostałości, np. drobiny mosiądzu (miedź, cynk), kryształki siarczanu baru ($BaSO_4$) i inne.

Wyniki uzyskane po wystrzale amunicją G.F.L. 9×19 mm Fiocchi z różnych odległości do tarcz wykonanych z materiału bawełnianego przedstawiono w tab. 5.

Tab. 5. Mikrodrobiny zebrane z powierzchni tarczy z okolic przestrzeliny, strzały z różnych odległości amunicją G.F.L. 9×19 mm Fiocchi.

Klasy	**Rodzaj klasy**	**Liczba cząstek w zależności od odległości od tarczy**						
		5 cm	**10 cm**	**20 cm**	**30 cm**	**50 cm**	**70 cm**	**100 cm**
ZrO	**lead-free/ non-toxic** (bezołowiowe/ nietoksyczne)	**109**	**5**	**15**	**8**	**5**	**8**	**14**
Cu Zn	środowiskowe	221	102	22	9	3	30	2
Ni	środowiskowe	73	0	3	3	4	18	2
Fe	środowiskowe	229	96	285	116	146	66	189
Cu	środowiskowe	1220	272	162	28	19	168	12
Zn	środowiskowe	55	14	57	18	11	24	22
Bi	środowiskowe	0	0	0	0	0	0	0
Ba SO_4	środowiskowe	22	6	15	28	17	2	24
Pb Sn	środowiskowe	0	0	0	0	0	0	0
K Cl	środowiskowe	48	15	33	17	26	15	26
Ti	środowiskowe	12	3	17	7	13	5	11
Si	środowiskowe	2494	606	2049	511	506	1518	614
K Al Si	środowiskowe	8063	802	2716	476	1169	3502	1148

Na badanym materiale stwierdzono obecność cząstek metalicznych o składzie i morfologii nietypowej dla śladów powystrzałowych. Ujawniono wśród nich – w zależności od odległości – od kilku do kilkudziesięciu cząstek tlenku cyrkonu (ZrO). Najwięcej cząstek ZrO (109 cząstek) zidentyfikowano na powierzchni tarczy, do której oddano strzał z odległości 5 cm. Na pozostałych tarczach liczba cząstek ZrO zmieniała się wraz ze wzrostem odległości strzału, w niewielkim zakresie fluktuując w liczbie od kilku do kilkunastu (wykres 2).



Wykres 2. Zależność liczby cząstek ZrO od odległości strzału.

W zakresie odległości strzału od 10 cm do 100 cm nie obserwowano wyraźnego spadku liczby cząstek ZrO wraz ze wzrostem odległości. W zabezpieczonych mikrośladach obserwowano głównie trójskładnikowe cząsteczki zawierające glin (Al), krzem (Si) i potas (K). Pierwiastki te stanowiły więcej niż 90% analizowanych cząstek. Inne pierwiastki, które wykryto za pomocą mikroanalizatora EDS, to chlor (Cl), nikiel (Ni), żelazo (Fe), miedź (Cu) i cynk (Zn).

Badania spektroskopią Ramana

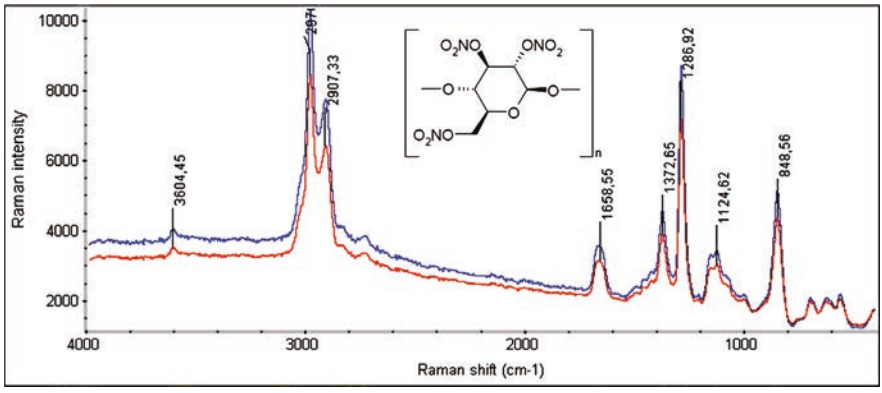
W niniejszym artykule omówiono wybrane zakresy występowania pasm charakterystycznych w widmach cząsteczek i makrocząsteczek organicznych. W zakresie 3100–2900 cm^{-1} występują pasma odpowiadające drganiom rozciągającym grupy CH_2, [ν_{CH2} (R, IR)]. W zakresie 1650–1500 cm^{-1} występują pasma odpowiadające drganiom rozciągającym asymetrycznym grupy NO_2. W zakresie 1390–1250 cm^{-1} pojawiają się pasma odpowiadające drganiom rozciągającym symetrycznym grup NO_2. W zakresie poniżej 850 cm^{-1} są widoczne pasma odpowiadające drganiom rozciągającym, symetrycznym (ν_{NO2}), nożycowym (δ_{NO2},). W zakresie 697 cm^{-1} 446 cm^{-1} i 1455 cm^{-1} występują pasma odpowiadające obecności soli $PbSO_4$ i $BaCO_3$[39]. Zakres pasm charakterystycznych zestawiono w tab. 6.

[39] J. Bueno, V. Sikirzhytski, I.K. Lednev, *Raman spectroscopic analysis of gunshot residua*…, s. 4334; M. Lopez-Lopez, J.J. Delgado, C. Garcia-Ruiz, *Ammunition identification by means of the organic analysis of gunshot residues*…, s. 3581; S.P. Sharma, S.C. Lahiri, *A preliminary investigation into the use of FTIR microscopy as a probe for the identification of bullet entrance holes and the distance of firing*, „Science & Justice" 2009, nr 49, s. 197; M. Lopez-Lopez, J.L. Ferrando, C. Garcia-Ruiz, *Comparative analysis of smokeless gunpowders by Fourier transform infrared and Raman spectroscopy*, „Analytica Chimica Acta" 2012, nr 717, s. 92; S. Stich i in., *Raman microscopic identification of gunshot residue,* „Journal of Raman Spectroscopy" 1998, nr 29, s. 787.

Tab. 6. Zakresy występowania pasm charakterystycznych wskazanych jako diagnostyczne w identyfikacji poszczególnych związków organicznych. Podano zakresy częstości drgań, rodzaj pasma, oznaczenia rodzajów drgań oraz rodzaj drgania.

Zakres częstości drgań/cm^{-1}	Rodzaj pasma	Oznaczenie rodzaju drgania	Rodzaj drgań
2971, 2907	CH_2	ν_{CH2}	rozciągające wiązania symetryczne
1650–1500	NO_2	$\nu_{asymNO2}$	rozciągające wiązania asymetryczne
	C=C	$\nu_{C=C}$	rozciągające
1455	CO_3	ν_{1CO3}	rozciągające wiązania asymetryczne
1390–1250	NO_2	ν_{symNO2}	rozciągające wiązania symetryczne
1200–1000	CO	ν_{CO}	rozciągające
Poniżej 850	NO_2	$\delta_{NO2,}\ \nu_{NO2}$	drgania nożycowe symetryczne
	CO_3	ν_{2CO3}	asymetryczne drgania deformacyjne

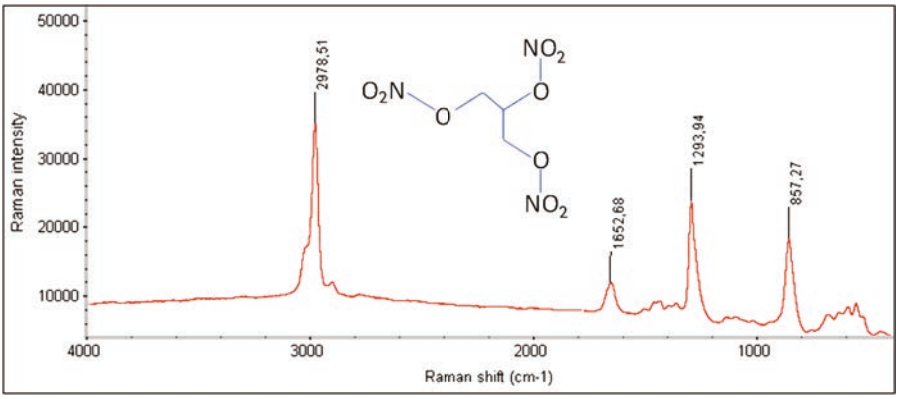
Dla nitrocelulozy (wykres 3) charakterystyczne są pasma przy 2971 cm^{-1} i 2907 cm^{-1} odpowiadające drganiom rozciągającym symetrycznym grupy CH_2. Pasmo przy 1658 cm^{-1} odpowiada drganiom rozciągającym asymetrycznym grupy NO_2, a pasmo przy 1286 cm^{-1} – drganiom rozciągającym symetrycznym grupy NO_2. Obserwowano również pik przy 1124 cm^{-1} odpowiadający drganiom rozciągającym grupy C–O oraz przy 848 cm^{-1} – drganiom nożycowym NO_2 [40].



Wykres 3. Widmo Ramana czystej nitrocelulozy w zakresie 4000–400 cm^{-1} – linia wzbudzająca 532 nm.

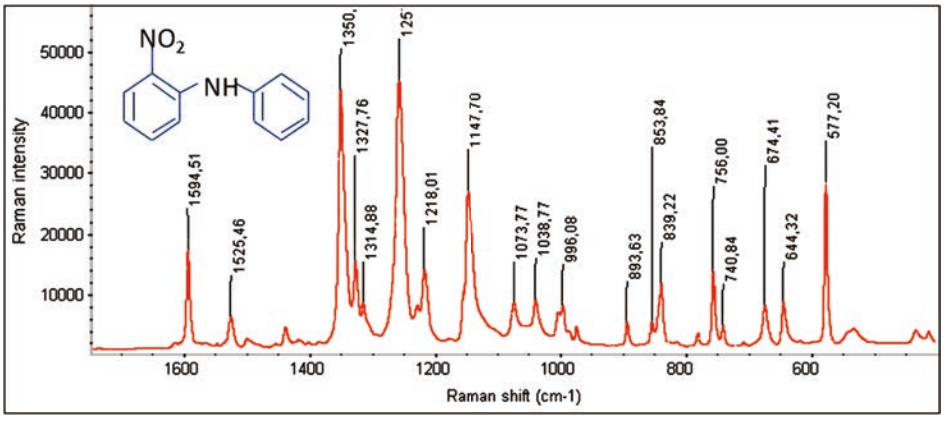
W widmie nitrogliceryny (wykres 4) wyróżniono pasma przy 2978 cm^{-1} odpowiadające drganiom rozciągającym symetrycznym grupy CH_2. Pasmo przy 1652 cm^{-1} odpowiada drganiom rozciągającym asymetrycznym grupy NO_2, a pasmo przy 1293 cm^{-1} – drganiom rozciągającym symetrycznym grupy NO_2. Obserwowano również pik w 857 cm^{-1} odpowiadający drganiom nożycowym NO_2 [41].

[40] S.P. Sharma, S.C. Lahiri, *A preliminary investigation into the use of FTIR microscopy*…, s. 197.
[41] Tamże.



Wykres 4. Widmo Ramana czystej nitrogliceryny w zakresie 4000–400 cm^{-1} – linia wzbudzająca 532 nm.

W widmie 2-nitrodifenyloaminy (wykres 5) zaobserwowano pasmo przy 1594 cm^{-1} odpowiadające drganiom rozciągającym symetrycznym C=C pierścienia aromatycznego oraz pasma w zakresie 1400–1150 cm^{-1} odpowiadające drganiom deformacyjnym CH i drganiom rozciągającym C=C, charakterystyczne dla pierścieni aromatycznych. Pasma w zakresie 1000–550 cm^{-1} odpowiadały drganiom wahadłowym grupy CH oraz drganiom rozciągającym C=C, charakterystycznym dla pierścieni aromatycznych. Podobne widmo zostało przedstawione w publikacjach P. Sett i inni oraz Lindblom i inni[42].

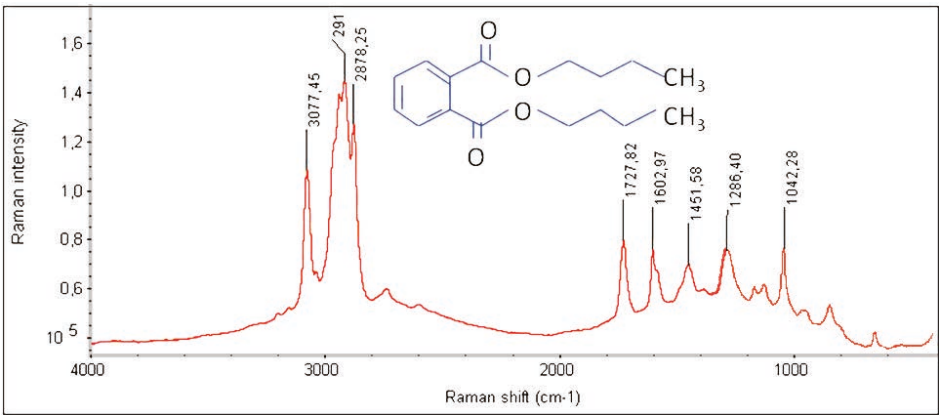


Wykres 5. Widmo Ramana czystej 2-nitrodifenyloaminy w zakresie 2000–400 cm^{-1} – linia wzbudzająca 532 nm.

W zakresie 3200–2800 cm^{-1} ftalanu dibutylu (wykres 6) występuje pasmo przy 3077 cm^{-1} odpowiadające drganiom rozciągającym C=H oraz pasma pomiędzy 3000–

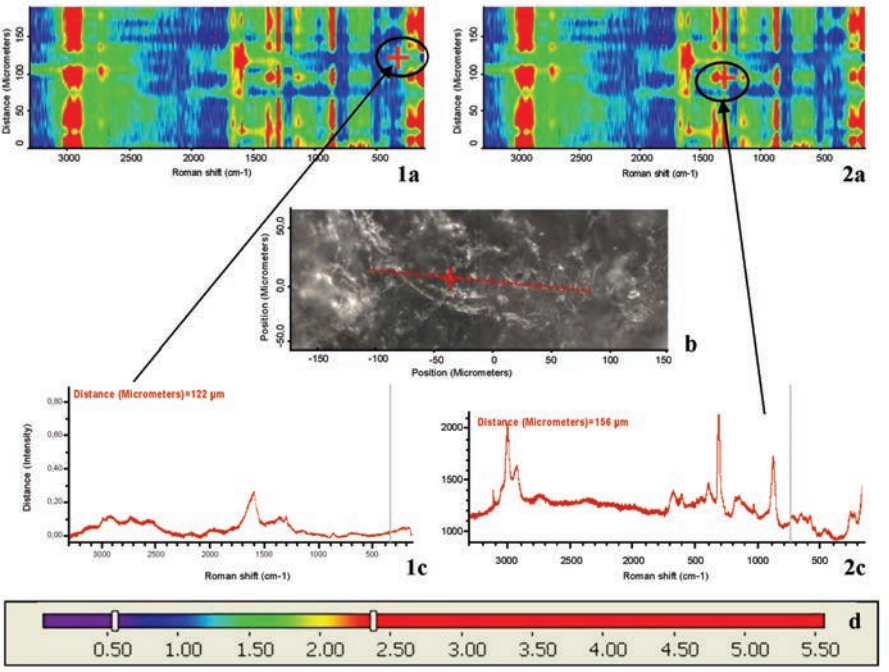
[42] T. Lindblom, A.A. Christy, F.O. Libnau, *Quantitative determination of stabilizer in single base propellant by chemometric analysis of Fourier transform infrared spectra*, „Chemometrics and Intelligent Laboratory Systems" 1995, nr 29, s. 243; P. Sett, A.K De., S. Chattopadhyay, P.K. Mallick, *Raman excitation profile of diphenylamine*, „Chemical Physics" 2002, nr 276, s. 211.

2800 cm^{-1} odpowiadające drganiom rozciągającym grup CH_2 i CH_3. Pasmo przy 1728 cm^{-1} przypisano drganiom rozciągającym C=O, wąskie pasmo przy 1602 cm^{-1} zaś drganiom rozciągającym symetrycznym pierścienia aromatycznego.



Wykres 6. Widmo Ramana czystego ftalanu dibutylu w zakresie 4000–400 cm^{-1} – linia wzbudzająca 532 nm.

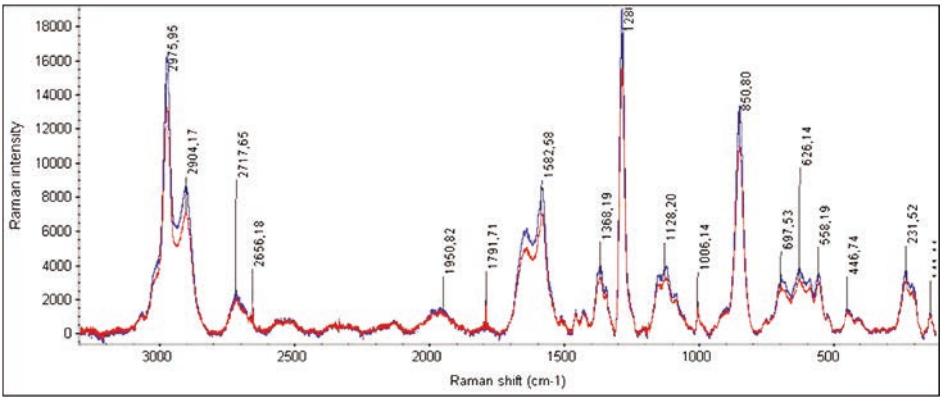
W celu zbadania homogeniczności mikrodrobin niespalonego lub częściowo spalonego prochu wykonano mapowanie ramanowskie kilku ziaren prochu. Jedynie niektóre ziarna wykazały obecność ostrych pasm charakterystycznych. Najbardziej wyraźne w widmie ramanowskim mikrodrobin pozostałości powystrzałowych są pasma odpowiadające grupom NO_2 oraz CH_2, nitrogliceryny i nitrocelulozy. Na zdjęciu 6 i wykresie 7 pokazano mapy zmiany intensywności pasma drgań rozciągających grupy NO_2 oraz pasma drgań rozciągających symetrycznych grupy CH_2. W przypadku mikrodrobiny pochodzącej z pozostałości od amunicji G.F.L 9×19 mm Fiocchi zawierającej nitroglicerynę i nitrocelulozę intensywność pasma grupy NO_2 zmienia się od 0,10 do 5,50. Ta zmiana pozwala sądzić, że układ nie jest homogeniczny. Pojawiają się obszary niemal pozbawione związków chemicznych zawierających pasma grupy NO_2.



Zdj. 6. Mapy zmiany intensywności pasma drgań rozciągających grupy NO_2 w ziarnie niespalonego prochu z amunicji G.F.L. 9×19 mm Fiocchi (1a, 2a); obraz analizowanego fragmentu powierzchni próbki z mikroskopu konfokalnego (b); widma Ramana w punktach zaznaczonych czerwonym krzyżykiem odpowiednio na mapach (1c, 2c); skala przyporządkowania kolorów wartościom zmiany intensywności pasma grupy NO_2 (d).

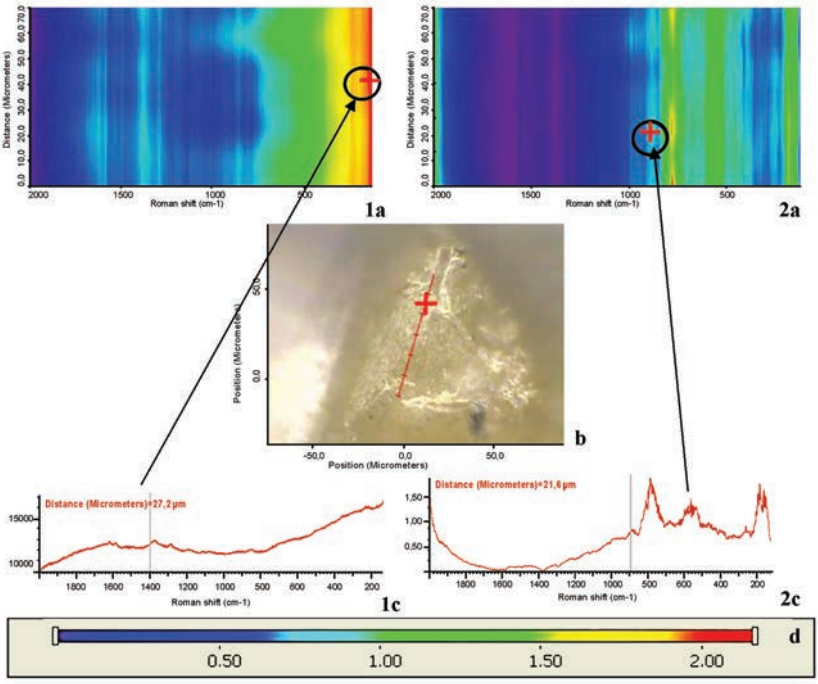
Widma przedstawione na zdj. 6 odzwierciedlają charakter badanej mikrodrobiny pod względem składu chemicznego w jednym punkcie na mapie. W zależności od rozkładu barw na mapie obserwowano zmiany intensywności pasm interesujących osoby badające. W punkcie zaznaczonym na mapie (zdj. 6.1a) czerwonym krzyżykiem w obszarze jasnozielonym widoczne w widmie (zdj. 6.1c) jest głównie pasmo odpowiadające drganiom rozciągającym C–C. Natomiast w punkcie zaznaczonym na mapie (zdj. 6.2a) czerwonym krzyżykiem w obszarze czerwonym widoczne w widmie (zdj. 6.2c) są wszystkie pasma związane z obecnością nitrogliceryny i nitrocelulozy.

Widmo sumaryczne (wykres 7) jest to złożenie widm nitrogliceryny i nitrocelulozy. Obserwowane są również inne pasma. Prawdopodobnie są to pasma odpowiadające pasmom charakterystycznym dla ftalanu dibutylu oraz 2-nitrodifenyloaminy. W celu dokładnego określenia pozostałych składników mikrodrobin wymagane jest przeprowadzenie dokładniejszych badań.



Wykres 7. Sumaryczne widmo Ramana zebrane z 19 punktów pomiarowych mapy dla ziarna niespalonego prochu z amunicji G.F.L. 9×19 mm Fiocchi w zakresie 4000–400 cm^{-1}, przy pobudzeniu niskoenergetyczną linią 780 nm lasera czerwonego.

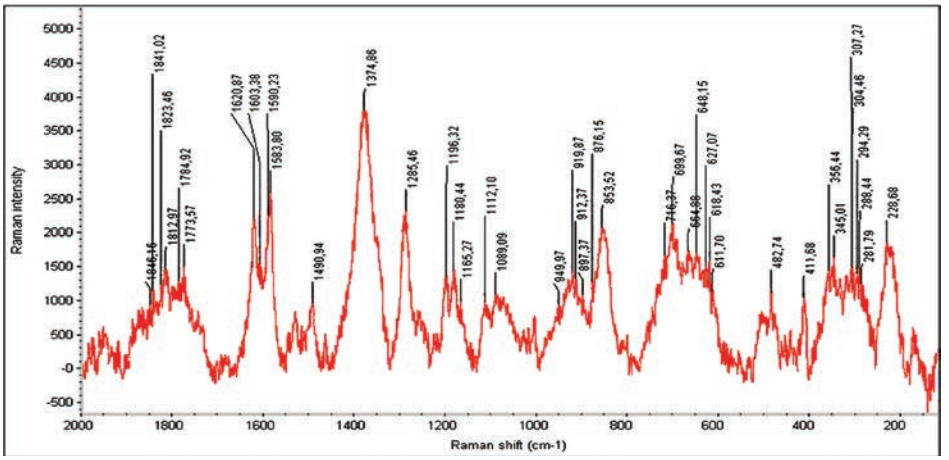
W przypadku mikrodrobiny pochodzącej z pozostałości od amunicji S&B 9×19 mm Luger zawierającej nitrocelulozę intensywność pasma grupy NO_2 zmienia się od 0,10 do 2,20. Ta zmiana pozwala sądzić, że układ nie jest homogeniczny (zdj. 7).



Zdj. 7. Mapy zmiany intensywności pasma drgań rozciągających grupy NO_2 w ziarnie niespalonego prochu z amunicji S&B 9×19 mm Luger (1a i 2a); obraz analizowanego fragmentu powierzchni próbki z mikroskopu konfokalnego (b); widma Ramana w punkcie zaznaczonym czerwonym krzyżykiem odpowiednio na mapach (1c i 2c); skala przyporządkowania kolorów wartościom zmiany intensywności pasma grupy NO_2 (d).

Podobnie jak w poprzedniej próbce w zależności od rozkładu barw na mapie obserwowano zmiany intensywności interesujących nas pasm. W punkcie zaznaczonym na mapie czerwonym krzyżykiem w obszarze czerwonym (zdj. 7.1a) widoczne w widmie na zdj. 7.1c są pasma nitrocelulozy o niewielkiej intensywności. Natomiast w punkcie zaznaczonym na mapie czerwonym krzyżykiem w obszarze jasnoniebieskim (zdj. 7.2a) widoczne w widmie na zdj. 7.2c są pasma o większej intensywności, co jest związane z obecnością nitrocelulozy.

Widmo sumaryczne (wykres 8) zawiera głównie widmo nitrocelulozy. Pasma w zakresie ~1600 cm^{-1} i 1300 cm^{-1} są odpowiedzialne za obecność w mikrodrobinach cząsteczek węgla.



Wykres 8. Sumaryczne widmo Ramana zebrane z siedmiu punktów pomiarowych mapy dla ziarna niespalonego prochu z amunicji S&B 9×19 mm Luger w zakresie 4000–400 cm^{-1}, przy pobudzeniu niskoenergetyczną linią 780 nm lasera czerwonego.

Podsumowanie

Badania morfologii oraz nieorganicznych składników typowych cząstek pozostałości powystrzałowych zapewniają pewną identyfikację materiału dowodowego. Zaprezentowano tutaj znaną od dawna w świecie nauki metodę analizy cząstek, jaką jest skaningowa mikroskopia elektronowa (SEM), która w pierwszej fazie badań ma na celu ich zlokalizowanie. Mikroanalizator rentgenowski (EDS) sprzężony z mikroskopem daje możliwość określenia składu pierwiastkowego analizowanych cząstek. Na podstawie przeprowadzonych badań dwóch zestawów śladów powystrzałowych otrzymanych podczas eksperymentu z użyciem pistoletów Glock i Walter oraz amunicji, kaliber 9 mm, stwierdzono, że ich powtarzającą się cechą jest występowanie wśród całej populacji (prowadzone są badania populacyjne) metalicznych śladów powystrzałowych pochodzących ze spłonki amunicji S&B 9×19 mm Luger dużej liczby charakterystycznych i zgodnych cząstek oraz ze spłonki amunicji G.F.L. 9×19 mm Fiocchi do kilkudziesięciu cząstek tlenku cyrkonu. Zgodnie z przewidywaniami liczba charakterystycznych i zgodnych cząstek pochodzących ze spłonki amunicji S&B 9×19 mm Luger zmniejszała

się wraz z odległością. Samo ujawnienie cząstek charakterystycznych i zgodnych w zabezpieczonym materiale nie powinno być pominięte przy formułowaniu opinii. W takich przypadkach wnioskowanie w kategorii prawdopodobieństwa wydaje się uzasadnione, gdyż może wnieść istotny wkład do badań.

Ujawnione pozostałości pochodzące ze spłonki amunicji ekologicznej, celowo znakowanej i wykorzystywanej jedynie przez służby, wskazują na kontaminację. Pozwala to na odróżnienie tych pozostałości od pozostałości spłonkowych o typowym składzie zebranych na miejscu zdarzenia, które pochodzą z amunicji stosowanej w celach przestępczych.

Eksperyment z amunicją ekologiczną, G.F.L. 9×19 mm Fiocchi wykazał obecność nietypowych pozostałości powystrzałowych zawierających głównie cząstki tlenku cyrkonu (ZrO) zgodne ze składem spłonki. W porównaniu z wynikami uzyskanymi po wystrzeleniu amunicji o typowym składzie pierwiastkowym spłonki, nie obserwowano wyraźnych zmian liczby cząstek ZrO wraz ze wzrostem odległości. Ze względu na dostępność rynkową badanej amunicji tlenek cyrkonu nie jest już tak pewnym dowodem, mimo że rzadko występuje w środowisku. Opinia oparta jedynie na wynikach analizy SEM/EDX będzie miała zatem charakter negatywny.

Po przeprowadzeniu badań związanych z możliwością uzyskania pozostałości powystrzałowych z powierzchni denka pocisku, stwierdzono, że jedynie pocisk pochodzący z amunicji S&B 9×19 mm Luger zawierał charakterystyczne i zgodne cząstki pozostałości powystrzałowych. W przypadku pocisku pochodzącego z amunicji ekologicznej nie znaleziono cząstek tlenku cyrkonu.

Na podstawie analizy ujawniania cząstek pozostałości powystrzałowych można wnioskować, że jedynie amunicja o typowym składzie spłonkowym może dawać pozytywne wyniki badań metodą SEM/EDS. W przypadku pozostałości pochodzących z amunicji ekologicznej – pod warunkiem, że nie jest ona stosowana jedynie przez służby – analiza z wykorzystaniem metody SEM/EDS jest niewystarczająca i trudna. Jak na wstępie wspomniano, pomocna może się stać analiza organicznych składników pozostałości powystrzałowych.

Analizowano również pozostałości powystrzałowe ujawnione na tarczy wykonanej z materiału bawełnianego, do której oddano strzał z odległości około 20 cm. Porównania składu organicznego pozostałości dokonano dla amunicji S&B 9×19 mm Luger oraz amunicji ekologicznej G.F.L. 9×19 mm Fiocchi. W próbkach uzyskanych z amunicji S&B 9×19 mm Luger wykazano obecność nitrocelulozy. Maksimum pasma występowało przy 1285 cm^{-1}. W materiale uzyskanym z amunicji G.F.L. 9×19 mm Fiocchi wykazano obecność nitrocelulozy i nitrogliceryny oraz prawdopodobnie takich pochodnych, jak 2-nitrodifenyloaminy i 4-nitrodifenyloaminy. Maksimum pasma nitrodifenyloaminy występowało przy 1368 cm^{-1}.

Mapowanie ramanowskie wykazało niehomogeniczność ziaren prochu. Jedynie niektóre ziarna wykazały obecność ostrych pasm charakterystycznych. W większości badane ziarna zawierały głównie węgiel.

W wyniku przeprowadzonego eksperymentu[43] wykazano możliwość identyfikacji składników nieorganicznych oraz niektórych związków organicznych zawartych w pozostałościach powystrzałowych na podstawie SEM/EDS oraz spektrometrii mi-

[43] Za pomoc w przeprowadzeniu eksperymentu autorka serdecznie dziękuje: Zastępcy Dyrektora BBK ABW płk. Dariuszowi Błachutowi, Pawłowi Zajmie, a także kierownictwu Centralnego Ośrodka Szkolenia ABW za udostępnienie strzelnicy oraz Kolegom kierującym i odpowiedzialnym za strzelnicę.

Badania zostały przeprowadzone na urządzeniach zakupionych w ramach projektu badawczego Nr 0023/RID3/2012/02 z 30 VII 2012 r., finansowanego ze środków NCBiR.

kroramanowskiej, a także wykazano możliwość obrazowania – mapowania zmian intensywności pasm niektórych grup funkcyjnych substancji organicznych obecnych w pojedynczym ziarnie.

Należy zauważyć, że zrealizowany eksperyment to jedynie wstęp do podjęcia dalszych, bardziej zaawansowanych badań prowadzących do identyfikacji, klasyfikacji oraz segregacji mikrośladów pochodzących z przestępstw z udziałem broni.

Bibliografia:

1. Arndt J. i in., *Preliminary evolution of the persistence of organic gunshot residua*, „Forensic Science International" 2012, nr 222.
2. Barańska H., Łabudziński A., Terpiński J., *Laserowa spektroskopia ramanowska*, Warszawa 1981, PWN.
3. Benito S. i in., *Characterization of organic gunshot residues in lead-free ammunition using a new sample collection device for liquid chromatography-quadrupole time-of-flight mass spectrometry*, „Forensic Science International" 2015, nr 246.
4. Berk R.E., *Automated SEM/EDS analysis of airbag residue. II: Airbag residue as a source of percussion primer residue particles*, „Journal of Forensic Science" 2009, nr 54.
5. Bueno J. i in., *Attenuated total reflectance FT-IR imaging for rapid and automated detection of gunshot residue*, „Analytical Chemistry" 2014, nr 86.
6. Bueno J. i in., *Attenuated total reflectance FT-IR Spectroscopy for gunshot residue analysis: potential for ammunition determination*, „Analytical Chemistry" 2013, nr 85.
7. Bueno J., Sikirzhytski V., Lednev I.K., *Raman spectroscopic analysis of gunshot residua offering great potential for caliber differentiation*, „Analytical Chemistry" 2012, nr 84.
8. Burnett B., *Errors in gunshot residue assessment by scanning electron microscopy/elemental analysis in criminal cases: III. Friction-brake particles assigned as highly specific gunshot residue particles* [online], http://www.meixatech.com/articles.html 2011 [dostęp: 1 IX 2016].
9. Cardinetti B. i in., *X-ray mapping technique: a preliminary study in discriminating gunshot residue particles from aggregates of environmental occupation origin*, „Forensic Science International" 2004, nr 143.
10. Collins P. i in., *Glass-containing gunshot residue particles: a new type of highly characteristic particle?*, „Journal of Forensic Science" 2003, nr 48.
11. Dalby O., Butler D., Birkett J., *Analysis of gunshot residue and associated materials – a review*, „Journal of Forensic Science" 2010, nr 4.
12. Destefani C.A. i in., *Europium-organic complex as luminescent marker for the visual identification of gunshot residue and characterization by electrospray ionization FT-ICR mass spectrometry*, „Microchemical Journal" 2014, nr 116.
13. Ditrich H., *Distribution of gunshot residua – the influence of weapon type*, „Forensic Science International" 2012, nr 220.
14. Filewicz A., *Kryminalistyczne badania pozostałości po wystrzale z broni palnej (GSR)*, Warszawa 2001, Centralne Laboratorium Kryminalistyczne KGP.
15. *Guide for primer gunshot residue analysis by scanning electron microscopy/energy dispersive X-ray spectrometry* [online], Scientific Working Group for Gunshot Residue, http://www.swggsr.org/documents.html 2011 [dostęp: 1 IX 2016].

16. Gunaratnan L., Himberg K., *The identification of gunshot residue particles from lead free Sintox ammunition*, „Journal of Forensic Science" 1994, nr 39.
17. Ivanowić A., *Is there a way to precisely identify that the suspect fired from the firearm?*, „Forensic Science International" 2003, nr 136 (Supplement 1).
18. Kosanke K.L., Dujay R.C., Kosanke B.J., *Characterization of pyrotechnic reaction residue particles by SEM/EDS*, „Journal of Forensic Science" 2003, nr 48.
19. Kosanke K.L., Dujay R.C., Kosanke B.J., *Pyrotechnic reaction residue particles*, „Journal of Forensic Science" 2006, nr 51.
20. Krüsemann H., *SEMs and forensic science*, „Problems of Forensic Sciences" 2001, nr 47.
21. Laza D. i in., *Development of a quantitative LC-MS/MS method for the analysis of common propellant powder stabilizers in gunshot residua*, „Journal of Forensic Science" 2007, nr 52.
22. Lindblom T., Christy A.A., Libnau F.O., *Quantitative determination of stabilizer in single base propellant by chemometric analysis of Fourier transform infrared spectra*, „Chemometrics and Intelligent Laboratory Systems" 1995, nr 29.
23. Lopez-Lopez M., Delgado J.J., Garcia-Ruiz C., *Ammunition identification by means of the organic analysis of gunshot residues using Raman spectroscopy*, „Analytical Chemistry" 2012, nr 84.
24. Lopez-Lopez M., Ferrando J.L., Garcia-Ruiz C., *Comparative analysis of smokeless gunpowders by Fourier transform infrared and Raman spectroscopy*, „Analytica Chimica Acta" 2012, nr 717.
25. Lopez-Lopez M. i in., *Analysis of macroscopic gunshot residues by Raman spectroscopy to assess the weapon memory effect*, „Forensic Science International" 2013, nr 231.
26. Martiny A. i in., *SEM/EDS analysis and characterization of gunshot residues from Brazilian lead – free ammunition*, „Forensic Science International" 2008, nr 177.
27. Mejia R., *Why we cannot rely on firearms forensics,* „New Scientist" 2005, nr 2527.
28. Melo L.G.A. i in., *Nano characterization of gunshot residues from Brazilian ammunition*, „Forensic Science International" 2014, nr 240.
29. Meng H., Caddy B., *Gunshot residue analysis – a review*, „Journal of Forensic Science" 1997, nr 42.
30. Mosher P.V. i in., *Gunshot residue-similar particles produced by fireworks*, „Canadian Society of Forensic Science" 1998, nr 31.
31. Romolo F.S., Margot P., *Identification of gunshot residue: a critical review*, „Forensic Science International" 2000, nr 119.
32. Sadlej J., *Spektroskopia molekularna*, Warszawa 2002, WNT.
33. Sett P., De A.K., Chattopadhyay S., Mallick P.K., *Raman excitation profile of diphenylamine*, „Chemical Physics" 2002, nr 276.
34. Sharma S.P., Lahiri S.C., *A preliminary investigation into the use of FTIR microscopy as a probe for the identification of bullet entrance holes and the distance of firing*, „Science & Justice" 2009, nr 49.
35. *Standard Guide for Gunshot Residue Analysis by Scanning Electron Microscopy/ Energy-Dispersive Spectroscopy*, ASTM E 1588-10.
36. Stich S. i in., *Raman microscopic identification of gunshot residue,* „Journal of Raman Spectroscopy" 1998, nr 29.

37. Szummer A., *Podstawy ilościowej mikroanalizy rentgenowskiej*, Warszawa 1994, WNT.
38. Szymański H.A., *Raman spectroscopy*, New York 1967, Plenum Press.
39. Taudte R.V. i in., *Detection of gunshot residues using mass spectrometry*, „BioMed Research International" 2014.
40. Torre C. i in., *Brake linings: a source of non-GSR particles containing lead, barium and antimony*, „Journal of Forensic Science" 2002, nr 47.
41. Wade Moran J. i in., *Skin permeation of organic gunshot residua: implications for sampling and analysis*, „Analytical Chemistry" 2014, nr 86.
42. Weber I.T. i in., *High photoluminescent metal-organic framework as optical markers for the identification of gunshot residues*, „Analytical Chemistry" 2011, nr 83.
43. Weber I.T. i in., *Up-conversion properties of lanthanide-organic framework and how to track ammunitions using these materials*, „RSC Advances" 2012, nr 2.
44. Weber I.T. i in., *Use of luminescent gunshot residues markers in forensic context*, „Forensic Science International" 2014, nr 244.

Abstrakt

W publikacji przedstawiono rezultaty pilotażowych badań metodą skaningowej mikroskopii elektronowej sprzężonej z mikroanalizą rentgenowską oraz spektroskopii Ramana. Wykazano możliwość identyfikacji składników nieorganicznych oraz niektórych związków organicznych zawartych w pozostałościach powystrzałowych, a także wprowadzono nowy element badawczy w postaci mapowania zmian intensywności pasm niektórych grup funkcyjnych substancji organicznych obecnych w pojedynczym ziarnie. Celem badań jest stopniowe i systematyczne opracowywanie metodyki analizy chemicznej cząstek powystrzałowych pochodzących z amunicji zawierającej ołów oraz z amunicji bezołowiowej, a także opracowanie procedur badawczych dotyczących oznaczania pozostałości po użyciu z broni palnej, w tym typowanie rodzaju materiałów dowodowych i materiału porównawczego oraz wdrożenie ich do rutynowej praktyki opiniodawczej w Biurze Badań Kryminalistycznych ABW. Wskazane jest także opracowanie własnych kryteriów interpretacji wyników badań pozostałości powystrzałowych w celu powiązania osoby podejrzanej z użyciem broni palnej. Należy zaznaczyć, że zrealizowany eksperyment jest jedynie wstępem do podjęcia dalszych, bardziej zaawansowanych badań, prowadzących do identyfikacji, klasyfikacji oraz dyskryminacji mikrośladów pochodzących z przestępstw z udziałem broni.

Słowa kluczowe: skaningowa mikroskopia elektronowa, SEM, mikroanaliza rentgenowska, EDS, pozostałości po wystrzale z broni palnej, GSR, spektroskopia Ramana.

Abstract

The paper describes the results of the Raman spectroscopy and scanning electron microscopy equipped with X-ray in the primary analysis of gunshot residues. It demonstrates the ability to identify inorganic components and the organic compounds contained in the gunshot residue, and also introduces a new element of the research in the

form of mapping changes in the intensity of bands of some functional groups of organic substances to be found in a single grain. The aim of the research is a gradual and systematical elaboration of the methodology of chemical analysis of gunshot residue particles, originating from ammunition containing lead and unleaded ammunition. Further aim is to develop the testing procedures remains with use of firearms and their implementation in consultative routine practice in the Forensic Laboratory ABW, choosing the type of evidence and comparative materials. In order to relate the person suspected to fact of using firearms, it is advisable to elaborate individual criteria of interpreting the results of gunshot residues study. It should be noted that the conducted experiment determines only a prelude for conducting more advanced researches which lead to the identification, classification and discrimination of microtraces originated from crime use of firearms.

Keywords: scanning electron microscopy, SEM, X-ray analysis, EDX, gunshot residue, GSR, Raman spectroscopy.

Tomasz Kuć

Analiza funkcjonalności systemu kontroli i nadzoru nad służbami specjalnymi w Polsce

Organizacja działalności służb specjalnych w państwie to aksjologiczno-prakseologiczny dylemat współczesnych demokracji. Od czasu przemian ustrojowych zapoczątkowanych w 1989 r. dotyczy on także Polski. Akcentowany problem wynika z istoty funkcjonowania w systemie demokratycznym tajnych służb, które mogą być zarówno efektywnym instrumentem zapewniającym bezpieczeństwo państwa, jak i zagrożeniem dla jego konstytucyjnych standardów ustrojowych. Truizmem jest zatem twierdzenie, że demokratyczna kontrola służb powołanych do ochrony bezpieczeństwa państwa oraz nadzór nad nimi są bardzo ważnymi elementami warunkującymi ich właściwe i efektywne wykorzystanie. Cywilne i demokratyczne zwierzchnictwo nad organami wchodzącymi w skład tzw. resortów siłowych oraz nad służbami specjalnymi jest standardem w państwach o utrwalonych tradycjach demokratycznych. Zwierzchnictwo polityczne objęte przez organy mające społeczną legitymację do wykonywania tego zadania jest warunkiem sine qua non uznania sił zbrojnych i formacji zmilitaryzowanych za instrument bezpieczeństwa państwa, a co za tym idzie – instrument służący również ochronie jego obywateli[1].

Problem zwierzchnictwa dotyczy szczególnie służb specjalnych – ze względu na charakterystyczny element ich działania, tj. niejawność, która determinuje ich skuteczność, ale jednocześnie może wpływać na ich autonomizację i stwarzać możliwość nieuprawnionej presji na mechanizmy funkcjonowania państwa. Niezwykle istotnym czynnikiem ochrony standardów demokracji, w tym konstytucyjnych praw i wolności jednostki, jest więc wykreowany i wdrożony skuteczny system kontroli i nadzoru nad służbami stosującymi metody niejawne, niepodlegające publicznemu osądowi. Istotą takiego systemu jest to, że (…) *państwo, tworząc organizację, której udziela uprawnień do podejmowania niejawnych działań, sprawdza, czy są one prowadzone w jego interesie*[2]. W ramach standardów cywilnej i demokratycznej kontroli i nadzoru zakłada się, że władza wykonawcza (egzekutywa) wyznacza kierunki działalności służb specjalnych i utrzymuje nad nimi bieżący nadzór, władza ustawodawcza (legislatywa) zajmuje się funkcjonowaniem tajnych służb przez uchwalanie przepisów dotyczących ich zadań i uprawnień, ustalanie budżetu, żądanie informacji i przesłuchiwanie osób z grona kierownictwa służb, władza sądownicza natomiast sprawuje kontrolę nad stosowaniem części metod operacyjno-rozpoznawczych oraz osądza ewentualne nadużycia funkcjonariuszy służb.

Przy omawianiu organizacji i funkcjonowania służb specjalnych w państwie demokratycznym można wskazać na kilka obszarów zagrożeń. Pierwszy z nich jest związany z możliwością wystąpienia bezprawnego wpływu tajnych instrumentów bezpieczeństwa, jakim są służby specjalne, na mechanizmy funkcjonowania państwa przez wyolbrzymianie lub kreowanie zagrożeń. Rezultatem takiego zjawiska może być nieuzasadnione poszerzanie uprawnień służb, które skutkuje budową ich omnipotencji, stojącej w opozycji

[1] S. Zalewski, *Służby specjalne w państwie demokratycznym. Wydanie II poszerzone i uaktualnione*, Warszawa 2005, s. 115.

[2] Tenże, *Bezpieczeństwo polityczne państwa. Studium funkcjonalności instytucji*, Siedlce 2010, s. 179.

do wartości społeczeństwa demokratycznego i realizacji interesu państwa[3]. W tym obszarze nadzór i kontrola nad służbami specjalnymi koncentrują się przede wszystkim na ochronie suwerenności ośrodka władzy wykonawczej (rządu) przed ich nieuprawnioną ingerencją. Innymi słowy – służą one pełnemu podporządkowaniu instrumentu bezpieczeństwa ośrodkowi władzy politycznej. W polskich warunkach ustrojowych wpływ na efektywność takiego nadzoru realizuje się również przez działalność parlamentu, którego koalicyjna większość sejmowa ustanawia reguły prawne dotyczące funkcjonowania służb na zapotrzebowanie rządu wyłonionego z tej większości.

Drugi obszar zagrożeń dotyczący funkcjonowania służb specjalnych w demokratycznym państwie prawnym jest związany z postrzeganiem interesu państwa przez pryzmat interesu ośrodka politycznego sprawującego władzę, i – co za tym idzie – nadzoru nad służbami specjalnymi. *Trwałe podziały polityczne w społeczeństwie są wpisane w istotę demokracji* (…). *Niebezpieczeństwa pojawiają się wówczas, gdy podziały polityczne rodzą konflikty rozwiązywane przy pomocy instytucji powołanych do ochrony bezpieczeństwa państwa. Działania takie podważają społeczne zaufanie do tych instytucji. Jest to źródłem słabości polityki państwa. Widoczną konsekwencją jest zahamowanie procesu budowania tożsamości nowych instytucji państwa demokratycznego*[4]. Jednocześnie z punktu widzenia demokratycznego społeczeństwa takie zjawisko tworzy niebezpieczną, destrukcyjną współzależność służb specjalnych z ośrodkiem politycznym. Polityczna legitymizacja działań służb balansujących na granicy prawa powoduje ich społeczną alienację i w konsekwencji może prowadzić do sytuacji, w której ośrodek decyzyjny stanie się zakładnikiem własnych działań w związku z potencjalnym usamodzielnieniem się instrumentów bezpieczeństwa.

W demokratycznej kontroli nad służbami specjalnymi oraz organami władzy wykonawczej nadzorującymi ich działanie szczególną rolę odgrywają organy władzy ustawodawczej, ze wskazaniem na jej część stanowiącą opozycję parlamentarną w stosunku do rządu. Ideę sporu, która jest charakterystyczna dla walki politycznej, w kontekście omawianej kontroli należy postrzegać jako element pozytywny, będący rękojmią przestrzegania standardów demokracji i pośrednio wpływający na ochronę praw i wolności obywatelskich przed nieuprawnioną ingerencją organów państwa. Oprócz legislatywy istotny wkład w mechanizm kontroli nad służbami specjalnymi i weryfikację realizowanego nad nimi nadzoru wnoszą również organy sądownictwa, których rola polega na udzielaniu tajnym służbom zgody na podejmowanie czynności specjalnych wobec obywateli oraz na osądzaniu ich ewentualnych nadużyć i przekroczeń prawa.

Bez względu na to, czy omawiane zagrożenia ładu społecznego mają swoje źródło wewnątrz służb specjalnych, czy też są inspirowane politycznym sporem, z punktu widzenia wartości społeczeństwa demokratycznego oraz ochrony konstytucyjnych praw i wolności jednostki są zjawiskiem patologicznym i niebezpiecznym. W demokratycznym państwie prawnym miarą skuteczności i efektywności służb specjalnych jest ich polityczna neutralność i bezstronność. Służby w swoich działaniach powinny kierować się wartościami ustrojowymi państwa, konstytucyjnymi normami oraz ustawowymi upoważnieniami, przy których realizacji funkcjonariusze służb powinni przestrzegać etyki zawodowej[5].

---

[3] M. Minkina, *Problemy badań nad wywiadem*, w: *Współczesne bezpieczeństwo polityczne*, S. Jaczyński, M. Kubiak, M. Minkina (red.), Warszawa–Siedlce 2012, s. 186.

[4] Z. Grzegorowski, *Instytucja „służby specjalne" a rzeczywistość funkcjonowania państwa polskiego*, „Studia Gdańskie. Wizje i rzeczywistość" 2010, t. 8, s. 58.

[5] M. Minkina, *Służby specjalne a (i) prawa obywatelskie*, w: *Bezpieczeństwo i prawa człowieka w teoriach*

Wymienione elementy nadzoru i kontroli nad służbami specjalnymi realizowane przez organy władzy wykonawczej, parlamentu i sądownictwa tworzą pewien spójny system kontrolny, który od przemian ustrojowych jest systematycznie rozwijany i udoskonalany. Otwarte pozostaje pytanie o praktykę stosowania przyjętych rozwiązań prawnych. Istotna rola w weryfikacji działania tego systemu przypada mediom, które przez nagłaśnianie nieprawidłowości w jego funkcjonowaniu kształtują w społeczeństwie obraz służb specjalnych oraz wyrażają presję wywieraną przez opinię publiczną na ośrodek władzy w celu wdrażania rozwiązań naprawczych.

Nadzór i kontrola sprawowane przez egzekutywę

W nadzorze władzy wykonawczej nad służbami specjalnymi materializuje się ten aspekt cywilnej i demokratycznej kontroli i nadzoru, który dotyczy optymalnego ukierunkowania celów służb na realizację interesów państwa przez bezwzględne podporządkowanie ich działań decyzjom egzekutywy. Odnosi się on również do bieżącej kontroli nad realizacją wyznaczonych celów, przy czym tę kontrolę należy oceniać w węższym ujęciu, przez pryzmat instrumentu nadzoru, który jest prowadzony przez organ władczy[6]. *Zasadniczym celem nadzorcy jest zapewnienie efektywnego funkcjonowania służb w określonych warunkach politycznych i prawnych tak, aby zapewniały wsparcie polityki państwa. Jest to zatem proces tworzenia takich warunków, w których poszczególne służby, podległe różnym decydentom, zostałyby objęte spójnym – odpowiadającym potrzebom bezpieczeństwa państwa – systemem dyrektyw oraz weryfikacji ich realizacji*[7].

Na świecie istnieje wiele rozwiązań dotyczących organizacyjnego podporządkowania służb i systemu ich nadzoru realizowanego przez organy egzekutywy. W Polsce od czasu zmian przyjętych w 1996 r. decydującą rolę w ukierunkowywaniu zadań, koordynacji działań służb specjalnych i nadzorze nad nimi powierzono Prezesowi Rady Ministrów. Szczególnie materializuje się ona w bezpośrednim podporządkowaniu szefów cywilnych służb specjalnych szefowi rządu[8]. Uprawnienia nadzorcze Prezesa Rady Ministrów wobec cywilnych służb specjalnych wynikają z przepisów ustawy o działach administracji rządowej[9], w myśl których nadzoruje on organy administracji rządowej nieujętej w zakresie działów administracji. Regulują je również ustawy kompetencyjne służb, których przepisy literalne mówią – w odniesieniu do szefów Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu – o podległości, a szefa Centralnego Biura Antykorupcyjnego – o nadzorze szefa rządu[10]. Z zapisów art. 3 ust. 2 ustawy o ABW oraz AW[11] i art. 5 ust. 2 ustawy o CBA[12] wynika stosunek podporządkowania szefów cywilnych służb specjalnych premierowi. Dotyczy to również szefa CBA, w którego

i praktyce społecznej początków XXI wieku, R. Rosa, R. Matysiuk (red.), Siedlce 2009, s. 287.

[6] Zob. S. Zalewski, *Służby specjalne w państwie*…, s. 116.

[7] Tamże.

[8] W 1996 r. był to szef Urzędu Ochrony Państwa, a obecnie szefowie Agencji Bezpieczeństwa Wewnętrznego, Agencji Wywiadu i Centralnego Biura Antykorupcyjnego.

[9] *Ustawa z dnia 4 września 1997 r. o działach administracji rządowej* (tekst jednolity: Dz.U. z 2016 r. poz. 543).

[10] M. Bożek, *Nadzór Prezesa Rady Ministrów nad służbami specjalnymi i sposoby jego realizacji w świetle obowiązującego ustawodawstwa,* „Przegląd Sejmowy" 2010, nr 3, s. 13.

[11] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (tekst jednolity: Dz.U. z 2016 r. poz. 1897).

[12] *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (tekst jednolity: Dz.U. z 2016 r. poz. 1319).

przypadku mowa jest expressis verbis o nadzorze, ale ponieważ Prezes Rady Ministrów jest władny wydawać wiążące wytyczne i polecenia kierownikom organów administracji rządowej nieujętej w działach[13], także w odniesieniu do szefa CBA można mówić o jego hierarchicznej podległości[14].

Ustawa kompetencyjna wojskowych służb specjalnych (Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego) przy określaniu organizacyjnego podporządkowania szefów służb wskazuje na ministra obrony narodowej[15]. W porównaniu z sytuacją prawną występującą przed reformą służb wojskowych w 2006 r. pozycja szefa rządu wobec tych służb została jednak znacznie wzmocniona. Do momentu rozwiązania Wojskowych Służb Informacyjnych bezpośredni wpływ premiera na ich działalność wynikał jedynie z pełnionej przez niego funkcji przewodniczącego Kolegium do Spraw Służb Specjalnych. Dopiero po rozwiązaniu tych służb oraz powołaniu SKW i SWW część kompetencji ministra obrony narodowej została ustawowo zastrzeżona dla Prezesa Rady Ministrów lub ministra koordynatora służb specjalnych (jeśli został powołany).

Do ustawowych prerogatyw szefa rządu w zakresie programowania i koordynowania działań służb specjalnych oraz nadzoru nad nimi należy:

- powoływanie i odwoływanie szefów służb (w odniesieniu do SKW i SWW – na wniosek ministra obrony narodowej),
- powoływanie i odwoływanie zastępców szefów służb na wniosek ich szefów (wobec zastępców szefów służb wojskowych leży to w kompetencjach szefa MON),
- określanie kierunków działania służb w drodze wytycznych (dla SKW i SWW wytyczne określone przez szefa MON zatwierdza premier),
- przyjmowanie corocznych sprawozdań szefów służb specjalnych z działalności podległych im instytucji za rok poprzedni (sprawozdania od szefów SKW i SWW premier otrzymuje równolegle z szefem MON),
- zapoznawanie się z planami działań na kolejny rok (służby wojskowe przedstawiają plany ministrowi obrony narodowej, który je zatwierdza), przedstawionymi przez szefów służb,
- wydawanie zgody szefom służb na podejmowanie współpracy z organami i służbami innych państw (przed wydaniem zgody dla szefów SKW i SWW premier zasięga opinii szefa MON),
- przewodniczenie Kolegium do Spraw Służb Specjalnych, organowi opiniodawczo-doradczemu Rady Ministrów,
- wydawanie wiążących wytycznych, żądanie informacji i opinii od szefów służb w celu koordynacji działań w dziedzinie bezpieczeństwa i obronności państwa (wobec SKW oraz SWW – za pośrednictwem szefa MON),
- żądanie od szefów służb informacji związanych z planowaniem i wykonaniem powierzonych zadań w celu zapewnienia wymaganego współdziałania służb (o żądaniu skierowanym do szefa SKW lub szefa SWW jednocześnie jest informowany minister obrony narodowej),
- określanie organizacji wewnętrznej służb przez nadanie statutu w drodze zarządzenia (statut służbom wojskowym jest nadawany przez szefa MON po uzyskaniu zgody premiera),

[13] *Ustawa z dnia 4 września 1997 r. o działach*…, art. 33a, ust. 1.

[14] M. Bożek, *Nadzór Prezesa Rady* Ministrów…, s. 14.

[15] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (tekst jednolity: Dz.U. z 2016 r. poz. 1318.), art. 3, ust. 2.

- wyrażanie lub odmowa zgody szefom służb na kontynuację prowadzenia sprawy będącej przedmiotem czynności operacyjno-rozpoznawczych, niepozostającej we właściwości danej służby,
- koordynowanie działalności służb specjalnych (ABW, AW, CBA, SKW, SWW)[16].

Ustawy kompetencyjne regulujące działalność cywilnych służb specjalnych upoważniają Prezesa Rady Ministrów do wydawania aktów wykonawczych określających szczegóły funkcjonowania i współpracy służb, jak choćby do określania w drodze rozporządzenia zasad i trybu szkolenia zawodowego funkcjonariuszy danej służby, wzorów legitymacji służbowych czy też – w drodze zarządzenia – zakresu i trybu współpracy służb oraz szczegółowego rozdziału ich kompetencji. Jeśli chodzi o służby wojskowe, większość prerogatyw do wydawania szczegółowych aktów wykonawczych jest scedowana na ministra obrony narodowej[17]. Niemniej jednak na ogólne zasady dotyczące ich funkcjonowania szef rządu ma istotny wpływ, wykraczający poza konstytucyjne uprawnienia do kierowania pracą Rady Ministrów[18], której członkiem jest szef MON. W ustawach kompetencyjnych Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego przewidziano udział Prezesa Rady Ministrów zarówno w podejmowaniu decyzji dotyczących obsady personalnej szefów tych służb, jak i związanych z programowaniem i oceną wykonania zadań przez służby, co daje mu realny wpływ na ich funkcjonowanie.

Wobec powyższego uprawniona jest konstatacja, że w wyniku reform przeprowadzonych w latach 1996, 2002 oraz 2006 decydująca rola w nadzorze i kontroli nad organami władzy wykonawczej nad służbami specjalnymi została przypisana Prezesowi Rady Ministrów. W świetle przepisów ustaw kompetencyjnych służb oraz ustawy o działach administracji rządowej szef rządu ma szerokie uprawnienia, na które składa się grupa środków pozwalająca mu na ukierunkowanie,a także na organizację pracy i współdziałania służb specjalnych oraz ich ocenę[19]. Otwartą kwestią pozostaje ocena realnych możliwości osobistego nadzoru Prezesa Rady Ministrów nad bieżącą pracą służb specjalnych wobec konieczności kierowania całością prac rządu. Pewnym rozwiązaniem tego problemu jest możliwość scedowania przez premiera części swoich uprawnień wobec służb specjalnych (szczególnie ABW, AW i CBA) na ministra koordynatora służb specjalnych.

Po raz pierwszy minister koordynator służb specjalnych został powołany w styczniu 1997 r., w trybie przewidzianym w art. 33 ust. 1 pkt 1 ustawy o Radzie Ministrów[20], w związku z reformą centrum administracyjnego. To stanowisko istniało w latach 1997–2001 oraz 2005–2007 i było zmieniane w ramach przewidzianych zadań i uprawnień. W pierwszym okresie dość obszernie został sformułowany zakres działalności ministra koordynatora, znacznie natomiast zostały ograniczone instrumenty pozwalające na efektywne realizowanie tej funkcji[21]. Formalna pozycja pierwszego ministra koordynatora w systemie organów odpowiedzialnych za bezpieczeństwo państwa wynikała z rozpo-

[16] Por. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa*…, art. 7, 8, 12, 13, 14, 20, 22a; *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze*…, art. 2, 5, 6, 11, 12; *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu*…, art. 7, 9, 13, 19, 21, 25.

[17] Tamże.

[18] *Konstytucja Rzeczypospolitej Polskiej z dnia 2 kwietnia 1997 r*. (Dz.U. z 1997 r. Nr 78 poz. 483, ze zm.), art. 148.

[19] M. Bożek, *Nadzór Prezesa Rady Ministrów*…, s. 34.

[20] *Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów* (tekst jednolity: Dz.U. z 2012 r. poz. 392, ze zm.).

[21] S. Zalewski, *Cywilna kontrola służb specjalnych w Polsce,* „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne", Warszawa 2010, s. 114.

rządzenia Prezesa Rady Ministrów i obejmowała wykonywanie zadań w zakresie programowania służb, oceny ich działalności, formułowania opinii na temat kandydatów na szefów oraz ogólnej kontroli[22]. Do kompetencji ministra koordynatora w pierwszym okresie istnienia stanowiska oprócz zadań planistyczno-legislacyjnych włączono realizację następujących czynności:

> (…)
> • wykonywanie z upoważnienia Prezesa RM czynności wynikających ze sprawowanej przez Prezesa RM funkcji nadzoru nad działalnością Szefa Urzędu Ochrony Państwa oraz związanych z odpowiedzialnością za działalność służb specjalnych, w tym:
> – przygotowywanie projektu wytycznych Prezesa RM w sprawie działalności służb specjalnych,
> – sprawowanie bieżącego nadzoru i koordynowanie działań służb specjalnych oraz podejmowanych w celu ochrony bezpieczeństwa państwa działań Policji, Straży Granicznej, Żandarmerii Wojskowej i innych jednostek,
> – przygotowywanie opinii o kandydatach na stanowiska Szefów Urzędu Ochrony Państwa, Szefa Wojskowych Służb Informacyjnych i ich zastępców,
> – przygotowywanie oceny stanu realizacji wytycznych Prezesa RM w sprawie działalności służb specjalnych,
> • wykonywanie i nadzorowanie zadań i misji specjalnych w dziedzinie bezpieczeństwa państwa, wyznaczonych przez Prezesa RM,
> • reprezentowanie Prezesa RM w kontaktach międzynarodowych związanych z działalnością służb specjalnych[23].

Porównanie zakresu kompetencji kolejnego ministra koordynatora, Janusza Pałubickiego, z uprawnieniami poprzednika nie wskazuje na żadną istotną zmianę, która mogłaby skutkować zwiększeniem możliwości kontrolnych. W dalszym ciągu rola ministra koncentrowała się na kontroli ogólnej, formułowaniu ocen, przygotowywaniu projektów oraz koordynacji działań służb[24]. Zasadnicza zmiana dotycząca działalności ministra koordynatora pojawiła się w latach 2006–2007. Rozporządzenie premiera Jarosława Kaczyńskiego dawało ówczesnemu koordynatorowi Zbigniewowi Wassermannowi wiele formalnych instrumentów stwarzających możliwość realnej kontroli całości działań służb specjalnych, w tym służb wojskowych. Zgodnie z tym rozporządzeniem minister koordynator został upoważniony do: wnioskowania o zastosowanie wobec służb prawnych środków nadzoru pozostających w gestii premiera, prowadzenia postępowań kontrolnych działań służb oraz oceny ich współdziałania z innymi podmiotami bezpieczeństwa państwa, a także rozpatrywania skarg na działania służb specjalnych[25]. Z punktu widzenia efektywności nadzoru i kontroli koordynatora szczególnie istotne było upoważnienie go przez Prezesa Rady Ministrów do żądania od szefów służb informacji, dokumentów i sprawozdań dotyczących szczegółów spraw realizowanych przez podległe im jednostki. Zakres przyznanych kompetencji wskazywał literalnie na możliwość żądania przez

[22] *Rozporządzenie Prezesa Rady Ministrów z dnia 13 stycznia 1997 r. w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów Zbigniewa Siemiątkowskiego* (Dz.U. z 1997 r. Nr 5 poz. 27).

[23] Tamże.

[24] Por. *Rozporządzenie Prezesa Rady Ministrów z dnia 7 listopada 1997 r. w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów Janusza Pałubickiego* (Dz.U. z 1997 r. Nr 136 poz. 924).

[25] S. Zalewski, *Cywilna kontrola*…, s. 118.

koordynatora dostępu do akt postępowań karnych oraz spraw operacyjnych. Dotyczyło to również obszaru działalności wojskowych służb specjalnych (WSI, a po likwidacji tej służby – SKW i SWW) i było obwarowane jedynie wymogiem poinformowania o takim żądaniu ministra obrony narodowej[26]. Decyzja premiera o przekazaniu ministrowi koordynatorowi tak szerokich prerogatyw była w okresie późniejszym kwestionowana przez sejmową Komisję do Spraw Służb Specjalnych (KSS) z powodu możliwości przekroczenia uprawnień, jednak zarzuty w tej sprawie nie zostały potwierdzone[27].

Po wyborach parlamentarnych i zmianie koalicji rządowej w 2007 r. premier Donald Tusk powołał na krótki okres Pawła Grasia na stanowisko pełnomocnika rządu ds. bezpieczeństwa i koordynatora służb specjalnych. Pozycja prawna tego organu nie została jasno sprecyzowana. Głównym zadaniem koordynatora było przeprowadzenie audytu działalności poprzednika[28]. W styczniu 2008 r. Paweł Graś złożył dymisję, a stanowisko zostało zlikwidowane[29]. Szef rządu objął służby specjalne osobistym nadzorem, a koordynację ich działalności powierzył sekretarzowi stanu w Kancelarii Premiera, który jednocześnie objął stanowisko sekretarza Kolegium do Spraw Służb Specjalnych[30]. W listopadzie 2011 r. Jacek Cichocki, który koordynował prace służb specjalnych, został powołany przez Prezesa Rady Ministrów na stanowisko ministra spraw wewnętrznych, łącząc je z dotychczasowymi obowiązkami. Jednocześnie szef rządu – w drodze rozporządzenia – przekazał ministrowi Cichockiemu swoje uprawnienia w zakresie nadzoru nad służbami. To rozwiązanie wytworzyło szczególną, niespotykaną dotychczas sytuację[31], w której ministrowi spraw wewnętrznych odpowiedzialnemu za pracę Policji, Straży Granicznej, Biura Ochrony Rządu i Straży Pożarnej powierzono jednocześnie realizowanie w imieniu premiera nadzoru nad wszystkimi służbami specjalnymi. Bez względu na celowość rozwiązania polegającego na koncentracji tak szerokiego zakresu kompetencji w ramach jednego podmiotu, otwarte pozostaje pytanie o możliwość efektywnej realizacji wynikających z nich zadań. Obowiązki ministra spraw wewnętrznych wobec służb podległych resortowi spraw wewnętrznych, przy uwzględnieniu ich liczby, mogły wpływać na obniżenie skuteczności nadzoru nad służbami specjalnymi. Dobrą stroną takiego rozwiązania była z pewnością lepsza koordynacja działań służb oraz organów pozostających w strukturze resortu spraw wewnętrznych, w przypadku podejmowania przez nie działań na rzecz ochrony bezpieczeństwa państwa. Oprócz obowiązków ministra wobec instytucji resortu spraw wewnętrznych, istotnym czynnikiem, który mógł mieć wpływ na skuteczność jego nadzoru nad służbami specjalnymi, był wysoki poziom ogólności upoważnienia szefa rządu.

---

[26] Zob. *Rozporządzenie Prezesa Rady Ministrów z dnia 3 sierpnia 2006 r. w sprawie szczegółowego zakresu działania Ministra – członka Rady Ministrów – Koordynatora Służb Specjalnych Zbigniewa Wassermana* (Dz.U. z 2006 r. Nr 141 poz. 998).

[27] Zob. S. Zalewski, *Cywilna kontrola*…, s. 120–121; *Kontrola w Kancelarii Premiera: Wassermann i Kaczyński nie złamali prawa*, „Gazeta Wyborcza" [online] z 26 czerwca 2008 r., http://wiadomosci.gazeta.pl/wiadomosci/1,114873,5399898,Kontrola_w_Kancelarii_Premiera__Wasserman_i_Kaczynski.html [dostęp: 13 III 2013].

[28] W. Czuchnowski, *Nowy rząd wyczyści specsłużby po PiS-ie,* „Gazeta Wyborcza" [online] z 25 października 2007 r., http://wyborcza.pl/1,85996,4610377.html [dostęp: 13 III 2013].

[29] W. Czuchnowski, D. Uhlig, *Dlaczego odszedł minister od służb?*, „Gazeta Wyborcza" [online] z 16 stycznia 2008 r., http://wyborcza.pl/dziennikarze/1,96017,4840844.html [dostęp: 13 III 2013].

[30] *Służby specjalne muszą być profesjonalne i apolityczne* [online], http://www.kprm.gov.pl/wydarzenia/aktualnosci/sluzby-specjalne-musza-byc-profesjonalne-i-apolityczne.htm [dostęp: 13 III 2013].

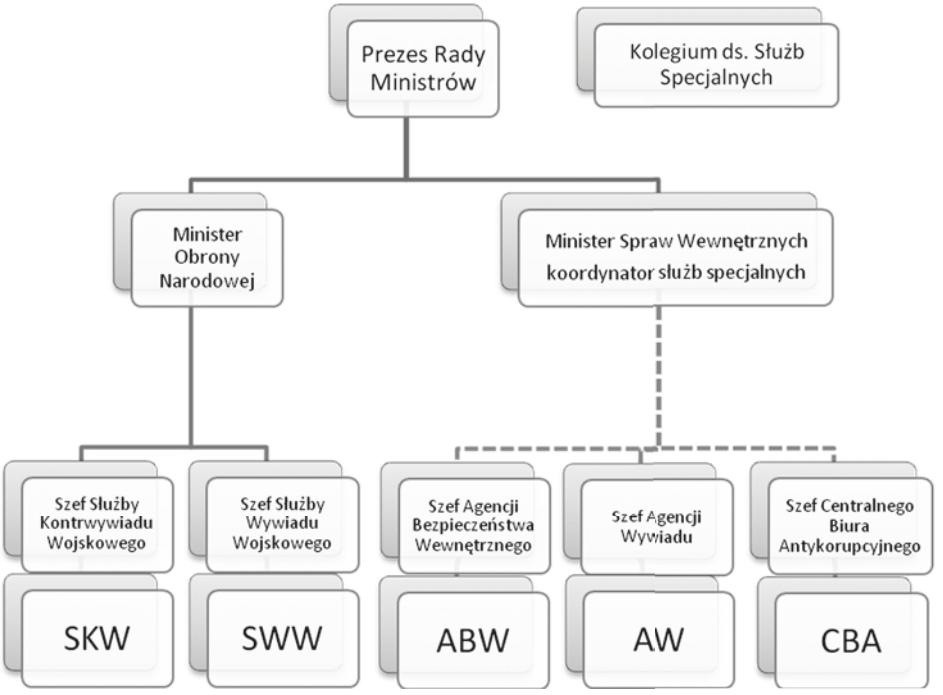
[31] Minister spraw wewnętrznych sprawował nadzór nad cywilną służbą specjalną, tj. Urzędem Ochrony Państwa, do 1996 r., natomiast służba wojskowa (Wojskowe Służby Informacyjne) podlega Ministrowi Obrony Narodowej.

Problemem wartym rozważenia jest upoważnienie ministra spraw wewnętrznych do żądania od (…) *szefów służb specjalnych informacji związanych z planowaniem i wykonywaniem powierzonych im zadań*[32]. Z cytowanego zapisu rozporządzenia Prezesa Rady Ministrów nie wynika jednoznacznie, jakich informacji mógł żądać minister. Czy w zakres żądania mogą wchodzić jedynie ogólne dane dotyczące pracy służb, czy również informacje dotyczące szczegółów ich działań śledczych i operacyjnych? Wobec zakazu przekazywania określonych informacji poza służby specjalne, co wynika z ich ustaw kompetencyjnych, ogólnikowość przepisu rozporządzenia zdecydowanie obniżała wartość narzędzi nadzorczych ministra spraw wewnętrznych.

W 2013 r., po rekonstrukcji rządu i zmianie obsady stanowiska szefa resortu spraw wewnętrznych, rozwiązania systemowe dotyczące koordynacji pracy służb specjalnych i nadzoru nad nimi oraz obszar upoważnienia do ich wykonywania pozostały w dotychczasowej formie. Oprócz wzmiankowanego żądania informacji, zakres zadań ministra spraw wewnętrznych obejmował: przygotowywanie aktów prawnych dotyczących działania służb, zapewnianie ich współdziałania, wyrażanie zgody na współpracę z organami i służbami zagranicznymi, zapoznawanie się z informacjami dostarczanymi przez służby, istotnymi dla bezpieczeństwa i międzynarodowej pozycji państwa, decydowanie o przekazywaniu tych informacji, a także realizację czynności związanych z podporządkowaniem służbowym szefów ABW, AW i CBA szefowi rządu, z wyłączeniem ich powoływania i odwoływania[33]. Analiza zakresu upoważnień przekazywanych ministrowi koordynatorowi przez Prezesa Rady Ministrów (szczególnie w latach 2006–2007) oraz zadań z zakresu koordynacji działań służb specjalnych i nadzoru nad nimi, scedowanych na ministra spraw wewnętrznych, prowadzi do konstatacji, że przeważa model zakładający ukierunkowanie ministra koordynatora sużb specjalnych jedynie na obszar działania służb. Rozwiązanie problemu skuteczności osobistego nadzoru premiera nad służbami specjalnymi, wobec konieczności kierowania ogółem spraw państwa, przez przekazanie tych obowiązków ministrowi odpowiedzialnemu za liczne organy resortu spraw wewnętrznych miało charakter połowiczny. Z punktu widzenia efektywności nadzoru władzy wykonawczej nad tak wyjątkową częścią administracji państwowej, jaką są służby specjalne, nie była to koncepcja modelowa.

[32] *Rozporządzenie Prezesa Rady Ministrów z dnia 24 listopada 2011 r. w sprawie szczegółowego zakresu działania Jacka Cichockiego – Ministra Spraw Wewnętrznych – w zakresie koordynacji służb specjalnych* (Dz.U. z 2011 r. Nr 254 poz. 1524).

[33] *Rozporządzenie Prezesa Rady z dnia 28 lutego 2013 r. w sprawie szczegółowego zakresu działania Bartłomieja Sienkiewicza – Ministra Spraw Wewnętrznych – w zakresie koordynacji służb specjalnych* (Dz.U. z 2013 r. poz. 272).



Wykres. System nadzoru egzekutywy nad służbami specjalnymi i koordynacji ich działań w latach 2011–2014.

Źródło: Opracowanie własne.

Jesienią 2014 r., po powołaniu nowego rządu, Prezes Rady Ministrów powrócił w sprawie nadzoru egzekutywy nad służbami specjalnymi do rozwiązania z lat 2008–2011. Część uprawnień premiera związanych z koordynowaniem działań służb specjalnych ponownie została scedowana na ministra Jacka Cichockiego, pełniącego jednocześnie funkcję szefa Kancelarii Prezesa Rady Ministrów. Analiza treści rozporządzenia szefa rządu w tej kwestii skłania do wniosku o kontynuowaniu dotychczasowych rozwiązań służących wsparciu premiera w nadzorze nad specsłużbami[34].

Zmiana rządu spowodowana werdyktem wyborczym z jesieni 2016 r. stała się przyczynkiem do kolejnej zmiany koncepcji prowadzenia nadzoru nad służbami specjalnymi przez egzekutywę. Sprowadza się ona do scedowania zasadniczej części prerogatyw i obowiązków szefa rządu na członka Rady Ministrów zajmującego się jedynie kontrolą i nadzorem nad służbami. Zakres zadań oraz uprawnień ministra – członka Rady Ministrów Mariusza Kamińskiego – koordynatora służb specjalnych, określony w rozporządzeniu Prezesa Rady Ministrów[35], wskazuje, że przyjęte obecnie rozwiązanie w kwestii kontroli i nad-

[34] Zob. *Rozporządzenie Prezesa Rady Ministrów z dnia 23 września 2014 r. w sprawie szczegółowego zakresu działania Ministra-Członka Rady Ministrów Jacka Cichockiego w zakresie koordynacji służb specjalnych* (Dz.U. z 2014 poz. 1276).

[35] Por. *Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra-Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych* (Dz.U. z 2015 poz. 1921).

zoru nad służbami przez władzę wykonawczą jest kontynuacją i rozwinięciem koncepcji z lat 2006–2007. Analiza treści rozporządzenia pozwala twierdzić, że wyczerpująco określono w nim zakres działalności ministra koordynatora i jednocześnie przyznano mu uprawnienia umożliwiające efektywne wykonywanie tej funkcji. Pozytywną stroną tego rozwiązania, oprócz wykreowania realnych instrumentów nadzoru i kontroli pracy służb specjalnych, jest również wytworzenie funkcjonalnego ogniwa koordynującego ich współdziałanie.

Dopełnienie systemu kontroli i nadzoru egzekutywy nad służbami specjalnymi stanowi działalność organu opiniodawczo-doradczego Rady Ministrów, jakim jest Kolegium do Spraw Służb Specjalnych. Funkcjonowanie tego kolegialnego organu nie jest rozwiązaniem nowatorskim, a potrzeba jego powołania wynikała między innymi z bezpośredniego podporządkowania w 1996 r. szefa Urzędu Ochrony Państwa Prezesowi Rady Ministrów i konieczności wsparcia nowych zadań premiera. Z pewnością działalność tego gremium ma niebagatelne znaczenie również w chwili obecnej, pomimo powołania członka Rady Ministrów, koordynatora służb specjalnych, i przekazania mu zadań premiera w odniesieniu do służb. Niemniej jednak zadania Kolegium nie sprowadzają się jedynie do udoskonalania nadzoru sprawowanego przez premiera lub ministra koordynatora nad służbami specjalnymi.

Kolegium do Spraw Służb Specjalnych zostało powołane na mocy nowelizacji ustawy o Urzędzie Ochrony Państwa z 8 sierpnia 1996 r.[36] w celu opiniodawczo-doradczego wsparcia Rady Ministrów w zakresie programowania, nadzoru nad służbami specjalnymi i koordynacji ich działań (wówczas UOP i WSI), a także Policji, Straży Granicznej oraz Żandarmerii Wojskowej, w przypadku podejmowanych przez nie czynności mających na celu ochronę bezpieczeństwa państwa[37]. Warto w tym miejscu zwrócić uwagę na obszar zainteresowania Kolegium wykraczający poza aktywność służb specjalnych, obejmujący ogół organów podejmujących działania na rzecz bezpieczeństwa państwa oraz uprawnionych do realizacji czynności operacyjno-rozpoznawczych. W związku z poszerzaniem obszarów zagrożeń bezpieczeństwa państwa oraz – będącym tego skutkiem – zwiększaniem liczby służb i instytucji podejmujących wysiłki na rzecz neutralizacji tych zagrożeń, zarówno podmiotowy, jak i przedmiotowy obszar działania Kolegium systematycznie wzrastał. Podmiotowy obszar zainteresowania Kolegium nie został ograniczony jedynie do kryterium podejmowania przez daną służbę czynności operacyjno-rozpoznawczych, ale obejmował także organy ukierunkowane na ochronę bezpieczeństwa państwa w wielu jego aspektach[38]. Istotny wpływ na zakres zadań oraz skład personalny Kolegium miały również zmiany systemowe w służbach specjalnych, skutkujące zwiększeniem liczby podmiotów określanych tym mianem – z dwóch w 1996 r. do pięciu w 2006 r.

Obecnie Kolegium do Spraw Służb Specjalnych działa na podstawie przepisów ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. Szczegóły dotyczące zakresu i trybu pracy tego gremium zostały uregulowane przepisami rozporządzenia Rady Ministrów[39]. Obszar działalności Kolegium – przy uwzględnieniu kryterium przedmiotowego i podmiotowego – obejmuje programowanie, nadzór nad służba-

[36] *Ustawa z dnia 8 sierpnia 1996 r. o zmianie niektórych ustaw normujących funkcjonowanie gospodarki i administracji publicznej* (Dz.U. z 1996 r. Nr 106 poz. 496, ze zm.).

[37] A. Żebrowski, *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej*, Kraków 2005, s. 212.

[38] S. Zalewski, *Cywilna kontrola*…, s. 112.

[39] *Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 r. w sprawie szczegółowego trybu i zasad funkcjonowania Kolegium do Spraw Służb Specjalnych oraz zakresu czynności sekretarza tego Kolegium,* (Dz.U. z 2002 r. Nr 103 poz. 929).

mi specjalnymi (ABW, AW, CBA, SKW, SWW), koordynowanie ich działalności oraz koordynowanie czynności podejmowanych na rzecz ochrony bezpieczeństwa państwa przez: Policję, Straż Graniczną, Żandarmerię Wojskową, Służbę Celną, Biuro Ochrony Rządu, Służbę Więzienną, izby skarbowe, urzędy skarbowe, organy kontroli skarbowej, organy informacji finansowej, a także służby rozpoznania Sił Zbrojnych RP[40]. Skład organu jest odzwierciedleniem obszaru jego zainteresowania. Pracom Kolegium przewodniczy Prezes Rady Ministrów. W posiedzeniach na prawach członków uczestniczą: sekretarz Kolegium, minister spraw wewnętrznych, minister obrony narodowej, minister spraw zagranicznych, minister finansów, szef Biura Bezpieczeństwa Narodowego oraz minister koordynator (jeśli został powołany). Pozostali uczestnicy prac Kolegium to szefowie służb specjalnych (ABW, AW, CBA, SKW, SWW) oraz przewodniczący Komisji do Spraw Służb Specjalnych. Prezydent Rzeczpospolitej jest uprawniony do wydelegowania do uczestnictwa w posiedzeniach tego organu swojego przedstawiciela[41], przewodniczący Kolegium natomiast może zapraszać do udziału w obradach inne osoby, których obecność jest konieczna ze względu na poruszaną tematykę. Przedmiotem prac Kolegium jest formułowanie ocen i wyrażanie uzgodnionego wcześniej stanowiska, które, jeśli nie osiągnięto konsensusu, jest podejmowane większością głosów w drodze głosowania[42]. Zakres tych prac dotyczy:

- powoływania i odwoływania szefów służb specjalnych,
- kierunków i planów działania służb,
- projektu budżetu w części dotyczącej służb specjalnych,
- projektów legislacji dotyczących służb specjalnych,
- wykonania przez służby zadań pod kątem zgodności z przyjętymi planami i kierunkami,
- oceny corocznych sprawozdań szefów z działań podległych im służb specjalnych,
- koordynowania działalności służb specjalnych z Policją, Strażą Graniczną, Żandarmerią Wojskową, Biurem Ochrony Rządu, Służbą Celną, urzędami skarbowymi, izbami skarbowymi, organami kontroli skarbowej, organami informacji finansowej i służbami rozpoznania Sił Zbrojnych RP w ochronie bezpieczeństwa państwa,
- współdziałania organów administracji publicznej ze służbami specjalnymi,
- współdziałania służb specjalnych z organami i służbami innych państw,
- organizowania wymiany informacji istotnych dla bezpieczeństwa i międzynarodowej pozycji państwa między organami administracji rządowej,
- ochrony informacji niejawnych[43].

Główny obszar działalności Kolegium koncentruje się na wsparciu Rady Ministrów przy wyznaczaniu kierunków działania służb specjalnych, ich funkcjonalnego zorganizowania, oceny ich działań pod kątem realizacji zaplanowanych zadań oraz koordynacji ich współpracy. Ponieważ jednak w systemie bezpieczeństwa oprócz nominalnych służb specjalnych funkcjonują także inne podmioty podejmujące działania na rzecz ochrony bezpieczeństwa państwa (w tym uprawnione do realizowania czynności operacyjno-rozpoznawczych), na istotę pracy tego gremium wpływa również koordynacja działań

[40] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa*…, art. 11.

[41] S. Zalewski, *Cywilna kontrola*…, s. 112.

[42] *Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 r. w sprawie szczegółowego trybu i zasad funkcjonowania Kolegium*…, § 6 ust. 2.

[43] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa*…, art. 12.

tych podmiotów ze służbami specjalnymi. Szczególnie ważny element tej koordynacji jest związany z wymianą danych na temat zagrożeń dotyczących bezpieczeństwa państwa. *Świadczy to o poszerzeniu zapotrzebowania na informacje nie tylko dla władzy wykonawczej, ale i ustawodawczej.* (…) *Rola koordynatora materializuje się w sferze informacyjnej, co w istotny sposób ułatwia wydanie opinii i rekomendacji dla Prezesa Rady Ministrów* (…) *oraz sprzyja zwiększeniu efektywności działań Kolegium do Spraw Służb Specjalnych*[44]. Warto również wspomnieć o przejęciu przez Kolegium zadań związanych ze sferą ochrony informacji niejawnych, które do 2001 r. były realizowane przez Komitet Ochrony Informacji Niejawnych.

Wobec dużej liczby służb i instytucji pozostających w kręgu zainteresowań Kolegium oraz obszernego zakresu przedmiotowego jego działania, uprawnione jest twierdzenie, że ten podmiot jest istotnym i trwałym elementem systemu cywilnej i demokratycznej kontroli nad służbami realizującymi zadania w zakresie bezpieczeństwa państwa. Jego działalność materializuje się we wsparciu decyzyjno-informacyjnym Rady Ministrów i premiera dotyczącym funkcjonowania instytucji ochrony bezpieczeństwa państwa, w tym szczególnie służb specjalnych. Wobec wzrostu liczby podmiotów państwowych, które są uprawnione do realizowania czynności operacyjno-rozpoznawczych, szeroki zakres podmiotowy działania Kolegium pozwala na sformułowanie poglądu o jego nowoczesnym charakterze uwzględniającym zmiany zagrożeń bezpieczeństwa państwa oraz zmiany w organizacji systemu mającego je neutralizować.

Uprawnienia kontrolne władzy ustawodawczej

Służby specjalne są szczególnym instrumentem bezpieczeństwa pozostającym w dyspozycji Rady Ministrów, która w myśl postanowień Konstytucji Rzeczpospolitej Polskiej odpowiada za zapewnienie bezpieczeństwa wewnętrznego i zewnętrznego państwa[45]. Na równi z innymi organami władzy publicznej działają na zasadzie praworządności, zgodnie z którą zostały określone zarówno prawne podstawy ich działania, jak i wyznaczone granice kompetencji[46]. Wyjątkowo istotnego znaczenia nabiera ta zasada wobec działań służb specjalnych, których credo stanowi niejawne działanie decydujące o ich wyjątkowości, ale i czyniące z nich podmiot z natury trudny do kontroli oraz wkraczający w obszar praw i wolności jednostki. Rola władzy ustawodawczej w tworzeniu mechanizmów skutecznego nadzorowania tajnych służb i kontroli nad nimi zarysowuje się już na etapie procesu legislacji. Jest ona pochodną funkcji ustawodawczej parlamentu i chociaż nie można jej traktować jako kontroli sensu stricto, prawne podstawy funkcjonowania służb specjalnych ustanawiane przez sejm RP określają jednocześnie ramy systemu nadzoru i kontroli nad nimi. Nie mogą one jednak być sprzeczne z ustawą zasadniczą lub odbiegać od międzynarodowych standardów w zakresie ochrony praw i wolności obywatelskich[47].

Udział władzy ustawodawczej usytuowany w obszarze wykonawczym cywilnej i demokratycznej kontroli nad służbami specjalnymi materializuje się w sposób szcze-

[44] M. Kucharski, *Rządowe organy konsultacyjno-doradcze*, w: *Instytucje bezpieczeństwa narodowego*, M. Paździor, B. Szmulik (red.), Warszawa 2012, s. 77.

[45] *Konstytucja Rzeczypospolitej Polskiej*…, art. 146 ust. 4 pkt 7, 8.

[46] Tamże, art. 7.

[47] J. Jaskiernia, *Bezpieczeństwo państwa a ochrona praw i wolności jednostki*, w: *Świat wobec współczesnych wyzwań i zagrożeń*, J. Simonides (red.), Warszawa 2010, s. 286.

gólny w działaniach organu sejmu, jakim jest Komisja do Spraw Służb Specjalnych. Działalność Komisji ma charakter stały i oprócz powoływanych doraźnie sejmowych komisji śledczych do zbadania zgodności z prawem konkretnych działań tajnych służb, jest istotnym instrumentem funkcji kontrolnej parlamentu[48]. Należy przy tym nadmienić, że kontrola prowadzona przez władzę ustawodawczą nie ogranicza się jedynie do ochrony wolności i praw obywatelskich, ale trzeba ją rozpatrywać w szerokim kontekście ochrony wartości i standardów państwa demokratycznego. Ta ochrona materializuje się również w parlamentarnej kontroli władzy wykonawczej, której szczególnym instrumentem są służby specjalne. Właśnie ze względu na tę szczególność – związaną z tajnym charakterem działalności, która jednocześnie decyduje o skuteczności służb – w przypadku kontroli nad nimi niemożliwe jest zastosowanie ogólnych demokratycznych reguł kontrolnych, jak choćby prawa obywateli do informacji publicznej[49]. Uprawnione jest więc twierdzenie, że specjalne, wyodrębnione organy władzy ustawodawczej właściwe w sprawach kontroli specsłużb, to jeden z podstawowych elementów niezależnej weryfikacji ich funkcjonowania w praktyce, ze wskazaniem na szczególną rolę ich części wyłonionej z parlamentarnej opozycji.

Już w okresie zimnej wojny, w latach 60. XX w., w krajach Europy Zachodniej wytworzyła się praktyka powoływania organów będących instrumentami parlamentarnej kontroli nad służbami specjalnymi[50]. Z reguły te instrumenty przybierają postać parlamentarnych komisji, ich kompetencje w poszczególnych krajach bywają jednak znacznie zróżnicowanie. W Republice Federalnej Niemiec jedenastoosobowa parlamentarna Komisja ds. Kontroli Służb Specjalnych jest powoływana spośród deputowanych do Bundestagu, a do katalogu jej uprawnień należy zapoznawanie się z informacjami na temat całokształtu funkcjonowania służb, w tym ze szczegółami dotyczącymi zakresu i metod ich działania, również tych dotyczących technik operacyjnych[51]. We Włoszech natomiast komisja parlamentarna nie może żądać informacji na temat szczegółów operacji prowadzonych w danym momencie[52].

W Polsce instytucjonalnym pierwowzorem organów związanych z parlamentarną kontrolą funkcjonowania służb specjalnych była podkomisja stała do spraw kontroli nad służbami specjalnymi powołana w 1991 r. przez Sejm X kadencji[53]. Jednym z wyników jej prac był postulat powołania stałej komisji sejmowej, która mogłaby w sposób bardziej efektywny sprawować kontrolę nad służbami[54]. W toku prac Sejmu II kadencji[55] intensyfikowano działania w kierunku powołania sejmowej komisji o charakterze odmiennym od pozostałych kontrolnych organów parlamentu z uwagi na delikatny i obarczony klauzulą tajności obszar jej funkcjonowania. Na początku lat 90. XX w. transformacja ustrojowa ukierunkowana na wprowadzanie w Polsce standardów demokracji wymusiła stworzenie skutecznego mechanizmu kontroli parlamentu

[48] Tamże.

[49] J. Jaskiernia, *Demokratyczna kontrola nad służbami specjalnymi a problem ochrony praw i wolności jednostki*, w: *Współczesne wyzwania wobec praw człowieka w świetle polskiego prawa konstytucyjnego*, Z. Kędzia, A. Rost (red.), Poznań 2009, s. 43.

[50] Tenże, *Bezpieczeństwo państwa*…, s. 287.

[51] J. Gawryszewski, *Służby specjalne w Republice Federalnej Niemiec*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 6, s. 15.

[52] J. Jaskiernia, *Demokratyczna kontrola*…, s. 42.

[53] Lata 1989–1991 (przyp. red.).

[54] S. Zalewski, *Służby specjalne. Programowanie, nadzór, koordynacja*, Warszawa 2003, s. 7.

[55] Lata 1993–1997 (przyp. red.).

nad działalnością organów władzy wykonawczej. Szczególnie ważną i delikatną częścią tego systemu były instrumenty kontrolne legislatywy nad instytucjami wykonującymi zadania o charakterze tajnym podległymi egzekutywie[56]. Powołanie organu kontrolnego sejmu było podyktowane koniecznością dostosowania rozwiązań krajowych do norm obowiązujących w krajach o utrwalonej demokracji.

Analiza czasu przygotowań do powołania Komisji do Spraw Służb Specjalnych oraz jej ostateczne powstanie w 1995 r. wskazuje na jej praktyczne wykorzystanie także przez organy władzy wykonawczej. Działający od 1993 r. rząd, wyłoniony z parlamentarnej koalicji Sojuszu Lewicy Demokratycznej i Polskiego Stronnictwa Ludowego, w myśl przepisów tzw. małej konstytucji był pozbawiony realnych instrumentów kontroli nad służbami specjalnymi. Było to spowodowane poddaniem służb specjalnych, tj. Urzędu Ochrony Państwa i Wojskowych Służb Informacyjnych, pod nadzór odpowiednio ministra spraw wewnętrznych i ministra obrony narodowej, którzy działali w formule tzw. resortów prezydenckich. Powołanie sejmowej Komisji do Spraw Służb Specjalnych dawało koalicji rządowej możliwość osiągnięcia pośredniego wpływu – przez koalicyjnych posłów wchodzących w skład Komisji – na funkcjonowanie specsłużb[57]. Bez względu na inspiracje towarzyszące powołaniu KSS w sejmie do chwili obecnej tworzy ona jeden z filarów cywilnej i demokratycznej kontroli niejawnych instrumentów będących w dyspozycji władzy wykonawczej.

Podstawą prawną funkcjonowania KSS jest *Regulamin Sejmu*[58], szczególnie jego rozdział 12, który jest poświęcony wyłącznie działaniu i organizacji KSS. Formalnie rzecz ujmując, Komisja jest jednym ze stałych kolegialnych organów sejmu. W literaturze można spotkać pewną doktrynalną kwalifikację określającą to gremium – podobnie jak inne komisje sejmowe – jako organ wewnętrzny i pomocniczy Izby Poselskiej[59]. Zważywszy jednak na szczególny charakter KSS wynikający z prawnych powinności innych podmiotów wobec Komisji, a nie sejmu jako całości, oraz to, że część jej decyzji jest definitywna i ostateczna, bardziej uprawnione jest mówienie o KSS jako szczególnym organie sejmu posiadającym kompetencje zewnętrzne[60].

Przedmiotowy zakres działania KSS jest określony w załączniku do wspomnianego *Regulaminu Sejmu*. Może być on klasyfikowany w trzech zasadniczych obszarach: legislacyjnym, opiniodawczym i kontrolnym[61]. W obszarze legislacyjnym można identyfikować zadania KSS związane z:

- opiniowaniem projektów ustaw, rozporządzeń, zarządzeń oraz innych aktów normatywnych dotyczących służb specjalnych, w tym regulujących działalność tych służb,
- opiniowaniem projektu budżetu w zakresie dotyczącym służb specjalnych;

w obszarze opiniodawczym,

---

[56] J. Szymanek, *Organy parlamentarne właściwe w sprawach bezpieczeństwa i porządku publicznego*, w: *Instytucje bezpieczeństwa narodowego,* M. Paździor, B. Szmulik (red.), Warszawa 2012, s. 43.

[57] A. Mróz, H. Pajdała, *Komisja do Spraw Służb Specjalnych – uwagi na tle dotychczasowego funkcjonowania*, „Przegląd Sejmowy" 2004, nr 5, s. 74.

[58] *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r. Regulamin Sejmu Rzeczypospolitej Polskiej*, *załącznik – Przedmiotowy zakres działania komisji sejmowych* (tekst jednolity: M.P. z 2012 r. poz. 32, ze zm.).

[59] Tamże, s. 78.

[60] J. Szymanek, *Organy parlamentarne*..., s. 50–51.

[61] P. Radziewicz, *Uprawnienia, środki działania oraz prawne podstawy funkcjonowania sejmowej Komisji do Spraw Służb Specjalnych*, „Przegląd Legislacyjny" 2006, nr 2, s. 29.

- opiniowaniem wniosków w sprawie powołania i odwołania poszczególnych osób na stanowiska szefów służb specjalnych i ich zastępców,
- opiniowaniem kierunków działań i rozpatrywaniem corocznych sprawozdań szefów służb specjalnych.

Zadania kontrolne natomiast są związane z:

- rozpatrywaniem corocznego sprawozdania z wykonania budżetu służb specjalnych oraz innych informacji finansowych służb specjalnych,
- zapoznawaniem się z informacjami służb specjalnych o szczególnie istotnych wydarzeniach z ich działalności, w tym dotyczących podejrzeń występowania nieprawidłowości w ich funkcjonowaniu oraz podejrzeń naruszenia przez nie prawa, przez dostęp i wgląd do informacji, materiałów i dokumentów uzyskanych w wyniku wykonywania ustawowych zadań, zgodnie z ustawą o ochronie informacji niejawnych[62] oraz ustaw regulujących działalność służb specjalnych,
- oceną współdziałania służb specjalnych z innymi organami, służbami oraz instytucjami uprawnionymi do wykonywania czynności operacyjno-rozpoznawczych w zakresie działań podejmowanych przez nie na rzecz bezpieczeństwa państwa,
- oceną współdziałania służb specjalnych z siłami zbrojnymi, organami administracji rządowej, organami ścigania i innymi instytucjami państwowymi i jednostkami samorządu terytorialnego oraz właściwymi organami i służbami specjalnymi innych państw,
- oceną ochrony informacji niejawnych oraz badaniem skarg dotyczących działalności służb specjalnych[63].

W skład Komisji wchodzi obecnie siedmiu posłów, ta liczba jednak nie ma charakteru wiążącego, a określa jedynie maksymalną granicę. Skład Komisji, na wniosek prezydium, jest ustalany przez sejm w drodze uchwały na początku każdej nowej kadencji. Ideą takiego rozwiązania jest możliwie proporcjonalne uchwycenie w składzie Komisji reprezentacji klubów poselskich obecnych w sejmie[64]. Marszałek sejmu przyjmuje zgłoszenia kandydatów na członków Komisji od przewodniczących klubów poselskich lub grupy co najmniej 35 posłów. Wybór członków KSS jest dokonywany spośród kandydujących posłów w głosowaniu łącznym izby[65].

W literaturze przedmiotu można się spotkać z twierdzeniem o nieingerencji marszałka sejmu w weryfikację kandydatów na członków KSS[66]. W argumentacji przywołuje się treść art. 137 ust. 4 *Regulaminu Sejmu*, zgodnie z którym wybór składu Komisji przez sejm następuje na wniosek Prezydium Sejmu po uzyskaniu opinii Konwentu Seniorów. Taki pogląd wydaje się nieuzasadniony z uwagi na to, że marszałek sejmu, oprócz wicemarszałków desygnowanych przez kluby parlamentarne, wchodzi w skład Prezydium Sejmu. Praktyką sejmową jest powierzanie stanowiska marszałka posłowi pochodzącemu z ugrupowania politycznego, które uzyskało najwyższy wynik wyborczy, a stanowisk wicemarszałków – przedstawicielom klubów koalicji[67]. Ta sytuacja daje

[62] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (tekst jednolity: Dz.U. z 2016 r. poz. 1167).

[63] *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r.…*, załącznik – *Przedmiotowy zakres działania komisji sejmowych*, pkt 2.

[64] M. Zubik, *Organizacja wewnętrzna Sejmu Rzeczypospolitej Polskiej*, Warszawa 2003, s. 282.

[65] J. Szymanek, *Organy parlamentarne*..., s. 46.

[66] Tamże.

[67] Skład Prezydium Sejmu VII kadencji stanowiło trzech posłów koalicji oraz dwóch opozycji i jeden niezrzeszony, http://www.sejm.gov.pl/Sejm7.nsf/page/prezydium_sejmu [dostęp: 12 III 2012].

marszałkowi sejmu możliwość weryfikacji kandydatów na członków KSS przez niezgłoszenie ich do głosowania, co znajdowało zastosowanie w praktyce[68]. Jeżeli jeszcze dodać, że uchwały KSS są podejmowane bezwzględną większością głosów przy obecności co najmniej połowy członków, a jej posiedzenia mają charakter niejawny[69], to przy założeniu wewnętrznej spójności koalicji sprawującej władzę, uprawniony wydaje się wniosek o ograniczonym wpływie posłów opozycji na ostateczne wyniki pracy kontrolnej tego sejmowego organu.

Dość osobliwą sytuację powoduje wymóg posiadania przez członków KSS poświadczeń bezpieczeństwa osobowego dających im możliwość zapoznawania się z informacjami klasyfikowanymi jako niejawne o klauzuli „ściśle tajne". Zgodnie z przepisami ustawy o ochronie informacji niejawnych poszerzone postępowanie sprawdzające osób ubiegających się o tzw. certyfikat bezpieczeństwa prowadzi Agencja Bezpieczeństwa Wewnętrznego[70]. Jednocześnie ABW znajduje się w zakresie działania przedmiotowego Komisji. To prowadzi do kuriozalnej sytuacji, w której instytucja podlegająca kontroli ma wpływ na obsadę organu kontrolującego przez hipotetyczną możliwość odmowy wydania poświadczenia bezpieczeństwa posłowi będącemu jego członkiem lub kandydatem na członka[71].

Istotą działania kontrolnego KSS jest zakres jej zadań związanych z zapoznawaniem się z informacjami służb specjalnych o szczególnie ważnych wydarzeniach z ich działalności, w tym dotyczących występowania nieprawidłowości oraz podejrzeń naruszenia przez nie prawa. Komisja jest uprawniona do (…) *dostępu i wglądu do informacji, dokumentów i materiałów uzyskanych w wyniku wykonania zadań ustawowych służb*[72], z czego wynika teoretyczna możliwość żądania informacji dotyczących również pracy operacyjnej. Osoby z kierownictwa tych instytucji na żądanie KSS mają obowiązek brać udział w posiedzeniach Komisji oraz udzielać jej członkom informacji i wyjaśnień[73]. Problem w dostępie KSS do wszystkich materiałów i dokumentów służb stwarza zapis w załączniku do *Regulaminu Sejmu*, zgodnie z którym zasady ich przekazywania wynikają z ustawy o ochronie informacji niejawnych oraz z ustaw regulujących ich działalność[74]. Na gruncie przepisów ustaw o specsłużbach ich szefowie mogą decydować o przekazaniu informacji, materiałów i dokumentów zawierających informacje niejawne określonej osobie lub instytucji (w tym KSS), jednak z wyłączeniem informacji dotyczących szczegółów pracy operacyjnej[75]. Ustawy kompetencyjne służb nie przewidują dla KSS drogi odwoławczej od takiej decyzji. Jedynie w razie odmowy udzielenia tego typu informacji na żądanie sądu lub prokuratora (jeśli jest to związane ze ściganiem sprawców określonej kategorii przestępstw) decyzje szefów służb podlegają weryfikacji przez Pierwszego Prezesa Sądu Najwyższego, którego werdykt jest dla nich wiążący[76].

---

[68] *„Nie" dla Macierewicza w komisji ds. służb specjalnych* [online], http://wiadomosci.onet.pl/kraj/nie-dla-macierewicza-w-komisji-ds-sluzb-specjalnyc,1,4213666,wiadomosc.html [dostęp: 12 III 2013].

[69] *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r.*…, art. 138, 139.

[70] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*…, art. 10, ust. 3.

[71] J. Szymanek, *Organy parlamentarne*..., s. 47.

[72] *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r.*…, *załącznik*…, pkt 2.

[73] M. Bożek, *Służby specjalne poza kontrolą Sejmu* [online], http://lubczasopismo.salon24.pl/dziennika-rzesledczy/post/322458,sluzby-specjalne-poza-kontrola-sejmu [dostęp: 12 III 2013].

[74] *Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r.*…, *załącznik*… pkt 2.

[75] Zob. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa*…, art. 39; *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu*…, art. 43; *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze*…, art. 28.

[76] Tamże.

To oznacza ograniczenie uprawnień przynależnych Komisji, o których mowa w *Regulaminie Sejmu*, i, co za tym idzie, spadek skuteczności kontroli parlamentarnej. Również zapis w ustawach kompetencyjnych służb specjalnych mówiący o poddaniu ich szefów kontroli sejmu, przy jednoczesnym braku sprecyzowania ich obowiązków wobec parlamentu oraz zasad i trybu, w jakim kontrola ma się odbywać, ma charakter wyłącznie symboliczny. Wobec szefów tych podmiotów sejm nie jest w stanie egzekwować odpowiedzialności politycznej, ponieważ nie są oni członkami Rady Ministrów. Ocenie parlamentu mogą podlegać jedynie członkowie rządu sprawujący nad nimi nadzór (Prezes Rady Ministrów, minister obrony narodowej). Teoretycznie, wobec złej oceny tego nadzoru, sejm może doprowadzić do dymisji osób go sprawujących, ale w praktyce posłowie koalicji nie udzielają poparcia takim wnioskom, ponieważ te osoby tworzą zaplecze polityczne rządu[77]. Powyższe uwagi prowadzą do konstatacji o znacznym ograniczeniu realnych możliwości kontrolnych legislatywy wobec niejawnych instrumentów bezpieczeństwa pozostających w dyspozycji rządu. Sposobem na poprawę tego stanu nie może być całkowita transparentność specsłużb i poddawanie publicznej ocenie każdego obszaru ich aktywności. Istnieje natomiast pilna potrzeba poszukiwania rozwiązań stwarzających możliwość efektywnej i obiektywnej kontroli parlamentarnej nad służbami specjalnymi i nadzoru realizowanego nad nimi przez władzę wykonawczą, przy uwzględnieniu ochrony niejawności ich działania.

W kontroli władzy ustawodawczej nad służbami specjalnymi należy uwzględnić również pośrednią rolę sejmu wynikającą z jego funkcji kreacyjnej. Wpływ izby poselskiej na system cywilnej i demokratycznej kontroli tych podmiotów materializuje się przez wybór Rzecznika Praw Obywatelskich, prezesa Najwyższej Izby Kontroli oraz sędziów wchodzących w skład Trybunału Konstytucyjnego.

Rolą Rzecznika Praw Obywatelskich jest ochrona wolności i praw człowieka i obywatela, które są gwarantowane przez Konstytucję RP oraz inne akty normatywne[78]. W związku ze stosowaniem niejawnego instrumentarium służb specjalnych prawa i wolności obywatelskie z natury rzeczy mogą być naruszane, dlatego też działalność Rzecznika jest ważnym elementem ich ochrony. Może on wnioskować o dostęp do materiałów i informacji dotyczących okoliczności, w których te prawa mogły być złamane, oraz wnioskować do służb specjalnych o przedstawienie ustaleń i wyjaśnień w omawianej kwestii[79]. W związku z tym, że Rzecznik Praw Obywatelskich w swojej działalności jest niezależny i niezawisły od innych organów państwowych i odpowiada tylko przed sejmem, można go postrzegać jako istotny organ systemu cywilnej, demokratycznej kontroli nad służbami specjalnymi. Potwierdzeniem tej tezy jest również możliwość kierowania przez niego wniosków o zbadanie zgodności z Konstytucją ustaw i przepisów prawa wydawanych przez centralne organy państwowe do Trybunału Konstytucyjnego[80].

Członkowie Trybunału Konstytucyjnego są wybierani przez sejm na dziewięcioletnią kadencję, w wykonywaniu swojego urzędu są niezawiśli, a orzeczenia TK podejmowane większością głosów mają moc powszechnie obowiązującą i są ostateczne[81]. Orzecznictwo TK jest niezwykle ważnym elementem demokratycznego państwa praw-

[77] M. Bożek, *Służby specjalne poza…*
[78] *Konstytucja Rzeczypospolitej Polskiej*…, art. 208.
[79] A. Żebrowski, *Ewolucja polskich służb*…, s. 219.
[80] *Konstytucja Rzeczypospolitej Polskiej*…, art. 188.
[81] Tamże, art. 194, 195, 190.

nego, ponieważ w jego skład wchodzą niezależne autorytety prawnicze dające rękojmię rzetelności i bezstronności. Ustawy regulujące działanie służb specjalnych oraz szczegółowe akty wykonawcze dotyczące funkcjonowania tych służb podlegają ocenie TK pod względem zgodności z ustawą zasadniczą, w tym z przepisami dotyczącymi ochrony praw i wolności obywatelskich[82]. Jest to o tyle ważne, że konstytucyjne ograniczenia swobód obywatelskich ustanawiane w celu zapewnienia bezpieczeństwa państwa nie mogą naruszać ich istoty[83]. Wiążące orzecznictwo Trybunału Konstytucyjnego w tej kwestii to ważny wkład w system cywilnej i demokratycznej kontroli nad służbami specjalnymi. Materializuje się on na etapie tworzenia prawa regulującego działanie tych podmiotów przez jego weryfikację pod względem konstytucyjności. Występuje również w fazie wykonywania, ponieważ orzeczenie TK o niezgodności z Konstytucją przepisów prawa, na mocy których orzeczenie sądowe lub ostateczna decyzja administracyjna zostały wydane, jest podstawą do ich wznowienia lub uchylenia[84].

Służby specjalne na równi z pozostałymi instytucjami demokratycznego państwa podlegają ocenie naczelnego organu kontroli państwowej, jakim jest Najwyższa Izba Kontroli[85]. Ten organ podlega sejmowi i przedstawia izbie poselskiej sprawozdania ze swojej działalności oraz informuje o wynikach przeprowadzanych kontroli, które są dokonywane pod kątem legalności, gospodarności, celowości i rzetelności[86]. Taka kontrola jest prowadzona również w służbach specjalnych, ale nie jest ona ukierunkowana na badanie operacyjnego aspektu ich pracy. Dotyczy ona obszaru finansowo-gospodarczego działalności tych podmiotów i jest prowadzona przez kontrolerów upoważnionych przez prezesa NIK[87]. W przypadku stwierdzenia nieprawidłowości lub naruszeń prawa Izba nie ma jednak uprawnień do prowadzenia postępowań przygotowawczych. W strukturze NIK brakuje pionu prokuratorskiego, co znacznie osłabia efektywność jej działania[88].

Zakres uprawnień kontrolnych władzy sądowniczej

Podstawowymi wartościami chronionymi w warunkach funkcjonowania demokracji konstytucyjnych są prawa i wolności obywatelskie. Zgodnie z Konstytucją RP ich ograniczenia mogą być wprowadzane tylko w drodze ustawy, gdy są konieczne do ochrony bezpieczeństwa państwa lub porządku publicznego. Wspomniana dyspozycja konstytucyjna w szczególny sposób wiąże się z niejawną prakseologią pracy służb specjalnych, która a priori zakłada ingerencję w obszar konstytucyjnych praw i wolności jednostki. W szczególny sposób naruszenia swobód obywatelskich materializują się w części czynności operacyjno-rozpoznawczych związanych z realizacją tzw. kontroli operacyjnej polegającej na sprawdzaniu treści korespondencji, zawartości przesyłek oraz

[82] Orzeczenie Trybunału Konstytucyjnego dotyczące niezgodności z Konstytucją RP zapisów ustawy o ABW i AW dotyczących mianowania Szefów ABW i AW w randze sekretarzy stanu, sposobu prawnego uregulowania obserwacji i rejestracji zdarzeń przy użyciu środków technicznych oraz arbitralnego wypowiedzenia stosunku służbowego funkcjonariuszom ABW lub AW spowodowało konieczność zmiany wzmiankowanych przepisów, zob. *Wyrok Trybunału Konstytucyjnego z dnia 20 kwietnia 2004 r. sygn. akt K 45/02*, (Dz.U. z 2004 r. Nr 109 poz. 1159).

[83] *Konstytucja Rzeczypospolitej Polskiej*…, art. 31.

[84] Tamże, art. 190 ust. 4.

[85] S. Zalewski, *Służby specjalne w państwie*…, s.118.

[86] *Konstytucja Rzeczypospolitej Polskiej*…, art. 203, 204.

[87] M. Grzybowski, A. Żebrowski, *Kontrola władzy ustawodawczej i wykonawczej nad służbami specjalnymi (zagadnienia podstawowe)*, Kraków 1999, s. 56.

[88] R. Pieja, *Przewodnik po cywilnych służbach specjalnych. Od UB do ABW*, Mikołów 2011, s. 62.

stosowaniu środków technicznych do niejawnego pozyskiwania i rejestrowania informacji oraz dowodów, w tym rozmów telefonicznych i innych informacji przekazywanych przez sieci telekomunikacyjne[89].

Działania podejmowane w ramach kontroli operacyjnej dotykają obszaru praw i wolności obywatelskich określonych w art. 47 Konstytucji, w którym jest mowa o prawnej ochronie życia prywatnego obywateli, oraz w art. 49, z którego wynika prawo obywateli do wolności i ochrony tajemnicy komunikowania się. Zgodnie z dyspozycją art. 31 Konstytucji, ograniczenia praw i wolności w wymienionych obszarach związane z podejmowaniem przez służby specjalne działań niejawnych są usankcjonowane przepisami ich ustaw kompetencyjnych. Z punktu widzenia przepisów Konstytucji sytuacja jest klarowna, problemem natomiast jest praktyka weryfikacji konieczności wykorzystania części ich niejawnego instrumentarium. W tym właśnie aspekcie działania służb specjalnych materializuje się zasadniczy udział władzy sądowniczej w systemie ich cywilnej i demokratycznej kontroli.

Do czasu reformy służb specjalnych w 2002 r. o użyciu wobec obywateli niejawnych instrumentów operacyjnych w postaci tzw. kontroli operacyjnej decydował minister spraw wewnętrznych, a od 1996 r. – szef Urzędu Ochrony Państwa. Jedyną formą zewnętrznej kontroli tej procedury była konieczność uzyskania zgody prokuratora generalnego na przeprowadzenie tych działań. Ustawa o UOP nie przewidywała oceny zasadności podjęcia kontroli operacyjnej przez przedstawicieli władzy sądowniczej[90]. Najważniejsza zmiana tego rozwiązania nastąpiła na gruncie przepisów ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, które zostały powołane po likwidacji UOP. W celu przeprowadzenia kontroli operacyjnej szef ABW jest zobowiązany do uzyskania na to pisemnej zgody prokuratora generalnego (tak jak poprzednio szef UOP), ale w kolejnej instancji wniosek podlega weryfikacji Sądu Okręgowego w Warszawie[91]. Warunkiem wystąpienia szefa ABW z wnioskiem o zastosowanie kontroli operacyjnej jest bezskuteczność lub wysokie prawdopodobieństwo nieskuteczności albo nieprzydatności innych środków. Rolą sądu jest ocena materiałów przedstawionych przez służby pod kątem absolutnej konieczności zastosowania środków specjalnych wkraczających w obszar praw i wolności obywatelskich. W wyjątkowych przypadkach, kiedy zwłoka mogłaby spowodować utratę informacji lub zniszczenie dowodów, szef ABW może zlecić kontrolę operacyjną (za zgodą prokuratora generalnego) na okres pięciu dni i jednocześnie wystąpić do sądu z wnioskiem o zgodę na jej prowadzenie. Jeśli sąd nie wyda zgody na zastosowanie takiej kontroli, szef ABW jest zobowiązany do jej wstrzymania i zniszczenia pozyskanych w trakciemateriałów[92].

Władza sądownicza w systemie demokratycznej kontroli służb specjalnych ma wpływ na procedury dotyczące weryfikacji decyzji związanych z wydawaniem poświadczeń bezpieczeństwa osobowego i przemysłowego. Ustawa o ochronie informacji

[89] *Ustawa z dnia 24 maja 2004 r. o Agencji Bezpieczeństwa*…, art. 27 ust. 6.

[90] *Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa* (Dz.U. z 1990 r. Nr 30 poz. 180), art. 10.

[91] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa*…, art. 27 ust. 1 i ust. 2. Z pozostałych służb specjalnych uprawnienie do prowadzenia kontroli operacyjnej ma Służba Kontrwywiadu Wojskowego oraz Centralne Biuro Antykorupcyjne. Warunki stosowania kontroli operacyjnej są uregulowane w art. 31 *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu*… oraz w art. 17 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze*…

[92] Analogiczna procedura uzyskania zgody na kontrolę operacyjną obowiązuje również szefów SKW i CBA. Zob. T. Kuć, *Konstytucyjne swobody obywatelskie wobec dyskrecjonalnych działań służb specjalnych*, „Secretum" 2014, nr 1, s. 131–133.

niejawnych wskazuje na Prezesa Rady Ministrów jako na organ odwoławczy, jeśli zostanie wydana przez służby specjalne decyzja o odmowie lub cofnięciu poświadczenia bezpieczeństwa osobowego, oraz na szefów ABW i SKW – wobec takich decyzji wydawanych przez pełnomocników ochrony[93]. Brak korzystnego rozstrzygnięcia daje osobie sprawdzanej prawo do złożenia skargi na postanowienie lub na decyzję organu, który ją wydał, do sądu administracyjnego. To rozwiązanie otwiera obywatelowi sądową drogę odwoławczą, jednak ze względu na to, że przedmiotem rozpatrywanej skargi mogą być materiały i informacje niejawne objęte jedną z klauzul tajności, osoba sprawdzana będąca stroną w sprawie nie jest pełnoprawnym uczestnikiem postępowania. Sąd administracyjny przeprowadza postępowanie skargowe w trybie niejawnym, a w związku z tym osoba sprawdzana nie może brać w nim udziału oraz zapoznawać się z sentencją wyroku, gdyż nie posiada poświadczenia bezpieczeństwa[94]. Sądowa weryfikacja decyzji podejmowanych przez służby specjalne zabezpiecza obywateli przed arbitralnością postępowań sprawdzających. Należy jednak zauważyć, że ze względu na szczególną materię spraw podlegających ocenie, orzeczenia sądu o uchyleniu decyzji niekorzystnej dla osoby sprawdzanej nie wiążą się z automatycznym wydaniem poświadczenia przez upoważnione podmioty. Ta decyzja pozostaje w kompetencji organu pierwszej instancji, tj. Prezesa Rady Ministrów[95].

Omawiając udział władzy sądowniczej w systemie cywilnej i demokratycznej kontroli nad służbami specjalnymi, należy wspomnieć również o zastosowaniu normalnego trybu odwoławczego w odniesieniu do decyzji szefów tych instytucji, które mają charakter administracyjny. Jest to istotne z punktu widzenia osób tam zatrudnionych, ponieważ otwiera możliwość składania skargi kasacyjnej na decyzje szefów związane z pełnieniem przez nich służby do Naczelnego Sądu Administracyjnego. W takim trybie mogą być weryfikowane sprawy związane z normowaniem czasu pracy, przydzielaniem mieszkań czy rozwiązywaniem stosunku służbowego[96]. Ten aspekt sądowej kontroli nie dotyczy ogółu społeczeństwa, a jedynie wąskiej grupy obywateli pozostającej w stosunku podległości służbowej.

Z perspektywy ogólnej udział władzy sądowniczej w systemie cywilnej i demokratycznej kontroli nad służbami specjalnymi sprowadza się do oceny ich działań pod kątem ewentualnego przekroczenia uprawnień lub niedopełnienia obowiązków. Zgodnie z zasadami demokratycznego państwa prawnego wszelkie organy państwa podejmują działania na podstawie ustanowionego prawa oraz w obrębie jego upoważnień. W równym stopniu dotyczy to także szczególnego instrumentu władzy wykonawczej, którym są służby specjalne. Zarówno ich kierownictwo, jak i zatrudnieni w nich funkcjonariusze są upoważnieni i zobowiązani jedynie do realizacji ustawowych zadań z wykorzystaniem przyznanych prawnie środków. Potwierdzeniem tej tezy jest orzeczenie sądu skazujące byłego szefa UOP za nieuzasadnione zatrzymanie prezesa Orlenu[97]. Funkcjonariusze służb specjalnych są zobowiązani do odmowy wykonania poleceń przełożonych, jeśli wiązałoby się to z popełnieniem przestępstwa, oraz do powiadomienia o tym fakcie

[93] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji*…, art. 35 i art. 37.

[94] Tamże, art. 38.

[95] S. *Zalewski, Służby specjalne w państwie…,* s. 129.

[96] Tenże, *Cywilna kontrola*…, s. 121.

[97] A. Kazimierczuk, *Siemiątkowski prawomocnie skazany w sprawie zatrzymania Modrzejewskiego*, „Rzeczpospolita" [online] z 24 kwietnia 2013 r., http://beta.rp.pl/artykul/1003330-Siemiatkowski-prawomocnie-skazany-ws--zatrzymania-Modrzejewskiego.html [dostęp: 11 XII 2014].

szefa, z pominięciem drogi służbowej[98]. Wykonanie takiego polecenia wiąże się z oceną niezawisłego sądu i ewentualną odpowiedzialnością karną.

Podsumowanie

Element tajemnicy występujący w działaniu służb specjalnych jest sprzeczny z wartościami demokratycznymi, takimi jak transparentność organizacji państwowej i prawo obywateli do dostępu do informacji publicznej. Ta sytuacja wymusza konieczność wykreowania i wdrożenia skutecznych mechanizmów nadzoru i kontroli nad tajnymi instrumentami bezpieczeństwa pozostającymi w dyspozycji organów wykonawczych. W tworzeniu rozwiązań nadzorczo-kontrolnych nieodzowne jest uwzględnienie konieczności ochrony przed nieuprawnionym ujawnieniem informacji wrażliwych dla pracy służb, stanowiących o sednie ich skuteczności. Zbudowanie sprawnego sytemu kontrolnego jest oparte na poszukiwaniu odpowiedzi na pytania, jak skutecznie ukierunkować tajne instrumenty bezpieczeństwa na realizację interesu państwa oraz w jaki sposób dokonać rzetelnej oceny ich pracy przy jednoczesnej ochronie informacji wrażliwych stanowiących podstawę ich prakseologii.

Analiza funkcjonalności poszczególnych elementów systemu nadzoru i kontroli nad służbami specjalnymi, zaprezentowana w artykule, wskazuje na potrzebę poszukiwania rozwiązań służących zwiększaniu skuteczności tych służb. Potwierdzeniem tej konkluzji jest diagnoza sformułowana przez Najwyższą Izbę Kontroli w raporcie dotyczącym nadzoru Prezesa Rady Ministrów nad pracą służb specjalnych. Wnioski zawarte w komunikacie NIK wskazują na istotne braki legislacyjne odnoszące się do instrumentów niezbędnych do prowadzenia rzetelnej weryfikacji ich działalności[99]. Przekazanie obowiązków koordynacyjno-nadzorczych premiera wobec tych podmiotów członkowi Rady Ministrów, bez wyposażenia go w narzędzia umożliwiające prowadzenie realnej kontroli, nie jest modelową koncepcją sprawowania nadzoru nad służbami specjalnymi przez władzę wykonawczą. Również parlamentarna kontrola nad działalnością służb i realizowanego nad nimi nadzoru egzekutywy, ze względu na ograniczone uprawnienia, którymi dysponuje Komisja do Spraw Służb Specjalnych, pozostawia pole do poszukiwania nowych, skuteczniejszych rozwiązań. Problemy w funkcjonowaniu tego obszaru kontroli zostały również dostrzeżone przez środowiska polityczne, czego przykładem jest inicjatywa utworzenia nowego, niezależnego politycznie organu kontrolnego – komisji kontrolującej służby specjalne – którego członkowie byliby powoływani przez sejm. Warto nadmienić, że miałby on narzędzia umożliwiające skuteczną weryfikację ich działalności, w tym badania ewentualnych nieprawidłowości w ich pracy i naruszeń prawa[100].

Uprawnione jest twierdzenie, że służby specjalne są wyjątkowym elementem systemu organów i instytucji powołanych do zapewniania bezpieczeństwa państwa. Zasadniczym celem tego systemu jest zagwarantowanie bezpieczeństwa wszystkim obywate-

[98] Zob. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa…,* art. 79 ust. 2 i 3; *Ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego* (tekst jednolity: Dz.U. z 2016 r. poz. 740), art. 38 ust. 2 i 3; *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze…,* art. 71 ust. 2 i 3.

[99] K. Piątek, *NIK o nadzorze nad służbami specjalnymi*, „Rzeczpospolita" [online] z 26 sierpnia 2014 r., http://www4.rp.pl/artykul/1135890-NIK-o-nadzorze-nad-sluzbami-specjalnymi.html [dostęp: 11 XII 2014].

[100] Zob. *Projekt ustawy z dnia … 2013 r. o Komisji Kontroli Służb Specjalnych* [online], http://bip.msw.gov.pl/bip/projekty-aktow-prawnyc/2013/22523,Projekt-ustawy-z-dnia-2013-r-o-Komisji-Kontroli-Sluzb-Specjalnych.html [dostęp: 11 XII 2014].

lom, a także strukturom organizacji państwowej, ponieważ silne i bezpieczne państwo najlepiej realizuje zarówno potrzeby ogólnospołeczne, jak i jednostkowe. Trzeba jednocześnie podkreślić, że w demokracji bezpieczeństwo państwa powinno być wartością nadrzędną, wykreowaną ponad politycznymi podziałami. Sprawą szczególnej wagi jest zatem opracowanie i wdrożenie konsensualnego i funkcjonalnego systemu kontroli i nadzoru nad służbami specjalnymi, który umożliwiałby ich optymalne ukierunkowanie na realizację interesu państwa. Ta sprawa nabiera wyjątkowego znaczenia wobec dynamicznych zmian zachodzących w ostatnim czasie w zakresie bezpieczeństwa, zarówno w skali europejskiej, jak i globalnej.

Bibliografia:

1. Bożek M., *Nadzór Prezesa Rady Ministrów nad służbami specjalnymi i sposoby jego realizacji w świetle obowiązującego ustawodawstwa*, „Przegląd Sejmowy" 2010, nr 3, s. 9–40.
2. Bożek M., *Służby specjalne poza kontrolą Sejmu* [online], http://lubczasopismo.salon24.pl/dziennikarzesledczy/post/322458,sluzby-specjalne-poza-kontrola-sejmu [dostęp: 12 III 2013].
3. Czuchnowski W., *Nowy rząd wyczyści specsłużby po PiS-ie*, „Gazeta Wyborcza" [online] z 25 października 2007 r., http://wyborcza.pl/1,85996,4610377.html [dostęp: 13 III 2013].
4. Czuchnowski W., Uhlig D., *Dlaczego odszedł minister od służb?*, „Gazeta Wyborcza" [online], z 16 I 2008 r.. http://wyborcza.pl/dziennikarze/1,96017,4840844.html [dostęp: 13 III 2013].
5. Gawryszewski J., *Służby specjalne w Republice Federalnej Niemiec*, „Przegląd Bezpieczeństwa Wewnętrznego" 2012, nr 6, s. 11–23.
6. Grzegorowski Z., *Instytucja „służby specjalne" a rzeczywistość funkcjonowania państwa polskiego*, „Studia Gdańskie. Wizje i rzeczywistość" 2010, t. 8, s. 45–64.
7. Grzybowski M., Żebrowski A., *Kontrola władzy ustawodawczej i wykonawczej nad służbami specjalnymi (zagadnienia podstawowe)*, Kraków 1999, Abrys.
8. http://www.sejm.gov.pl/Sejm7.nsf/page/prezydium_sejmu.
9. Jaskiernia J., *Bezpieczeństwo państwa a ochrona praw i wolności jednostki*, w: *Świat wobec współczesnych wyzwań i zagrożeń*, J. Simonides (red.), Warszawa 2010, Scholar.
10. Jaskiernia J., *Demokratyczna kontrola nad służbami specjalnymi a problem ochrony praw i wolności jednostki*, w: *Współczesne wyzwania wobec praw człowieka w świetle polskiego prawa konstytucyjnego*, Z. Kędzia, A. Rost (red.), Poznań 2009, Wydawnictwo Naukowe UAM.
11. Kazimierczuk A., *Siemiątkowski prawomocnie skazany w sprawie zatrzymania* Modrzejewskiego, „Rzeczpospolita" [online] z 24 kwietnia 2013 r., http://beta.rp.pl/artykul/1003330-Siemiatkowski-prawomocnie-skazany-ws--zatrzymania-Modrzejewskiego.html [dostęp: 11 XII 2014].
12. *Konstytucja Rzeczpospolitej Polskiej z dnia 2 kwietnia 1997 r*. (Dz.U. z 1997 r. Nr 78 poz. 483).
13. *Kontrola w Kancelarii Premiera: Wassermann i Kaczyński nie złamali prawa*, „Gazeta Wyborcza" [online], z 26 czerwca 2008 r., http://wiadomosci.gazeta.pl/wiadomosci/1,114873,5399898,Kontrola_w_Kancelarii_Premiera_Wasserman_i_Kaczynski.html [dostęp: 13 III 2013].

14. Kucharski M., *Rządowe organy konsultacyjno-doradcze*, w: *Instytucje bezpieczeństwa narodowego*, M. Paździor, B. Szmulik (red.), Warszawa 2012, C.H. Beck.
15. Kuć T., *Konstytucyjne swobody obywatelskie wobec dyskrecjonalnych działań służb specjalnych*, „Secretum" 2014, nr 1, s. 126–142.
16. Minkina M., *Problemy badań nad wywiadem*, w: *Współczesne bezpieczeństwo polityczne*, S. Jaczyński, M. Kubiak, M. Minkina (red.), Warszawa–Siedlce 2012, Wydawnictwo UPH, s. 167–187.
17. Minkina M., *Służby specjalne a (i) prawa obywatelskie*, w: *Bezpieczeństwo i prawa człowieka w teoriach i praktyce społecznej początków XXI wieku*, R. Rosa, R. Matysiuk (red.), Siedlce 2009, Wydawnictwo Akademii Podlaskiej, s. 287–306.
18. Mróz A., Pajdała H., *Komisja do Spraw Służb Specjalnych – uwagi na tle dotychczasowego funkcjonowania*, „Przegląd Sejmowy" 2004, nr 5, s. 73–92.
19. *„Nie" dla Macierewicza w komisji ds. służb specjalnych* [online], http://wiadomosci.onet.pl/kraj/nie-dla-macierewicza-w-komisji-ds-sluzb-specjalnyc,1,4213666,wiadomosc.html [dostęp: 12 III 2013].
20. *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 17 stycznia 2012 r. w sprawie ogłoszenia jednolitego tekstu uchwały Sejmu Rzeczpospolitej Polskiej – Regulamin Sejmu Rzeczpospolitej Polskiej*, *załącznik do obwieszczenia Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 17 stycznia 2012 – Uchwała Sejmu Rzeczypospolitej Polskiej z dnia 30 lipca 1992 r. – Regulamin Sejmu Rzeczypospolitej Polskiej* (M.P. z 2012 r. poz. 32).
21. *Obwieszczenie Marszałka Sejmu Rzeczypospolitej Polskiej z dnia 17 stycznia 2012 r. w sprawie ogłoszenia jednolitego tekstu uchwały Sejmu Rzeczpospolitej Polskiej – Regulamin Sejmu Rzeczpospolitej Polskiej*, *załącznik do uchwały Sejmu Rzeczpospolitej Polskiej z dnia 30 lipca 1992 r. „Przedmiotowy zakres działania komisji sejmowych"* (M.P. z 2012 r. poz. 32).
22. Piątek K., *NIK o nadzorze nad służbami specjalnymi*, „Rzeczpospolita" [online], z 26 VIII 2014 r., http://www4.rp.pl/artykul/1135890-NIK-o-nadzorze-nad-sluzbami-specjalnymi.html [dostęp: 11 XII 2014].
23. Pieja R., *Przewodnik po cywilnych służbach specjalnych. Od UB do ABW*, Mikołów 2011, Emerpress.
24. *Projekt ustawy z dnia… 2013 r. o Komisji Kontroli Służb Specjalnych* [online], http://bip.msw.gov.pl/bip/projekty-aktow-prawnyc/2013/22523,Projekt-ustawy-z-dnia-2013-r-o-Komisji-Kontroli-Sluzb-Specjalnych.html [dostęp: 11 XII 2014].
25. Radziewicz P., *Uprawnienia, środki działania oraz prawne podstawy funkcjonowania sejmowej Komisji do Spraw Służb Specjalnych*, „Przegląd Legislacyjny" 2006, nr 2, s. 19–34.
26. *Rozporządzenie Prezesa Rady Ministrów z dnia 13 stycznia 1997 r. w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów Zbigniewa Siemiątkowskiego* (Dz.U. z 1997 r. Nr 5 poz. 27).
27. *Rozporządzenie Prezesa Rady Ministrów z dnia 18 listopada 2015 r. w sprawie szczegółowego zakresu działania Ministra – Członka Rady Ministrów Mariusza Kamińskiego – Koordynatora Służb Specjalnych* (Dz.U. z 2015 r. poz. 1921).
28. *Rozporządzenie Prezesa Rady Ministrów z dnia 23 września 2014 r. w sprawie szczegółowego zakresu działania Ministra – Członka Rady Ministrów Jacka Cichockiego w zakresie koordynacji służb specjalnych* (Dz.U. z 2014 r. poz. 1276).

29. *Rozporządzenie Prezesa Rady Ministrów z dnia 24 listopada 2011 r. w sprawie szczegółowego zakresu działania Jacka Cichockiego – Ministra Spraw Wewnętrznych – w zakresie koordynacji służb specjalnych* (Dz.U. z 2011 r. Nr 254 poz. 1524).
30. *Rozporządzenie Prezesa Rady Ministrów z dnia 3 sierpnia 2006 r. w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów – Koordynatora Służb Specjalnych Zbigniewa Wassermana* (Dz.U. z 2006 r. Nr 141 poz. 998).
31. *Rozporządzenie Prezesa Rady Ministrów z dnia 7 listopada 1997 r. w sprawie ustalenia szczegółowego zakresu działania Ministra – członka Rady Ministrów Janusza Pałubickiego* (Dz.U. z 1997 r. Nr 136 poz. 924).
32. *Rozporządzenie Prezesa Rady Ministrów z dnia 28 lutego 2013 r. w sprawie szczegółowego zakresu działania Bartłomieja Sienkiewicza – Ministra Spraw Wewnętrznych – w zakresie koordynacji służb specjalnych* (Dz.U. z 2013 r. poz. 272).
33. *Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 r. w sprawie szczegółowego trybu i zasad funkcjonowania Kolegium do Spraw Służb Specjalnych oraz zakresu czynności sekretarza tego Kolegium* (Dz.U. z 2002 r. Nr 103 poz. 929).
34. *Służby specjalne muszą być profesjonalne i apolityczne* [online], http://www.kprm.gov.pl/wydarzenia/aktualnosci/sluzby-specjalne-musza-byc-profesjonalne-i-apolityczne.html [dostęp: 13 III 2013].
35. Szymanek J., *Organy parlamentarne właściwe w sprawach bezpieczeństwa i porządku publicznego*, w: *Instytucje bezpieczeństwa narodowego*, M. Paździor, B. Szmulik (red.), Warszawa 2012, C.H. Beck, s. 15–51.
36. *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (tekst jednolity: Dz.U. z 2016 r. poz. 1897).
37. *Ustawa z dnia 4 września 1997 r. o działach administracji rządowej* (tekst jednolity: Dz.U. z 2016 r. poz. 543).
38. *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (tekst jednolity: Dz.U. z 2016 r. poz. 1167).
39. *Ustawa z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa* (Dz.U. z 1990 r. Nr 30 poz. 180).
40. *Ustawa z dnia 8 sierpnia 1996 r. o Radzie Ministrów* (tekst jednolity: Dz.U. z 2012 r. poz. 392, ze zm.).
41. *Ustawa z dnia 8 sierpnia 1996 r. o zmianie niektórych ustaw normujących funkcjonowanie gospodarki i administracji publicznej* (Dz.U. z 1996 r. Nr 106 poz. 496, ze zm.).
42. *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (tekst jednolity: Dz.U. z 2016 r. poz. 1319).
43. *Ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego* (tekst jednolity: Dz.U. z 2016 r. poz. 740).
44. *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (tekst jednolity: Dz.U. z 2016 r. poz. 1318).
45. *Wyrok Trybunału Konstytucyjnego z dnia 20 kwietnia 2004 r.*, sygn. akt K 45/02 (Dz.U. z 2004 r. Nr 109 poz. 1159).
46. Zalewski S., *Bezpieczeństwo polityczne państwa. Studium funkcjonalności instytucji*, Siedlce 2010, Wydawnictwo Akademii Podlaskiej.
47. Zalewski S., *Cywilna kontrola służb specjalnych w Polsce*, „Przegląd Bezpieczeństwa Wewnętrznego. Wydanie specjalne", Warszawa 2010, s. 106–123.

48. Zalewski S., *Służby specjalne w państwie demokratycznym*, wydanie II poszerzone i uaktualnione, Warszawa 2005, AON.
49. Zalewski S., *Służby specjalne. Programowanie, nadzór, koordynacja*, Warszawa 2003, Wydawnictwo KPRM.
50. Zubik M., *Organizacja wewnętrzna Sejmu Rzeczpospolitej Polskiej*, Warszawa 2003, Wydawnictwo Sejmowe.
51. Żebrowski A., *Ewolucja polskich służb specjalnych. Wybrane obszary walki informacyjnej*, Kraków 2005, Abrys.

Abstrakt

W artykule poruszono zagadnienia dotyczące systemu cywilnej i demokratycznej kontroli i nadzoru nad służbami specjalnymi w Polsce. Model tego systemu jest oparty na nadzorze sprawowanym przez przedstawicieli władzy wykonawczej, który z kolei jest poddany kontroli parlamentarnej w zakresie kreowania oraz wdrażania prawa regulującego działalność tajnych służb. Istotna rola przypada również władzy sądowniczej, której przedstawiciele nadzorują stosowanie dyskrecjonalnych metod wykorzystywanych przez służby oraz sądzą ewentualne nadużycia popełniane przez ich funkcjonariuszy. Dopełnieniem systemu jest kontrola społeczna sprawowana za pośrednictwem mediów, które przez nagłaśnianie faktów wskazujących na jego braki i niedoskonałości wyrażają presję opinii publicznej na ośrodek władzy w celu wprowadzenia rozwiązań naprawczych. Autor wskazuje na obszary zagrożeń związane z funkcjonowaniem służb specjalnych w warunkach demokratycznego państwa prawnego i w nawiązaniu do nich podejmuje próbę oceny funkcjonalności i efektywności rozwiązań zastosowanych w organizacji systemu nadzorczo-kontrolnego.

Słowa kluczowe: służby specjalne, nadzór, kontrola, demokracja, prawa i wolności obywatelskie.

Abstract

This paper discusses issues concerning the system of civil and democratic control and supervision of secret services in Poland. The model of the system is based on supervision conducted by the executive power, which in turn subjects to parliamentary control exercised by creating the law regarding secret service operations. The judiciary also performs an essential role in the system, as its representatives oversee the application of discretionary methods of the services and adjudicate upon possible abuses perpetrated by their officers. The system is complemented by social control exercised by means of mass media. Disclosure of deficiencies in its actual operation arouse public pressure upon the centre of power to implement corrective measures. The author points out risk areas regarding the operation of secret services under democratic law system and attempts to assess functionality and effectiveness of the solutions adopted in the area of the control-supervision system.

Keywords: secret services, supervision, control, democracy, rights and civil liberties.

Remigiusz Lewandowski

Analiza *Koncepcji wdrożenia polskiego dowodu osobistego z warstwą elektroniczną*

Wstęp

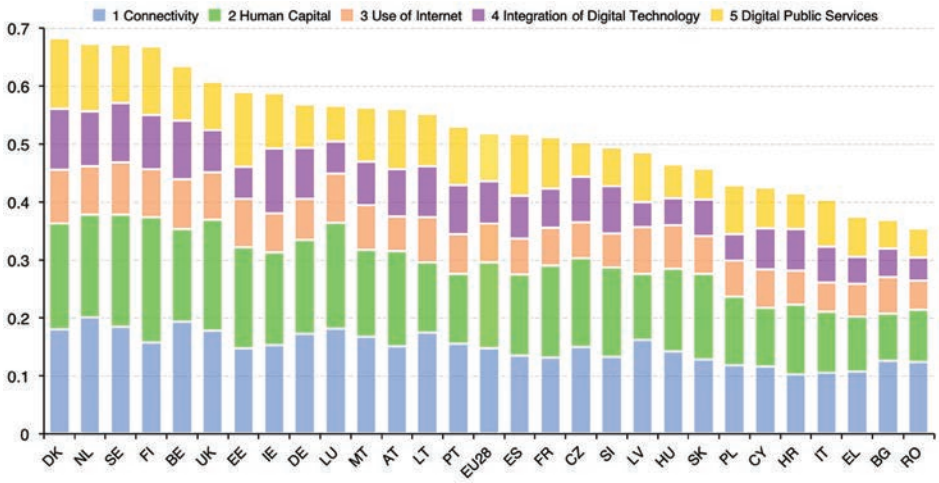
W październiku 2016 r. Ministerstwo Cyfryzacji opublikowało *Koncepcję wdrożenia polskiego dowodu osobistego z warstwą elektroniczną*[1]. Jest to kolejna inicjatywa tego ministerstwa w zakresie upowszechniania rozwiązań cyfrowych i eliminacji tzw. wykluczenia cyfrowego. *Koncepcja…* stanowi kolejną próbę wdrożenia w Polsce elektronicznego dowodu osobistego i stworzenia narzędzia umożliwiającego bezpieczny i powszechny dostęp do usług e-government. Sama idea wprowadzenia elektronicznego dowodu osobistego nie jest nowa. *Koncepcja…* stanowi także odpowiedź na propozycję wprowadzenia warstwy elektronicznej do dowodu osobistego[2], co postulowali eksperci zajmujący się cyfryzacją.

Podjęcie inicjatywy dotyczącej powszechnego i bezpiecznego dostępu do e-usług administracji publicznej jest niezwykle istotne w kontekście niskiego stopnia informatyzacji państwa. Zgodnie z indeksem DESI Komisji Europejskiej z 2016 r. (The Digital Economy and Society Index) Polska pozostaje na 22. miejscu wśród państw członkowskich Unii Europejskiej pod względem zaawansowania w budowie gospodarki cyfrowej i społeczeństwa cyfrowego. Autorzy raportu poświęconego DESI 2016 zwracają uwagę, że (…) *Polska spada do grupy państw pozostających w tyle, gdyż tempo nadrabiania przez nią zaległości jest niższe w porównaniu z wynikiem DESI między 2014 a 2015 r.*[3] Szczegóły indeksu za 2016 r. przedstawiono na rys. 1.

[1] https://mc.gov.pl/konsultacje/koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna-zapraszamy-do [dostęp: 16 I 2017].

[2] Patrz np. M. Kleiber, K. Szubert, *Słowo w sprawie przyszłości polskiego dowodu osobistego*, „Człowiek i Dokumenty" 2015, nr 38, s. 33–34.

[3] *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2016 r. Profil krajowy Polska*, http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14161 [dostęp: 16 I 2017].



Rys. 1. Indeks DESI 2016.

Źródło: https://ec.europa.eu/digital-single-market/desi [dostęp: 16 I 2017].
Legenda: 1. Connectivity – jakość sieci połączeń,
2. Human Capital – kapitał ludzki,
3. Use of Internet – korzystanie z Internetu,
4. Integration of Digital Technology – integracja technologii cyfrowej,
5. Digital Public Services – cyfrowe usługi publiczne.

Jak wynika z powyższego wykresu, spośród obszarów badanych w ramach indeksu – w relacji do średniej UE – dość nisko zostały ocenione przez unijnych ekspertów: kapitał ludzki (w odniesieniu do umiejętności korzystania z IT oraz Internetu), integracja technologii cyfrowych i dostęp do łączności internetowej. Obszar cyfrowych usług publicznych kształtuje się na poziomie zbliżonym do średniej UE, ale eksperci zwracają uwagę, że (…) *aktywne wykorzystanie e-administracji utrzymuje się na stosunkowo niskim poziomie i zaledwie 22% użytkowników Internetu składa formularze elektroniczne (21. miejsce w UE)*[4]. Ta konstatacja pozostaje zgodna z dość powszechnym odczuciem w tym zakresie, tj. z niezadowoleniem z małej liczby usług publicznych oraz narzędzi służących do dostępu do nich, które są udostępnione elektronicznie.

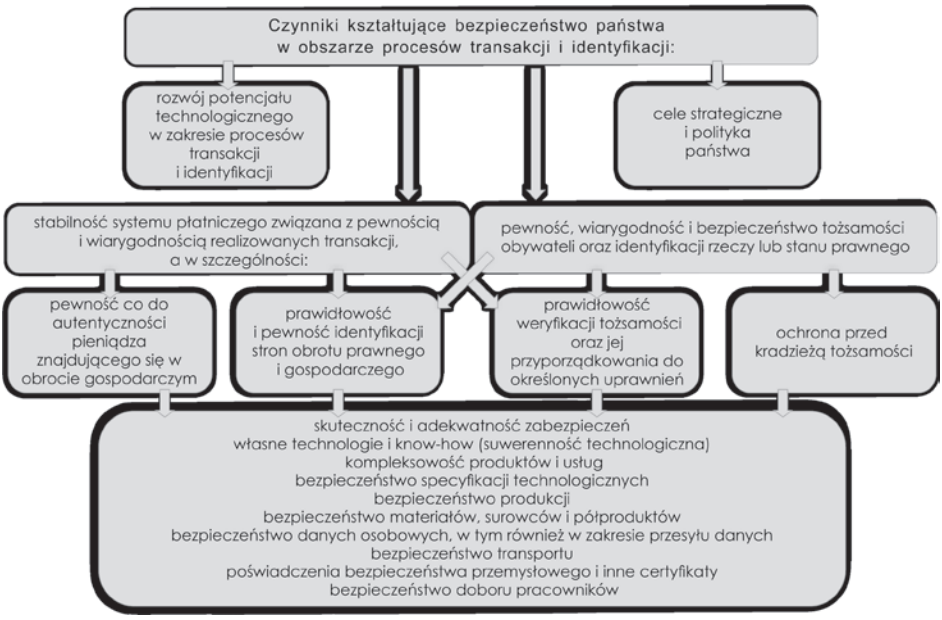
Elektroniczny dowód osobisty może stanowić także narzędzie wpływające na poprawę stanu informatyzacji państwa i społeczeństwa. Niemniej, analizując potencjalne formy i funkcjonalności takiego dowodu, należy mieć na uwadze przede wszystkim jego funkcję w zakresie potwierdzania tożsamości[5] i związany z tym aspekt bezpieczeństwa państwa. Z dokumentami tożsamości wiąże się bowiem pojęcie bezpieczeństwa identyfikacyjnego, rozumianego jako stan niezakłóconego bezpieczeństwa państwa w obszarze obejmującym:

1) prawidłową weryfikację deklarowanej tożsamości osób,
2) weryfikację prawidłowości przyporządkowania danej osoby i jej tożsamości do określonych uprawnień wynikających z dokumentu, jakim się posługuje,

[4] Tamże.
[5] R. Lewandowski, *O potrzebie regulacji sfery dokumentów publicznych*, „Człowiek i Dokumenty" 2016, nr 42, s. 53–58.

3) obrót prawny i gospodarczy związany z użyciem dokumentów potwierdzających tożsamość lub określone uprawnienia,
4) ochronę obywateli przed kradzieżą tożsamości[6].

W tym kontekście należy uznać, że bezpieczeństwo identyfikacyjne i dotyczące go dokumenty publiczne, zwłaszcza dowód osobisty, mają wpływ na zapewnianie bezpieczeństwa państwa. Ten związek obejmuje szczególnie bezpieczeństwo ekonomiczne i publiczne. Zależności pomiędzy wiarygodnością dokumentów a bezpieczeństwem państwa przedstawiono na rys. 2.



Rys. 2. Czynniki kształtujące bezpieczeństwo państwa w zakresie wiarygodności identyfikacji.

Źródło: R. Lewandowski, *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, Volumina, s. 289.

Wpływ dokumentów, w tym dowodu osobistego, na bezpieczeństwo ekonomiczne państwa wynika z posługiwania się dokumentami tożsamości w obrocie gospodarczym i prawnym w celu zidentyfikowania stron transakcji. Naruszenie wiarygodności tego typu dokumentów może prowadzić do naruszenia stabilności systemu płatniczego, uszczupleń podatkowych budżetu państwa oraz do strat po stronie osób fizycznych i prawnych. W tym zakresie naruszenie wiarygodności należy rozumieć jako narzędzie służące do popełniania przestępstw gospodarczych. Skala zagrożeń ekonomicznych może być jednak znaczna także w przypadku przestępstw o charakterze terrorystycznym, popełnia-

[6] R. Lewandowski, *Evaluation of legal and technical solutions with respect to new types of documents in the health care system – KUZ, KSM and KSA*, „Journal of Health Policy, Insurance and Management – Polityka Zdrowotna" 2015, nr 16, s. 77.

nych z wykorzystaniem dokumentów podrobionych lub przerobionych. Tego rodzaju przestępstwa mogą bowiem dotykać nie tylko podmioty bezpośrednio poszkodowane, lecz także całe społeczeństwo – przez wzrost ryzyka systematycznego i związanych z nim kosztów społecznych[7]. Bezpieczeństwo bowiem (w tym ekonomiczne) jest dobrem publicznym, które przynosi wymierne korzyści społeczeństwu i warunkuje konsumpcję innych dóbr[8]. Niektórzy badacze wskazują, że w skrajnych przypadkach naruszenie bezpieczeństwa identyfikacyjnego może powodować zachwianie systemu gospodarczego państwa i godzić w jego podstawowe interesy ekonomiczne[9].

Dokument tożsamości i jego odpowiednie zabezpieczenie przed podrobieniem i przerobieniem jest również czynnikiem warunkującym bezpieczeństwo publiczne. Należy zauważyć, że fałszowanie dokumentów i kradzież tożsamości występuje także w przypadku działalności agenturalnej i terrorystycznej, czy też szerzej – działalności wymierzonej w bezpieczeństwo publiczne. Skradziona tożsamość lub sfałszowany dokument nader często stanowią niezbędne atrybuty terrorysty[10].

W niniejszym artykule oparto się na analizie *Koncepcji wdrożenia polskiego dowodu osobistego z warstwą elektroniczną* oraz analizie literatury przedmiotu i publicznie dostępnych danych dotyczących stopnia informatyzacji Polski. Jego celem jest identyfikacja potencjalnych słabości *Koncepcji…* oraz zaproponowanie rozwiązań ukierunkowanych na poprawę jakości elektronicznego dowodu osobistego z punktu widzenia bezpieczeństwa państwa i obywateli oraz z punktu widzenia jego funkcjonalności.

Metodyka i fundamentalne cele projektu

Koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną jest złożona ze wstępu, sześciu rozdziałów merytorycznych, podsumowania i rekomendacji. Rozdziały merytoryczne dotyczą zakresu danych, które mają być umieszczone w dowodzie osobistym, tj.: jego funkcjonalności, skutków finansowych jego wdrożenia, opisów wariantów wymiany dowodów osobistych, zadań związanych z wdrożeniem dowodu osobistego z warstwą elektroniczną, finansowego rozliczenia projektu pl.ID oraz analizy różnego rodzaju ryzyka związanego z wprowadzeniem nowego typu dowodu.

W żadnej części dokumentu nie przedstawiono metodyki, zgodnie z którą *Koncepcja…* była tworzona. To generuje jej zasadniczą słabość. Zapoznając się z treścią *Koncepcji*..., można odnieść wrażenie, że metodyki adekwatnej do zagadnienia nie zastosowano w całości tego materiału i że jest on rezultatem raczej tzw. burzy mózgów (skądinąd dobrej techniki, ale nieprzystającej do tego kompleksowego przedsięwzięcia) niż usystematyzowanego i uporządkowanego algorytmu działań zmierzających do wypracowania zasadniczych atrybutów elektronicznego dowodu osobistego.

---

[7] R. Lewandowski, T. Goliński, *Zarządzanie wiarygodnością dokumentów a bezpieczeństwo ekonomiczne*, w: *Zarządzanie w systemie gospodarczym. Szanse i zagrożenia*, K. Raczkowski (red.), Warszawa 2015, s, 118–119.

[8] K. Stańczyk, J. Płaczek, *Próba oszacowania bezpieczeństwa finansowego Polski*, w: *Zarządzanie w systemie gospodarczym. Szanse*..., s. 387.

[9] Np. J. Grzemski, A. Krześ, *Analiza pojęcia „przestępstwa godzące w podstawy ekonomiczne państwa" w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2, s. 150.

[10] R. Lewandowski, T. Goliński, *Nielegalna migracja a bezpieczeństwo identyfikacyjne*, w: *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, M. Tomaszewska-Michalak, T. Tomaszewski (red.), Warszawa 2015, s. 123.

W analizowanym materiale uwagę zwraca pominięcie zagadnienia fundamentalnego przy projektowaniu nowego typu dokumentu, tj. odpowiedzi na pytanie, jaki jest podstawowy cel związany z wprowadzeniem elektronicznych dowodów osobistych i jakie potrzeby publiczne ma ten dokument zaspokoić. Przy czym potrzeby należy analizować m.in. z punktu widzenia:

- społeczeństwa,
- podmiotów gospodarczych,
- administracji publicznej.

Przykładowo w odniesieniu do potrzeb społeczeństwa można podnieść kwestię konieczności szerokiego i powszechnego udostępnienia narzędzia uwierzytelniania w systemach e-government[11], a także skoncentrowania w ramach jednego dokumentu innych dokumentów, którymi posługują się obywatele (multifunkcjonalność)[12]. Kolejną potrzebą sygnalizowaną zarówno przez osoby fizyczne, jak i prawne (w tym podmioty gospodarcze) jest potrzeba potwierdzania tożsamości osoby legitymującej się danym dokumentem[13]. Jest to, co należy podkreślić, także jedna z zasadniczych potrzeb administracji publicznej – pewność dotycząca prawidłowej weryfikacji tożsamości obywatela. Należy podkreślić, że administracja publiczna, a już z pewnością Policja, Straż Graniczna i służby specjalne, ma znacznie większe możliwości w zakresie weryfikowania tożsamości niż zwykli obywatele. Stąd też istotne jest zapewnienie, szczególnie dla prawidłowości obrotu prawnego i gospodarczego, że również osoby niewyspecjalizowane będą mogły w sposób prawidłowy weryfikować tożsamość. Jaskrawym przykładem może tu być chociażby działalność notarialna czy bankowa, w których przypadku konieczność prawidłowego zweryfikowania tożsamości ma zasadnicze znaczenie dla obu wyżej wymienionych obrotów.

Brak odpowiedzi na pytanie o cel projektu wdrożenia elektronicznych dowodów osobistych może sprawiać wrażenie, że tego typu dowód jest jedynie próbą wprowadzenia (relatywnie) nowoczesnego rozwiązania do sfery dokumentów publicznych li tylko i wyłącznie dla samej chęci wykazania się „nowoczesnością" lub też w celu uniknięcia zwrotu Komisji Europejskiej środków pomocowych do tej pory wydatkowanych na projekt pl.ID (ich suma – 160 mln zł – jest niewspółmiernie wysoka w stosunku do dodatkowych kosztów całego przedsięwzięcia, które wynoszą 1,5 mld zł). Przed podjęciem jakichkolwiek decyzji dotyczących ewentualnego wdrożenia elektronicznych dowodów osobistych konieczna jest zatem refleksja nad wskazanymi zagadnieniami, a następnie wypracowanie na jej podstawie podstawowych celów, jakim nowe dokumenty mają służyć, a także zidentyfikowanie potrzeb zaspokajanych przez tego typu dowody. Na bazie tak określonego fundamentu jest możliwe przejście do kolejnych faz koncepcji budowy nowego dokumentu, tj.:

1) mapy funkcjonalności nowego dowodu osobistego,
2) analizy zagrożeń związanych z wdrożeniem nowego dowodu osobistego,
3) projektu formy dokumentu (materialny versus zdigitalizowany),
4) propozycji zestawu zabezpieczeń adekwatnych do formy dokumentu, zdiagnozowanych zagrożeń i zdefiniowanych funkcjonalności.

[11] Patrz np. R. Lewandowski, *Evaluation of Legal And Technical Solutions*…, s. 77.

[12] Tamże, s. 83.

[13] R. Lewandowski, *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, s. 287–288.

Jak wynika z lektury *Koncepcji wdrożenia polskiego dowodu osobistego z warstwą elektroniczną*, przy tworzeniu tego materiału nie opracowano wykazu powiązanych ze sobą prac analitycznych, generującego model sporządzania dokumentu publicznego[14]. To znacząco osłabia jakość *Koncepcji…* i – co gorsza – może ostatecznie prowadzić do wyboru oraz wprowadzenia rozwiązań ułomnych, nieodpowiadających potrzebom społeczeństwa czy administracji publicznej, a także wiązać się z nieuzasadnionymi wydatkami budżetu państwa. Wiele szczegółowych niedociągnięć dotyczących koncepcji przyjętych w omawianym dokumencie przedstawiono w dalszej części niniejszej analizy.

Funkcjonalność elektronicznego dowodu osobistego

Karta Ubezpieczenia Zdrowotnego (KUZ)

Pozytywnie należy ocenić plan włączenia do dowodu osobistego z warstwą elektroniczną funkcjonalności Karty Ubezpieczenia Zdrowotnego (KUZ). W ramach tego typu funkcjonalności prezentowanej w *Koncepcji…* jest to jedyna znacząca wartość związana z wdrożeniem projektu. Wynika ona przede wszystkim z:

- ograniczenia wyłudzeń związanych z finansowaniem przez NFZ świadczeń zdrowotnych dzięki mechanizmowi KUZ i poświadczania realizacji usług,
- uniknięcia dublowania wydatków publicznych związanych z emisją dokumentu dodatkowego (odrębnej karty KUZ).

Wprowadzenie funkcjonalności KUZ, także w przypadku dowodu elektronicznego, było przedmiotem badań naukowych, w których wskazywano na wiele pozytywnych konsekwencji takiego działania[15]. Te wnioski potwierdza praktyka stosowana przez różne państwa europejskie, które wdrożyły elektroniczny dowód osobisty, czyniąc z niego podstawowy dokument służący nie tylko identyfikacji, lecz także uwierzytelnianiu w systemach e-government[16].

Zdefiniowana wartość wynikająca z włączenia do dowodu osobistego funkcjonalności KUZ ma jednak charakter warunkowy, tj. da o sobie znać tylko wtedy, gdy ta funkcjonalność – czyli poświadczanie przez pacjentów zrealizowanych usług zdrowotnych – zostanie uruchomiona w planowanym terminie. Należy zwrócić uwagę, że niepowodzenie w tym zakresie – czyli brak możliwości poświadczania usług – będzie oznaczało, iż podstawowa funkcjonalność elektronicznego dowodu osobistego nie będzie działać, a zatem środki publiczne przeznaczone na ten cel (1,5 mld zł) zostaną zmarnotrawione. Stąd też zasadnicze znaczenie ma silne sprzęgnięcie projektu pl.ID z projektami dotyczącymi zarządzania uprawnieniami obywateli do publicznych świadczeń zdrowotnych oraz poprawy kontroli nad publicznymi wydatkami na ochronę zdrowia. Te projekty, w celu zapewnienia wymaganej koordynacji, winny być realizowane w ramach jednego portfela projektów i przez jedno centrum decyzyjne.

---

[14] Przykładowy model projektowania dokumentu przedstawiono w: E. Jakielaszek, *Dokument tożsamości w aspekcie współczesnej przestępczości*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki*…, s. 299–305.

[15] Patrz np. R. Lewandowski, *Evaluation of Legal And Technical Solutions*…, s. 75–84.

[16] R. Lewandowski, *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego*, „Polski Przegląd Nauk o Zdrowiu" 2016, nr 3, s. 311–212.

Z *Koncepcji wdrożenia polskiego dowodu osobistego z warstwą elektroniczną* można wyciągnąć wniosek, że planowany termin uruchomienia (zadziałania) funkcjonalności KUZ – to rok 2024. Tak odległy moment jej wdrożenia stawia pod znakiem zapytania sens wcześniejszej wymiany dowodu osobistego starego typu na typ elektroniczny (od 2019 r.). To oznacza, że przez pierwszych pięć lat obowiązywania dowodów elektronicznych ich elektroniczno-informatyczna funkcjonalność (w tym mikroprocesor umieszczony w dowodzie) w ogóle nie będzie wykorzystywana (jeśli nie zostałyby wprowadzone dane biometryczne) albo będzie wykorzystywana połowicznie (w przypadku wprowadzenia tych danych). Należy podkreślić, że konieczność związana z KUZ, dotycząca wydania elektronicznych dowodów osobistych wszystkim pełnoletnim obywatelom w krótkim czasie, nie implikuje przekazania tych dokumentów z pięcioletnim wyprzedzeniem jako jedynego rozwiązania powyższego problemu. To zagadnienie wymaga przeanalizowania alternatywnych rozwiązań.

Karta Specjalisty Medycznego (KSM)

Drugą wątpliwość wywołuje niewłączenie do dowodu osobistego funkcjonalności Karty Specjalisty Medycznego (KSM). Uzasadnienie dla tej decyzji ujęte w *Koncepcji…* jest całkowicie nieprzekonujące. Argumenty typu „komplikacja całego projektu", „dodatkowe koszty i ryzyko"[17], niepoparte rzetelną analizą i danymi liczbowymi, skłaniają do zapytania o faktyczne przyczyny takiej decyzji. Biorąc pod uwagę liczbę projektowanych KSM (kilkaset tysięcy sztuk)[18], ich włączenie do dowodu osobistego wiązałoby się raczej z oszczędnościami budżetowymi niż „dodatkowymi kosztami".

Karta Pacjenta (KP)

Niejasny i niespójny z założeniami dotyczącymi KUZ wydaje się passus zawarty w *Koncepcji…,* dotyczący Karty Pacjenta:

> Wydanie Karty Pacjenta przez PWPW w liczbie ok. 1,4 mln sztuk dla określonej grupy pacjentów jest możliwe w terminie III kw. 2018 roku – IV kw. 2019 roku, a koszt tego wydania wyniesie około 28 mln zł netto. Kwota ta nie obejmuje kosztów wytworzenia i utrzymania systemu informatycznego do zarządzania cyklem życia karty (ok. 0,9 mln zł netto) oraz kosztów utrzymania systemu do personalizacji dokumentów (ok. 0,15 mln zł netto miesięcznie), a także kosztów dystrybucji kart i ich dodruków w kolejnych latach. Ponadto mogą zostać wydane Karty Pacjenta dla pozostałych obywateli, przy czym wydanie to nastąpi na wniosek zainteresowanych osób oraz będzie odpłatne (wg szacunków PWPW możliwe jest wydawanie po 2019 po ok. 200 tys. kart rocznie)[19].

Karta Pacjenta nie została w *Koncepcji…* zdefiniowana – nie są znane ani cele emisji takiego dokumentu, ani jego funkcjonalność. Wydawanie dodatkowych dokumentów typu Karta Pacjenta oprócz elektronicznego dowodu osobistego z funkcjonal-

[17] *Koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną* [online], Ministerstwo Cyfryzacji, 2016 r., s. 6, https://mc.gov.pl/konsultacje/koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna-zapraszamy-do [16 I 2017].

[18] Dane za: https://legislacja.rcl.gov.pl/docs//2/241132/241140/241141/12277289/dokument150955.pdf.

[19] *Koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną*…, s. 16.

nością KUZ nie wydaje się być uzasadnione, zwłaszcza w kontekście przytoczonych kosztów związanych z tą Kartą – zarówno po stronie budżetu państwa (31,7 mln zł netto w okresie III kw. 2018 – IV kw. 2019 wraz z dalszymi kosztami w kolejnych latach), jak i obywateli.

Negatywnie należy ocenić także próbę obciążania obywateli dodatkowymi opłatami związanymi z zarządzaniem publicznym systemem opieki zdrowotnej (*...mogą zostać wydane Karty Pacjenta dla pozostałych obywateli, przy czym wydanie to nastąpi na wniosek zainteresowanych osób oraz będzie odpłatne)*. Społeczeństwo już ponosi koszty opieki zdrowotnej i zarządzania jej systemem w formie składek płaconych na NFZ. Dodatkowe „daniny" w tym zakresie nie znajdują uzasadnienia.

Weryfikacja tożsamości

Podstawową funkcją dowodu osobistego jest umożliwienie weryfikacji tożsamości osoby, której dowód został wydany i która się nim legitymuje. Obecnie tego typu weryfikacja następuje przede wszystkim dzięki subiektywnemu porównaniu fotografii widniejącej na dowodzie osobistym z twarzą posiadacza i stwierdzeniu wystarczającej zgodności cech. Nie jest to weryfikacja łatwa nawet dla wyspecjalizowanych służb, zwłaszcza w kontekście 10-letniego terminu ważności dowodu osobistego (stąd też w niektórych państwach stosuje się krótsze okresy ważności tego dokumentu, np. 5-letnie). Weryfikacja oparta wyłącznie na subiektywnym oglądzie nie jest doskonała i siłą rzeczy nie może dawać wymaganej pewności. Stąd we współczesnych dokumentach stosuje się rozwiązania pozwalające na ich powiązanie z osobą, dla której zostały wydane, z większą trafnością. Tym rozwiązaniem jest m.in. wykorzystanie biometrii. Biometria to wiedza o rozpoznawaniu żywych osób na podstawie pomiaru cech biologicznych (anatomicznych i fizjologicznych), zarówno pasywnych (jak np. wzór tęczówki oka, odciski palców, twarz, wzory siatkówki oka, geometria dłoni, układ naczyń krwionośnych), jak i aktywnych (np. dynamika pisma ręcznego, głos, ruch warg, chód)[20]. Współcześnie biometria stanowi stałe, a zarazem najważniejsze ogniwo łańcucha wartości dokumentów identyfikacyjnych.

Funkcjonalność dowodu osobistego opisana w *Koncepcji…* nie daje jednoznacznej odpowiedzi na pytanie, czy w elektronicznym dowodzie osobistym mają być przechowywane dane biometryczne obywatela, a jeśli tak, to jakiego typu. Rosnące zastosowanie biometrii przy sporządzaniu dokumentów nie powinno dziwić. Jest to jedna z najbardziej niezawodnych metod uwierzytelniania i weryfikacji tożsamości człowieka (lub identyfikacji osoby), ale jej skuteczność nie jest bezwarunkowa. Zwykle ograniczenie tej skuteczności jest wynikiem niewłaściwego wykorzystania technologii, a nie jej słabości[21]. W literaturze przedmiotu wskazuje się na wymogi, które muszą towarzyszyć prawidłowemu uwierzytelnianiu biometrycznemu, takie jak: optymalne warunki dokonania pomiaru biometrycznego, aktualizacja tego pomiaru, optymalny poziom tolerancji[22]. Skuteczność biometrii można znacząco podnieść przez wprowadzenie pomiaru nie jednej, lecz co najmniej dwóch cech biometrycznych. W ten sposób można jeszcze bardziej powiązać daną osobę z dokumentem, którym się ona posługuje.

[20] B. Hołyst, J. Pomykała, *Biometria w systemach uwierzytelniania*, „Biuletyn Wojskowej Akademii Technicznej" 2011, nr 4, s. 418–419.

[21] W. Gurtefer, A. Pacut, *Człowiek w systemie biometrycznym*, w: *Dokumenty a prawo*..., s. 79.

[22] B. Hołyst, J. Pomykała, *Biometria w systemach*..., s. 420–421.

W związku z powyższym polski elektroniczny dowód osobisty powinien zawierać dwa rodzaje danych biometrycznych obywateli. Ewentualna decyzja o niezamieszczaniu tego typu danych w nowym dowodzie powinna być przesłanką do utrzymania obecnego, „analogowego" dowodu osobistego. Nie ma bowiem ekonomicznego uzasadnienia realizacja kosztownego projektu pl.ID, polegającego m.in. na wyposażeniu dowodu w mikroprocesor i równocześnie niewykorzystaniu tej sposobności do podniesienia walorów dokumentu związanych z bezpieczeństwem identyfikacyjnym przez wprowadzenie rozwiązań biometrycznych. We współczesnym świecie ograniczenie zabezpieczeń dowodu tożsamości do zabezpieczeń fizycznych, niedostępnych na otwartym rynku, a także oparcie się na wyspecjalizowanym parku maszynowym (również reglamentowanym, jeśli chodzi o możliwości jego zakupu), to zbyt mało, aby skutecznie uchronić się przed fałszerzami, ponieważ przestępcy najczęściej wykorzystują imitacje zabezpieczeń[23]. Stąd tak ważne jest stosowanie zabezpieczeń zarówno fizycznych, jak i elektroniczno-informatycznych, w tym opartych na biometrii. Podkreślenia wymaga to, że prawidłowość weryfikacji tożsamości jest podstawowym atrybutem bezpieczeństwa identyfikacyjnego[24].

Należy zauważyć, że dowód osobisty jest również dokumentem podróży dla osób przemieszczających się w granicach strefy Schengen. Paszporty wydawane przez kraje tej strefy (w tym przez Polskę) obowiązkowo mają zapisane elektronicznie takie cechy biometryczne, jak wizerunek twarzy i obrazy dwóch odcisków palców. Przy stałym zwiększaniu wymogów dotyczących bezpieczeństwa w przyszłości może zaistnieć konieczność posługiwania się podczas podróży w strefie Schengen jedynie dokumentami z zapisanymi cechami biometrycznymi.

Ponadto, projektując wzór graficzny nowego dowodu i planując zakres danych do umieszczenia w warstwie graficznej, należałoby wyeliminować obecne słabości wzoru. Za największą z nich należy uznać brak podpisu obywatela w jego warstwie graficznej. To ważna cecha, która jest pomocna przy weryfikowaniu tożsamości, zwłaszcza przy sprawdzaniu danych biometrycznych zapisanych na mikroprocesorze.

Funkcjonalność tzw. Polskiej Karty Płatniczej

Za niezrozumiałe należy uznać całkowite pominięcie w *Koncepcji…* istotnych elementów rządowego programu Paperless/Cashless[25], a szczególnie kwestii związanych z budową krajowego schematu płatniczego (alternatywnego wobec systemów VISA i MasterCard). Być może przyczyną tego przeoczenia są niedociągnięcia metodologiczne powstałe przy tworzeniu *Koncepcji…*, wskazane w pierwszej części niniejszego opracowania.

Tworząc nowy elektroniczny dowód osobisty, z całą pewnością należy wziąć pod uwagę wprowadzenie w ramach jego funkcjonalności także tzw. Polskiej Karty Płatniczej. W niniejszym artykule nie przesądza się, czy rzeczywiście w tego rodzaju dowodzie ta funkcjonalność winna być wdrażana (być może należy oprzeć się na rozwiązaniach mobilnych), ale niewątpliwie to zagadnienie powinno być przeanalizowane. Pominięcie w *Koncepcji…* zagadnienia dotyczącego Polskiej Karty Płatniczej należy ocenić negatywnie.

[23] E. Jakielaszek, T. Zwoliński, *Weryfikacja dokumentów – mity a rzeczywistość*, w: *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*..., s. 103–104.

[24] R. Lewandowski, *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych*…, s. 287–288.

[25] https://www.mr.gov.pl/media/21329/Od_papierowej_do_cyfrowej_PL_prez_dluzsza_20062016.pdf .

Interfejs stykowy i bezstykowy

Koncepcja… zakłada, że dowód osobisty z warstwą elektroniczną będzie wyposażony w interfejsy stykowy i bezstykowy. Jednak brakuje uzasadnienia dla takiego wyboru. Należy zauważyć, że interfejs stykowy wykazuje znacznie większą zawodność niż bezstykowy. Poza tym jest to raczej rozwiązanie przebrzmiałe i zastępowane interfejsem bezstykowym – nie tylko mniej zawodnym, lecz także bardziej przyjaznym dla użytkownika. Wybór rozwiązania dualnego nie generuje zatem szczególnej wartości dla użytkownika, a jedynie dodatkowe koszty dla budżetu państwa. Z tego względu bardziej zasadne wydaje się zastosowanie jedynie interfejsu bezstykowego, tak jak ma to miejsce w przypadku większości elektronicznych dowodów osobistych.

Certyfikaty

Zgodnie z *Koncepcją…* w warstwie elektronicznej dowodu osobistego mają być umieszczone następujące certyfikaty:

1) certyfikat do identyfikacji i uwierzytelniania w systemach informatycznych online (kontener MSWiA, wydawca MSWiA we współpracy z PWPW), którego ważność będzie tożsama z ważnością dokumentu, tj. 10 lat;
2) certyfikat „podpisu osobistego" (kontener MSWiA, wydawca MSWiA we współpracy z PWPW), którego ważność będzie tożsama z ważnością dokumentu, czyli 10 lat;
3) certyfikat służący do poświadczania dostępu pacjenta do usługi medycznej (bez PIN) – kontener MSWiA i/lub MZ (wydawca MSWiA lub MZ);
4) możliwość zapisania – za pośrednictwem PWPW – dowolnego certyfikatu kwalifikowanego w odrębnym kontenerze, przy czym PWPW wystawi nieodpłatnie pierwszy, dwuletni certyfikat dla wszystkich chętnych obywateli. Po upływie tego okresu posiadacz dokumentu będzie mógł wystąpić do PWPW o odnowienie certyfikatu lub o nowy certyfikat – do innego podmiotu świadczącego takie usługi; koszty aktualizacji lub wgrania kolejnego certyfikatu dla podpisu kwalifikowanego będą leżały po stronie obywatela.

Umieszczenie czterech różnych certyfikatów w dowodzie osobistym wiąże się z całą pewnością ze wzrostem kosztów mikroprocesora (wymagana odpowiednio większa pamięć). Trudno jednak znaleźć uzasadnienie dla takiej liczby. Tańszym, a jednocześnie nie generującym negatywnych konsekwencji z punktu widzenia użytkownika, rozwiązaniem byłoby zastosowanie dwóch lub wyłącznie jednego certyfikatu.

Ponadto negatywnie należy ocenić koncepcję nieodpłatnego wystawienia certyfikatu przez jeden podmiot. Tego rodzaju przedsięwzięcie, które wykorzystuje dominującą pozycję jednego przedsiębiorstwa, poważnie naruszy strukturę rynku podpisu kwalifikowanego w Polsce i może doprowadzić wręcz do upadku inne podmioty wydające certyfikaty kwalifikowane.

Koszty

Koszty projektu przypadające na lata 2017–2023 oceniono na kwotę co najmniej[26] 1,5 mld zł. Są to wydatki dodatkowe, poza ponoszonymi obecnie (0,9 mld zł[27] – s. 11)

[26] *Koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną…*, s. 25.
[27] Tamże, s. 11.

we wskazanym okresie. To oznacza, że łączna kwota wydatków budżetowych na projekt pl.ID wyniesie w latach 2017–2023 co najmniej 2,4 mld zł, tj.:[28]

- w 2017 r. – 305 81 mln zł,
- w 2018 r. – 163 24 mln zł,
- w 2019 r. – 311 46 mln zł,
- w 2020 r. – 325 80 mln zł,
- w 2021 r. – 559 24 mln zł,
- w 2022 r. – 360 79 mln zł.

Kwota 2,4 mld zł (co najmniej) jest bardzo znacząca z punktu widzenia finansów publicznych i obciążeń budżetowych. Poziom wydatków winien być jedną z podstaw ostatecznej decyzji co do realizacji omówionego projektu. W tym kontekście negatywnie należy ocenić dokładność i obiektywizm przedstawionych szacunków. W wielu przypadkach koszty zostały wyliczone na podstawie danych przedstawionych przez jednego z wytwórców dokumentów[29]. Abstrahując od wyboru samego wytwórcy, poziom wydatków ponoszonych przez budżet państwa powinien zostać oszacowany w sposób obiektywny i wolny od jakichkolwiek podejrzeń o interesowność strony przygotowującej takie wyliczenia.

Pozostałe uwagi

Istotny jest także podział kompetencji dotyczących obsługi pełnego cyklu życia dokumentu pomiędzy zaangażowanymi podmiotami. Dostawca blankietów z mikroprocesorem nie powinien być w takim przypadku odpowiedzialny za usługi prepersonalizacji, gdyż może to rzutować na poziom bezpieczeństwa całego systemu – dostęp do kluczy transportowych powinien być ograniczony tylko do podmiotu wykonującego personalizację. Sama prepersonalizacja może być wykonywana, jak się to odbywa w systemach związanych z dowodami osobistymi w innych krajach, na etapie tuż przed personalizacją. Rozdział tych dwóch procesów budzi uzasadnione wątpliwości.

Analizując także funkcjonalność systemu informatycznego, w którym będzie osadzony polski dowód elektroniczny, zauważa się, że w *Koncepcji*... nie zadbano o takie elementy, jak dostarczenie obywatelom czytników dokumentów (w przypadku mikroprocesora stykowego) oraz oprogramowania middleware, za którego pomocą byłoby możliwe wykorzystanie dokumentu w celu weryfikacji tożsamości przez Internet. Samo posiadanie dokumentu elektronicznego przez przeciętnego obywatela, zarówno bez usług centralnych, jak i lokalnej możliwości jego wykorzystania powoduje, że dowód elektroniczny nie będzie się dla niego różnił od dowodu używanego obecnie.

Jeśli chodzi o techniczne aspekty nowego dowodu osobistego, to zastanawiające jest zachowanie zgodności dowodu z wymaganiami ICAO dla warstwy graficznej, bez wzmianki na temat warstwy elektronicznej. Tutaj także należy zastosować te mechanizmy, które są rekomendowane przez ICAO i wymagane przez polskie ustawodawstwo – chociażby protokoły dostępu (SAC i EAC) do danych osobistych na mikroprocesorze czy same dane biometryczne (dwie cechy biometryczne – zdjęcie twarzy i odcisk palca), jak zostało to już wcześniej przedstawione w niniejszym artykule.

[28] Tamże, s. 15.

[29] Stosowany jest zwrot „wg PWPW".

Wnioski

W obliczu zdiagnozowanych słabości *Koncepcji wdrożenia polskiego dowodu osobistego z warstwą elektroniczną*, tj.:

- braku poprawnej i adekwatnej metodologii tworzenia *Koncepcji…*,
- braku zdefiniowanych celów projektu oraz zidentyfikowanych potrzeb, które mają być zaspokojone przez wdrożenie elektronicznych dowodów osobistych,
- braku synchronizacji pomiędzy terminem rozpoczęcia emisji elektronicznych dowodów osobistych (2019 r.) a terminem uruchomienia funkcjonalności KUZ (2023 r.),
- braku funkcjonalności KSM w dowodzie osobistym,
- niejasności dotyczących emisji dodatkowych kart oprócz dowodu osobistego (Karty Pacjenta),
- niejasności dotyczących wprowadzenia do dowodu osobistego dwóch cech biometrycznych,
- nieujęcia wzoru podpisu w warstwie graficznej dowodu osobistego,
- niepodjęcia zagadnienia dotyczącego wprowadzenia tzw. Polskiej Karty Płatniczej w funkcjonalności dowodu,
- kosztownego i merytorycznie nieuzasadnionego umieszczenia w warstwie elektronicznej aż czterech certyfikatów,
- zapewnienia szczególnych preferencji w zakresie wystawiania certyfikatów tylko jednemu przedsiębiorstwu,
- zastosowania interfejsu dualnego: stykowego i bezstykowego,
- organizacyjnego rozdziału prepersonalizacji i personalizacji,
- wątpliwości dotyczących rzetelności oszacowania wydatków budżetowych

należy:

1) zlecić ponowne opracowanie *Koncepcji…* ze wskazaniem na konieczność wyeliminowania wyżej wymienianych niedociągnięć. Opracowaniem poprawnego dokumentu powinien się zająć zespół ekspertów specjalizujących się w tematyce dotyczącej dokumentów publicznych. Stworzenie dokumentu, o którym mowa, powinno nastąpić stosunkowo szybko – w przeciągu jednego kwartału,
2) skoordynować projekty pl.ID, krajowy schemat płatniczy (Polska Karta Płatnicza) oraz funkcjonalność KUZ (Platformy P1, P2, P3) w ramach powiązanych ze sobą projektów nadzorowanych przez jeden organ administracji publicznej (np. ministra cyfryzacji),
3) w przypadku decyzji o braku wprowadzenia cech biometrycznych i utrzymaniu braku synchronizacji terminu emisji elektronicznych dowodów osobistych z terminem uruchomienia funkcjonalności KUZ należy rozważyć przesunięcie terminu wdrożenia elektronicznych dowodów osobistych.

Bibliografia:

1. J. Grzemski, A. Krześ, *Analiza pojęcia „przestępstwa godzące w podstawy ekonomiczne państwa" w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 2.

2. W. Gurtefer, A. Pacut, *Człowiek w systemie biometrycznym*, w: *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, M. Tomaszewska-Michalak, T. Tomaszewski (red.), Warszawa 2015, SAWPiA UW.
3. B. Hołyst, J. Pomykała, *Biometria w systemach uwierzytelniania*, „Biuletyn Wojskowej Akademii Technicznej" 2011, nr 4.
4. *Indeks gospodarki cyfrowej i społeczeństwa cyfrowego na 2016 r. Profil krajowy Polska* [online], http://ec.europa.eu/newsroom/dae/document.cfm?action=display&doc_id=14161 [dostęp: 16 I 2017].
5. E. Jakielaszek, *Dokument tożsamości w aspekcie współczesnej przestępczości*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, Volumina.
6. E. Jakielaszek, T. Zwoliński, *Weryfikacja dokumentów – mity a rzeczywistość*, w: *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, M. Tomaszewska-Michalak, T. Tomaszewski (red.), Warszawa 2015, SAWPiA UW.
7. M. Kleiber, K. Szubert, *Słowo w sprawie przyszłości polskiego dowodu osobistego*, „Człowiek i Dokumenty" 2015, nr 38.
8. *Koncepcja wdrożenia polskiego dowodu osobistego z warstwą elektroniczną* [online], https://mc.gov.pl/konsultacje/koncepcja-wdrozenia-polskiego-dowodu-osobistego-z-warstwa-elektroniczna-zapraszamy-do [dostęp: 16 I 2017].
9. R. Lewandowski, *Bezpieczeństwo państwa a bezpieczeństwo dokumentów publicznych i banknotów*, w: M. Goc, T. Tomaszewski, R. Lewandowski, *Kryminalistyka – jedność nauki i praktyki. Przegląd zagadnień z zakresu zwalczania przestępczości*, Warszawa 2016, Volumina.
10. R. Lewandowski, *O potrzebie regulacji sfery dokumentów publicznych*, „Człowiek i Dokumenty" 2016, nr 42.
11. R. Lewandowski, *Analiza nowej koncepcji elektronicznej karty ubezpieczenia zdrowotnego*, „Polski Przegląd Nauk o Zdrowiu" 2016, nr 3.
12. R. Lewandowski, *Evaluation of Legal And Technical Solutions with Respect To New Types of Documents in The Health Care System – KUZ, KSM And KSA,* „Journal of Health Policy, Insurance and Management – Polityka Zdrowotna" 2015, t. 16.
13. R. Lewandowski, T. Goliński, *Nielegalna migracja a bezpieczeństwo identyfikacyjne*, w: *Dokumenty a prawo. Prawne oraz praktyczne aspekty korzystania z dokumentów i e-dokumentów*, M. Tomaszewska-Michalak, T. Tomaszewski (red.), Warszawa 2015, SAWPiA UW.
14. R. Lewandowski, T. Goliński, *Zarządzanie wiarygodnością dokumentów a bezpieczeństwo ekonomiczne*, w: *Zarządzanie w systemie gospodarczym. Szanse i zagrożenia*, K. Raczkowski (red.), Warszawa 2015, Wolters Kluwer.
15. K. Stańczyk, J. Płaczek, *Próba oszacowania bezpieczeństwa finansowego Polski*, w: *Zarządzanie w systemie gospodarczym. Szanse i zagrożenia*, K. Raczkowski (red.), Warszawa 2015, Wolters Kluwer.

Abstrakt

Artykuł przedstawia analizę *Koncepcji wdrożenia polskiego dowodu osobistego z warstwą elektroniczną.* Zidentyfikowano tu istotne słabości projektowanego rozwiązania, w tym m.in. brak zdefiniowanych celów i korzyści projektu, brak synchronizacji terminu rozpoczęcia emisji nowych dokumentów i terminu rozpoczęcia działania funkcjonalności KUZ, pominięcie biometrii przy sporządzaniu nowego typu dowodu osobistego, mnogość certyfikatów oraz zastosowanie interfejsu dualnego. Analiza prowadzi do wniosku o konieczności ponownego opracowania *Koncepcji*… oraz skoordynowania projektu pl.ID z innymi projektami pozostającymi w relacji funkcjonalnej (np. KUZ). W przypadku braku możliwości dopracowania wyżej wymienionego dokumentu należy rozważyć jego zawieszenie.

Słowa kluczowe: dowód osobisty, dokumenty publiczne, bezpieczeństwo identyfikacyjne.

Abstract

The article presents an analysis of the Polish ID with an electronic layer implementation concept. Intrinsic weaknesses of the project have been identified, including a lack of defined goals and project benefits, lack of synchronization of the starting point of new documents emission and the starting point of KUZ functionality, skip the biometrics, multitude of certificates and dual interface. The analysis concludes that the Concept rework is needed and ID.pl project with other functionally correlated projects should be coordinated (eg. KUZ). In case there is no possibility the document was elaborated, its suspension should be taken under consideration.

Keywords: ID, public documents, identification security.

Piotr Chlebowicz

Operacja specjalna jako metoda zwalczania przestępczości zorganizowanej

Uwagi wstępne

Rozwój różnorodnych form zjawiskowych przestępczości zorganizowanej w XX i XXI wieku spowodował, że agendy formalnej kontroli społecznej musiały wdrażać nowe strategie działań wykrywczych oraz poszukiwać nowych technik dowodowych. Klasyczne instrumenty i instytucje zarówno prawa karnego materialnego, jak i procesowego okazywały się bezradne w sprawach karnych dotyczących przestępczości zorganizowanej. Specyfika działania organizacji przestępczych, które stosowały przemoc, korupcję i strach, powodowała, że praca organów ścigania okazywała się nieefektywna nie tylko na etapie ujawniania przestępstw, lecz także przede wszystkim na etapie dowodzenia. Przypisanie sprawstwa i udowodnienie winy członkom grup oraz związków przestępczych w toku postępowania karnego okazywało się bardzo trudne lub niemożliwe. Przewaga zorganizowanych struktur przestępczych nad aparatem państwowym polega na możliwości realizowania przez nie opisanych wyżej działań, a zwłaszcza na sile powiązań w obrębie grupy przestępczej[1]. Można przyjąć, że niezależnie od uwarunkowań geograficznych i kulturowych grupy przestępcze tworzyły normy podkulturowe, które zapewniały im wewnętrzną spoistość. Odnosi się to zwłaszcza do hierarchicznych organizacji przestępczych zbudowanych na kryterium etnicznym, często wzmacnianym więzami klanowymi i rodzinnymi. W przypadku gangów motocyklowych[2], Cosy Nostry, Camorry, gangów albańskich oraz niektórych grup operujących na terenie Federacji Rosyjskiej system norm grupowych umożliwia kontrolę zachowań, ale przede wszystkim kształtuje postawy członków takich struktur. Jednym z rezultatów tych procesów jest hermetyczność grup przestępczych.

Świat przestępczości zorganizowanej – świadomy, że jest przedmiotem działań operacyjnych policji – podejmował i nadal podejmuje próby neutralizowania infiltracji[3]. Przykładem jest obwarowanie członkostwa w grupie spełnieniem wielu warunków. Kandydat na członka grupy przestępczej często jest sprawdzany pod kątem powiązań ze służbami policyjnymi. Niekiedy występuje tzw. instytucja polecenia, która polega na tym, że kandydat jest wskazywany przez członka danej grupy przestępczej[4]. Ta osoba zazwyczaj ponosi odpowiedzialność za polecanego kandydata. Ponadto „kodeksy przestępcze" niejednokrotnie przewidywały surowe sankcje wobec członka grupy, a nawet jego zabójstwo, jeśli zdecydował się na współpracę z policją.

---

[1] Skutki funkcjonowania zorganizowanych struktur przestępczych zostały syntetycznie scharakteryzowane w: J. Błachut, A. Gaberle, K. Krajewski, *Kryminologia*, Gdańsk 2001 r., s. 302–303.

[2] Zob. W. Pływaczewski, *Gangi motocyklowe – konglomerat motocyklowych pasji, skrajnej ideologii i przestępczości*, w: *Współczesne ekstremizmy. Geneza, przejawy, przeciwdziałanie*, W. Pływaczewski, P. Lubiewski (red.), Olsztyn 2014, s. 122–123.

[3] Zob. P. Michna, T. Safjański, J. Żelazek, *Działania kontrwykrywcze zorganizowanych grup przestępczych*, „Przegląd Policyjny" 2006, nr 4, s. 99.

[4] Ten mechanizm występuje także w klasycznych gangach, które cechują się średnim stopniem zorganizowania. Badania kryminologiczne potwierdziły istnienie takich reguł w gangach chuliganów piłkarskich. Por. P. Chlebowicz, *Chuligaństwo stadionowe. Studium kryminologiczne*, Warszawa 2009, s.120.

Właśnie z tego powodu w systemach prawnych USA i państw zachodnich zaczęły pojawiać się nowe instytucje, które miały być skutecznym środkiem zwalczania przestępczości zorganizowanej. Jednym z nich była operacja specjalna. Transformacja ustrojowa w Polsce stworzyła warunki do rozwoju form przestępczości zorganizowanej, które były znane policjom państw zachodnich. Naturalną konsekwencją modernizacji polskich służb policyjnych i specjalnych była także adaptacja instrumentów zwalczania przestępczości zorganizowanej i terrorystycznej, stosowanych w innych krajach, które sprawdziły się w zwalczaniu grup przestępczych i organizacji terrorystycznych. Przedmiotem niniejszego artykułu jest próba przeprowadzenia teoretycznej analizy operacji specjalnej na tle nauki, jaką jest kryminalistyka.

Jak zauważył Hubert Kołecki, jedną z funkcji tej nauki, będącą teoretyczną podbudową praktycznej działalności organów ścigania, jest rozwiązywanie problemów, które pojawiają się w pracy organów ścigania[5]. Geneza tej dyscypliny wiąże się z praktyką wykrywania przestępstw i ścigania ich sprawców. Jan Widacki podkreśla, że kryminalistyka (…) *była zbiorem praktycznych, opartych na doświadczeniu i aktualnym stanie wiedzy (w tym kryminologicznej) zasad postępowania sędziego śledczego i urzędników śledczych, bardziej uporządkowaną praktyką, opisem jej przypadków*[6]. W literaturze przedmiotu występuje wiele definicji kryminalistyki, jednak większość autorów zamieszcza definicję pojęcia taktyki kryminalistycznej. Zazwyczaj jest ona rozumiana jako sposoby i metody postępowania organów ścigania mających doprowadzić do ujawnienia przestępstwa, wykrycia sprawcy, oraz odzyskania mienia, które jest przedmiotem przestępstwa[7]. Wydaje się zatem, że rozważania dotyczące operacji specjalnej należy lokować właśnie w sferze taktyki kryminalistycznej.

Badania dotyczące taktyki działań operacyjno-rozpoznawczych napotykają na liczne przeszkody związane przede wszystkim z brakiem możliwości wglądu badaczy uniwersyteckich w praktykę. Przekłada się to wprost na brak rzetelnych danych faktograficznych. Nie ulega wątpliwości, że nieodłączną część czynności operacyjno-rozpoznawczych stanowi tajność. Z jednej strony poszczególne formy i metody pracy operacyjnej są objęte reżimem ochrony informacji niejawnych. Środowiska policyjne niechętnie odnoszą się do metod pracy operacyjnej oraz uzyskanych na tej podstawie wyników. Z drugiej jednak – eksperci podkreślają, że czynności operacyjno-rozpoznawcze (…) *są niczym więcej, niż metodami zbierania informacji i dowodów przez organy ścigania i mimo że czynności te kojarzą się ze ścisłą tajemnicą, nie ma żadnej czarnej magii co do ich określenia*[8].

W literaturze przedmiotu od dawna postuluje się odtajnienie instrukcji operacyjnych[9]. Zdaniem Adama Tarachy polski ustawodawca powinien skorzystać z rozwiązań prawa policyjnego obowiązującego między innymi w USA. Jako wzorcowe można

[5] H. Kołecki, *Niespójność kryminalistyki uniwersyteckiej z realiami i potrzebami praktyki zwalczania zorganizowanej przestępczości gospodarczej w Polsce*, w: *Nauka wobec współczesnych zagadnień prawa karnego w Polsce. Księga pamiątkowa dedykowana Profesorowi Tobisowi*, B. Janiszewski (red.), Poznań 2004, s. 123.

[6] Zob. szerzej: J. Widacki, *Współczesny zakres nazwy „kryminalistyka"*, „Studia Prawnicze. Rozprawy i materiały" 2013, nr 1, s. 39.

[7] M. Kulicki, V. Kwiatkowska-Darul, L. Stępka, *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2005, s. 42. Zob. też: Z. Czeczot, T. Tomaszewski, *Kryminalistyka ogólna*, Toruń 1996, s. 13.

[8] J.S. Baczyński, *Prokurator w postępowaniu operacyjno-rozpoznawczym*, „Prokurator" 2000, nr 3, s. 20.

[9] Instytut Pamięci Narodowej opracował i udostępnił dokument pod tytułem *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989). Materiały pomocnicze Biura Edukacji Publicznej IPN*, Warszawa 2004. Nawet pobieżna lektura tych materiałów pozwala na zorientowanie się w szczegółach pracy operacyjnej. Można założyć, że mimo zmiany realiów politycznych, przynajmniej część ujawnionych zasad, metod i reguł zachowuje swoją aktualność.

uznać regulacje tajnych operacji policyjnych zawartych w wytycznych prokuratora generalnego USA. W tym dokumencie uregulowano działania nie tylko policyjne, lecz także związane z wywiadem i kontrwywiadem[10]. Nie osłabia to efektywności tych działań, a wręcz przyczynia się do zwiększenia bezpieczeństwa prawnego funkcjonariuszy, którzy realizują operację specjalną. Transparentność procedur związanych z pracą operacyjną sensu largo umożliwia kontrolę tych działań z punktu widzenia standardów demokratycznego państwa prawa. Chodzi tutaj zarówno o nadzór i kontrolę tych czynności ze strony sądu czy prokuratury, jak i o urzeczywistnienie prawa obywateli do prywatności. Trzeba jednak odnotować, że ten pogląd bywa krytykowany. Zdaniem Piotra Kosmatego odtajnienie instrukcji wpłynie negatywnie na proces wykrywczy choćby z tego powodu, że obecnie obowiązujące instrukcje (…) *regulują tematykę zdecydowanie bardziej skomplikowaną i zaawansowaną technicznie*[11].

Polska prokuratura ma niewielkie możliwości faktycznej kontroli praworządności działań operacyjnych między innymi z tego powodu, że prokuratorzy zazwyczaj nie dysponują wiedzą dotyczącą aspektów taktyczno-technicznych tych działań[12]. Warto zauważyć, że niestworzenie ustawy o czynnościach operacyjno-rozpoznawczych pokazuje skalę problemów związanych z regulacją normatywną tej sfery działalności państwa[13].

W dobie społeczeństwa informacyjnego ukrywanie metod pracy policyjnej jest z góry skazane na niepowodzenie[14]. Praca operacyjna, a zwłaszcza współpraca z informatorami policyjnymi oraz przebieg operacji pod przykryciem, jest przedmiotem rozmaitych reportaży prasowych i telewizyjnych. Istnieje obszerna literatura, której autorami często są emerytowani oficerowie służb policyjnych i specjalnych[15]. Ta tematyka jest obecna także w kinie[16]. Jak trafnie stwierdza Piotr Niemczyk, twórczość literacka byłych funkcjonariuszy niebezpiecznie zbliża się do granicy naruszania przepisów o ochronie informacji niejawnych. Jego zdaniem (…) *bardzo wiele opisów jest precyzyjnych,*

[10] Zob. szerzej: A. Taracha, *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006, s. 118–119.

[11] Zob. szerzej: P. Kosmaty, *Granice tajnej inwigilacji obywateli w demokratycznym państwie prawa*, „Prokurator" 2009, nr 3–4, s. 33.

[12] A. Taracha, *Czynności operacyjno-rozpoznawcze*…, s. 112. Bogdan Święczkowski podkreślał natomiast, że kontrola prokuratorska operacji specjalnych jest możliwa i zależy przede wszystkim od motywacji i determinacji prokuratorów. Jego zdaniem: *Prokurator kontrolujący przykrywkowców musi mieć wiedzę o czynnościach operacyjnych, sporo doświadczenia życiowego i szczególny temperament. Bardziej policjant niż urzędnik* (…) *Pomysł był taki, żeby znaleźć prokuratorów, którzy potrafią dochować tajemnicy i którzy z upoważnienia prokuratora okręgowego nadzorowaliby i kontrolowali akcje specjalne*. Zob. szerzej: wywiad z B. Święczkowskim [online], http://kulisy24.com/prawo-i-bezprawie/policjant-wykonujacy-operacje-specjalna-porusza-sie-po-cienkiej-linii [dostęp: 16 II 2016].

[13] Por. T. Tomaszewski, *Projekt ustawy o czynnościach operacyjno-rozpoznawczych – analiza krytyczna*, w: *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, E. Gruza, M. Goc, T. Tomaszewski (red.), Warszawa 2010, s. 347–356.

[14] Warto wskazać witrynę internetową Wikileaks, która niekiedy jest postrzegana jako nowa faza rozwoju dziennikarstwa śledczego, oraz sprawę Edwarda Snowdena. W obu tych przypadkach doszło do ujawnienia wielu wrażliwych danych dotyczących polityki, wywiadu i dyplomacji. Zdaniem P. Kosmatego: *Należy jedynie ubolewać, że wśród wielu praktyków rozpowszechniony jest pogląd, zgodnie z którym wszystko, co wiąże się z działalnością operacyjną, musi być tajne* (…). *Zabawnym jest tworzenie szczelnej kurtyny milczenia okrywającej działania, o których można poczytać w powieściach kryminalnych.* Zob. szerzej: tenże, *Prawo operacyjne*, „Prokurator" 2010, nr 1–2, s. 85.

[15] Por. P. Niemczyk, *Literatura piękna jako źródło informacji o służbach specjalnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13, s. 86 i nast.

[16] Por. na przykład filmy: *Infiltracja* (*The Departed*), w reżyserii Martina Scorsese, *Donnie Brasco* Donniego Newella czy *Życie na podsłuchu* (*Das Leben der Anderen)* Floriana Henckela von Donnersmarcka.

szczegółowych i praktycznych[17]. Cytowany ekspert, który sam ma bogate doświadczenie w pracy w służbach wywiadowczych, zauważa, że: (…) *niektórzy autorzy w opisach środków i metod chronionych przepisami o pracy operacyjno-rozpoznawczej oraz niejawnych sposobów działań służb specjalnych i narzędzi, które one stosują, naruszają zasady nieujawniania tego rodzaju szczegółów*[18]. Być może znakiem naszych czasów jest to, że szeroko rozumiana problematyka szpiegowska zaczyna być poruszana nawet w literaturze dziecięcej[19].

Niejednokrotnie brak profesjonalizmu funkcjonariuszy państwowych prowadzi do dekonspiracji metod pracy policyjnej i jednocześnie obniża prestiż administracji odpowiedzialnej za porządek publiczny i bezpieczeństwo wewnętrzne (casus „agenta Tomka"). Nie jest to specyfika polska, w innych krajach również dochodziło do spektakularnych przecieków, a nawet utraty danych objętych klauzulami tajemnicy państwowej[20]. Należy podkreślić, że tajemnicą powinny być objęte dane osób i konkretne rozwiązania taktyczne stanowiące „kuchnię służb". Wydaje się jednak, że reguły tych operacji, podstawy prawne, granice podejmowanych czynności oraz ogólne schematy działań – znane przecież opinii publicznej, nie wspominając o środowisku przestępczym – mogą i powinny stanowić przedmiot dociekań naukowych. Refleksja naukowa na ten temat mogłaby przyczynić się do rozwoju teorii pracy operacyjnej postulowanej w literaturze przedmiotu[21].

Definicja operacji specjalnej

Pojęcie operacja specjalna zostało przeniesione na grunt polskiej kryminalistyki z doktryny amerykańskiej. Operacja specjalna (ang. *undercover operation* – UCO) to określenie dochodzenia prowadzonego przez tajnego agenta policji, które składa się z serii powiązanych ze sobą działań na przestrzeni pewnego okresu[22]. Sformułowanie „powiązane ze sobą działania" oznacza więcej niż trzy osobiste kontakty agenta z podmiotami, które są przedmiotem operacji[23]. Warto zauważyć, że w zaleceniu nr 31 FATF operację specjalną zdefiniowano jako specjalną technikę śledczą, która powinna być stosowana przez organy ścigania w celu sprawnej walki z procederem prania pieniędzy.

Z dostępnych danych wynika, że w polskiej Policji przygotowania do przeprowadzenia operacji specjalnych pojawiły się w 1994 r. jako element działań Biura do Walki z Przestępczością Zorganizowaną. Po utworzeniu Centralnego Biura Śledczego w jego strukturze wyodrębniono Zarząd Operacji Specjalnych.

Powstaje pytanie o umiejscowienie operacji specjalnej w typologii czynności operacyjno-rozpoznawczych. W kryminalistyce występuje wiele klasyfikacji tego pojęcia. Najczęściej wyróżnia się czynności proste i złożone. Na przykład J. Widacki do pierwszej

[17] P. Niemczyk, *Literatura piękna*…, s. 94.

[18] Tamże, s. 95.

[19] Tamże.

[20] Zob. na przykład: http://wiadomosci.onet.pl/swiat/niemieckie-media-wywiad-pomagal-amerykanom-w-inwigilowaniu-francuzow-i-ke/8ggr9g [dostęp: 23 III 2016], http://www.polskieradio.pl/5/3/Artykul/914697,35-lat-wiezienia-za-przeciek-do-WikiLeaks-Bradley-Manning-skazany [dostęp: 23 III 2016].

[21] Por. S. Koebcke, *Przyczynek do rozważań o teorii pracy operacyjnej*, „Problemy Kryminalistyki" 1981, nr 150.

[22] W. Jasiński, D. Potakowski, *Uregulowania prawne dotyczące amerykańskich operacji „pod przykryciem"*, „Prokuratura i Prawo" 1996, nr 11, s. 77.

[23] Tamże.

grupy zalicza: wywiad, obserwację, współpracę z osobowymi źródłami informacji, korzystanie z informacji zawartych w ewidencji, zakup kontrolowany i przesyłkę kontrolowaną, stosowanie techniki operacyjnej, kontrolę korespondencji, przykrycie oraz legalizację. Czynności złożone obejmują natomiast inwigilację, infiltrację środowisk przestępczych lub kryminogennych, rozpracowanie operacyjne i kombinację operacyjną[24].

Niewątpliwie z punktu widzenia niniejszego artykułu najbardziej interesujące są złożone formy pracy operacyjnej. Warto zwrócić szczególną uwagę na kombinację operacyjną. W projekcie ustawy o czynnościach operacyjno-rozpoznawczych przez k o m b i n a c j ę o p e r a c y j n ą rozumiano (…) *zaplanowane i przygotowane przedsięwzięcie realizowane przy użyciu pozostałych metod pracy operacyjnej, wykorzystujące błędne przeświadczenie osób, przeciwko którym jest skierowane, co do faktycznego znaczenia zaangażowanych zdarzeń oraz osób w nich występujących, służące osiągnięciu celów pracy operacyjnej*[25]. Na podstawie tej definicji można wyodrębnić główną cechę konstytutywną kombinacji specjalnej jako przedsięwzięcia opartego przede wszystkim na podstępie, uprzednio zaplanowanego i ukierunkowanego na osiągnięcie celów związanych z realizacją funkcji wykrywczych i dowodowych[26]. To właśnie kombinacja operacyjna jest podstawą definiowania operacji specjalnej. Twierdzi się bowiem, że operacja specjalna jest szczególną, kwalifikowaną postacią kombinacji operacyjnej[27]. Takie założenie przyjęto podczas prac nad ustawą o czynnościach operacyjno-rozpoznawczych. Operację specjalną zdefiniowano w niej jako szczególny rodzaj kombinacji, której przeprowadzenie cechuje się użyciem działań maskujących. Przez d z i a ł a n i a m a s k u j ą c e rozumie się wykorzystanie obiektów specjalnych stanowiących rzeczowe środki pracy operacyjnej (np. nieruchomości, lokale mieszkalne), użycie dokumentów maskujących oraz wykorzystanie błędnego przeświadczenia o znaczeniu zaistniałej sytuacji[28]. Zdaniem A. Tarachy (…) *tajne, skryte, a także podstępne działania organów ścigania są realizacją zasady równości broni wobec sprawców przestępstwa działających z ukrycia, tajnie, a często także podstępnie*[29].

W historii światowej kryminalistyki odnotowano wiele sukcesów związanych z przeprowadzeniem operacji specjalnych. Jako pierwszą ze współczesnych takich operacji często wymienia się operację FBI o kryptonimie „Abscam" z 1978 r. (opisaną dalej – przyp. red.). Wydaje się jednak, że działania mające widoczne znamiona operacji

[24] Zob. szerzej: *Kryminalistyka*, J. Widacki (red.), Warszawa 2008, s. 128–130.

[25] Projekt ustawy o czynnościach operacyjno-rozpoznawczych, art. 2 ust. 4 pkt 14. Druk sejmowy nr 353 [online], http://orka.sejm.gov.pl/Druki6ka.nsf/wgdruku/353 [dostęp: 29 II 2016]. Warto porównać przytoczoną definicję do definicji zawartej w instrukcji operacyjnej 1970a: Według tego dokumentu był to (…) *zespół planowych przedsięwzięć wzajemnie ze sobą powiązanych i podporządkowanych jednolitej koncepcji dla osiągnięcia założonego celu, np. wprowadzenia do sprawy tajnego współpracownika, uzyskania dowodu przestępnej działalności, zatrzymania osoby podejrzanej*. Istotą „kombinacji operacyjnej (…) *była potajemna interwencja SB w działalność inwigilowanych przez nią osób i środowisk, polegająca na sprowokowaniu nieświadomych osób do określonych działań*. Por. http://inwentarz.ipn.gov.pl/slownik?znak=K [dostęp: 17 II 2016].

[26] Jak zauważył B. Kurzępa: *Panuje zgodne przekonanie, że jest on charakterystycznym sposobem postępowania przy tych czynnościach* (chodzi o czynności operacyjno-rozpoznawcze – wtrącenie aut.) *i nie ma powodów, aby został wyeliminowany z arsenału metod walki z przestępczością.* Zob. B. Kurzępa, *Podstęp w toku czynności karnoprocesowych i operacyjnych*, Toruń 2003, s. 179.

[27] Zob. na przykład: E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2011, s. 68.

[28] Por. M. Chrabkowski, *Metody pracy operacyjnej*, w: *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), Szczytno 2013, s. 514.

[29] A. Taracha, *Czynności operacyjno-rozpoznawcze*…, s. 50.

specjalnych były stosowane znacznie wcześniej. Geneza francuskiej policji kryminalnej wiąże się z utworzeniem w 1812 r. Brygady Bezpieczeństwa (fr. Brigade de Sûreté). Jej twórca, Eugene-François Vidocq, zastosował metodę polegającą na wnikaniu w środowiska przestępcze, zbieraniu informacji i stosowaniu prowokacji. Nieodłącznym elementem tych działań był kamuflaż[30]. Z kolei w USA techniki charakterystyczne dla operacji specjalnej wykorzystywano na długo przed powstaniem FBI[31].

Przykłady współczesnych operacji specjalnych

W 1978 r. FBI rozpoczęła, wspomnianą już, operację pod kryptonimem „Abscam", która miała na celu wykrycie korupcji politycznej. Agenci FBI występowali pod legendą, podając się za arabskich biznesmenów. Mieli oni rzekomo stworzyć sprzyjające warunki do prowadzenia interesów przez fikcyjnego szejka Kambira Abdula Rahmana. Szejk zamierzał kupić azyl w USA, uzyskać pomoc w transferze jego pieniędzy z ojczystego kraju oraz rozpocząć „proces inwestycyjny". Agenci spotykali się z różnymi członkami Kongresu Stanów Zjednoczonych i Senatu USA, obiecywali gotówkę w zamian za azyl polityczny oraz inne korzyści dla szejka. Spotkania z politykami nagrywano, dokumentując kompromitujące sytuacje. Na przykład na jednym z takich nagrań kongresman z Florydy Richard Kelly po wypchaniu sobie kieszeni 25 tys. dolarów zapytał agenta pod przykryciem, czy coś widać[32].

Podczas przeprowadzania rozmów odnotowano także zachowania zasługujące na uznanie. Na przykład republikański senator z Dakoty Południowej Larry Pressler, jeden z 31 polityków objętych obserwacją FBI, po usłyszeniu propozycji przyjęcia łapówki w zamian za podjęcie działań na rzecz wspomnianego szejka Rahmana, odpowiedział: *Chwileczkę, to, co proponujesz, może być nielegalne*, po czym zawiadomił organy ścigania o próbie popełnienia przestępstwa[33].

Innym przykładem jest zainicjowanie przez FBI w 1975 r. operacji o kryptonimie „Donnie Brasco". Podczas jej przeprowadzania funkcjonariuszom udało się uplasować agenta w strukturach mafii. Ów agent, Joe Pistone, w ciągu sześciu lat zebrał dowody pozwalające na skazanie ponad stu gangsterów[34]. Operację przerwano w momencie, gdy J. Pistone otrzymał propozycję pełnoprawnego członkostwa w mafii, co wiązało się ze zleceniem mu zabójstwa. Skuteczność działań FBI sprawiła, że mafia wyznaczyła nagrodę za głowę agenta. Było to wydarzenie bez precedensu, gdyż dotychczas struktury mafijne unikały dokonywania zabójstw funkcjonariuszy FBI.

Znana jest również operacja „Dinero" zrealizowana przez amerykańską DEA (ang. Drug Enforcement Administration) wspólnie z policjami: kolumbijską, włoską

[30] Zob. szerzej: G. Feix, *Wielkie ucho Paryża*, Katowice 1988.

[31] Chodzi o działalność detektywistyczną Pinkertona: „Nie cenili co prawda szpiclów rekrutujących się ze świata przestępczego, natomiast sami w setkach przebrań przenikali do ośrodków wielkich band, do miast „Dzikiego Zachodu", którymi te bandy władały. W Seymour, twierdzy bandy Reno, która 6 października 1866 r. dokonała pierwszego napadu na pociąg na zachodzie Ameryki, osiedlił się jeden z ludzi Pinkertona, Dick Winston, jako właściciel baru i z wolna zaprzyjaźnił się z bandą Reno. A potem wywabił Johna Reno na peron w Seymour w momencie, kiedy Allan Pinkerton i sześciu jego ludzi zajechało na stację małym pociągiem specjalnym. Pochwycono Johna Reno i pociąg z więźniem odjechał, zanim reszta bandy pojęła, co się stało". Zob. szerzej: J. Thorwald, *Stulecie detektywów. Drogi i przygody kryminalistyki*, Kraków 1971, s. 94.

32 Opis operacji Abscam oparto na informacjach znajdujących się na stronach http://cba.gov.pl/pl/newsy-serwisu-antykorup/642,Dyrektywy-dotyczace-tajnych-dzialan-FBI.html [dostęp: 17 II 2016] oraz https://pl.wikipedia.org/wiki/Abscam [dostęp: 17 II 2016].

[33] Tamże.

[34] Zob. szerzej: C. Sifakis, *Mafia amerykańska. Encyklopedia*, Kraków 2007, s. 56–57.

i hiszpańską. Funkcjonariusze DEA, podając się za biznesmenów, rozpoczęli starania, aby otrzymać licencję bankową klasy B na Anquilli. Czas jej otrzymania – według standardowej procedury – trwa około roku. W ramach marketingu przygotowano materiały reklamowe przyszłego banku wydane w trzech językach: greckim, francuskim i hiszpańskim. Po uzyskaniu licencji bank rozpoczął działalność. Zachowania agentów pod przykryciem w niczym nie odbiegały od zachowań przyjętych w kręgach biznesowych (zarząd banku jadał w ekskluzywnej restauracji, miał do dyspozycji własny samolot itd.). Wiesław Jasiński podkreśla, że wpłaty dolarów poczodzących z narkotykowego biznesu rozpoczęły się niemalże od momentu otwarcia banku. Osób, które brały udział w praniu pieniędzy, nie zniechęcała marża sięgająca 18 proc. wartości wpłaconej sumy. Schemat przelewów zazwyczaj polegał na wpłatach dolarów na konta we Włoszech i Francji, skąd transferowano je do Kolumbii. Przez miesiąc funkcjonowania „banku" obroty wyniosły około 20 mln dolarów. Rezultatem akcji „Dinero" było aresztowanie ponad 100 przestępców, konfiskata 33 mln dolarów i 9 ton kokainy[35].

Próba analizy teoretycznej operacji specjalnej

Wydaje się, że kryminalistyczna charakterystyka przedsięwzięcia określanego jako operacja specjalna powinna uwzględniać następujące elementy:

- cel operacji specjalnych,
- typologię operacji specjalnych,
- zasady prowadzenia operacji specjalnych,
- tajnego agenta policji (ang. *undercover agent)*, który przeprowadza operację.

Z operacjami specjalnymi są połączone także specyficzne komponenty taktyczno-techniczne, takie jak działania maskujące, które obejmują stworzenie tzw. legendy oraz użycie dokumentów legalizacyjnych.

W niniejszym artykule zdecydowano się pominąć dwa ostatnie zagadnienia. Warto podkreślić, że oprócz operacji specjalnych, które są prowadzone przez służby policyjne, istnieją operacje wykonywane w ramach zadań kontrwywiadu i wywiadu. Stanowią one jednak odrębną kategorię działań, gdyż ich istota i priorytety zdecydowanie różnią się od klasycznych operacji policyjnych[36].

Ogólne cele operacji specjalnej mieszczą się w celach czynności operacyjno-rozpoznawczych. Jak wiadomo, są one prowadzone po to, aby rozpoznawać środowiska przestępcze, wykrywać przestępstwa i ich sprawców, udowadniać winę sprawcom przestępstw, a także zapobiegać przestępczości[37]. Janusz Gołębiewski wyróżnia takie cele czynności operacyjno-rozpoznawczych, jak: ustalanie źródeł dowodowych w postępowaniu karnym, ustalanie składów osobowych grup przestępczych, ujawnianie przestępstw, umożliwienie zatrzymywania sprawców, ustalanie miejsc ukrywania się osób poszukiwanych przez organy ścigania, miejsc pobytu osób zaginionych oraz miejsc przetrzymywania osób uprowadzonych[38]. Chodzi zatem o realizację zarówno funkcji wykrywczej, jak

[35] W. Jasiński, *Przeciw szarej strefie. Nowe zasady zapobiegania praniu pieniędzy*, Warszawa 2001, s. 225; J.W. Wójcik, *Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne*, Warszawa 2011, s. 474–475.

[36] Wynika to z różnic między klasycznymi służbami specjalnymi a służbami policyjnymi. Szerzej na ten temat zob. M. Bożek i in., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014. Por. M. Minkina, *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, s. 336 i nast.

[37] S. Pikulski, *Działania operacyjne Policji*, „Wojskowy Przegląd Prawniczy" 1996, nr 2, s. 53.

[38] J. Gołębiewski, *Praca operacyjna w zwalczaniu przestępczości zorganizowanej*, Warszawa 2008, s. 21–22.

i dowodowej. Wydaje się, że szczególną cechą operacji specjalnej jest właśnie harmonijne połączenie tych dwóch funkcji. A. Taracha podkreśla, że sprzężenie funkcji wykrywczej i dowodowej polega na połączeniu (…) *zbierania materiału dowodowego z możliwością prowadzenia przez tajnego agenta inwigilacji organizacji przestępczej*. Jego zdaniem przesądza to o tym, że operacja specjalna jest najskuteczniejszym środkiem w arsenale technik i metod pracy operacyjnej[39]. W. Jasiński podkreśla zaś, że miernikiem efektywności operacji specjalnej jest jakość dowodów zebranych podczas jej przeprowadzania. Z tego powodu za skuteczną – tzn. taką, która zrealizowała założone cele – uważa się operację, której wyniki doprowadziły do prawomocnego skazania za przestępstwo. Jego zdaniem średni światowy wskaźnik skuteczności wynosi około 20 proc.[40]

Jeśli uwzględni się kryterium celu, to okazuje się, że operacja specjalna występuje w wielu różnych odmianach. W literaturze przedmiotu dotyczącej problematyki prania pieniędzy W. Jasiński wskazał cztery typy operacji specjalnych:

1. **Operacje infiltracyjne**. Są one przeprowadzane, gdy nie ma innych możliwości wykrycia sprawców W tej sytuacji operacyjnej nie ma żadnych możliwości uzyskania dowodów. W danej sprawie występuje zatem brak operacyjnego dotarcia do osób piorących pieniądze (określanych w środowisku służb i w kryminalistyce słowem „pracze"). W tym przypadku takie działania są w zasadzie jedynym środkiem, którego mogą używać służby policyjne i specjalne. Infiltracja stanowi zatem jaskrawy przykład tzw. ofensywnych metod pracy operacyjnej.
2. **Operacje zakupów kontrolowanych**. Eksponuje się tu funkcję dowodową. Według W. Jasińskiego istota operacji polega na uzyskaniu dowodów przeciwko grupie piorącej pieniądze lub pojedynczej osobie. Odbywa się to przez przyjęcie od nich pieniędzy, które mają być wymienione, lub uczestniczenie w sprzedaży nieruchomości lub mienia ruchomego za fundusze nielegalne.
3. **Operacje specjalne** polegające na kontrolowanym wręczeniu lub przyjęciu korzyści majątkowej.
4. **Operacje maskujące**. Są to operacje, które służą przygotowaniu bazy dla następnych operacji. Ich celem jest maskowanie działań służb policyjnych oraz przygotowanie legendy dla policjantów działających pod przykryciem. Mogą one być wykorzystywane w innych przedsięwzięciach[41].

Mimo że zaprezentowany podział odnosi się do procederu prania pieniędzy, to prawdopodobnie ma on walor ogólniejszy.

Organizacja operacji specjalnej jest przedsięwzięciem skomplikowanym, które z samej istoty jest balansowaniem na krawędzi ryzyka. Z tego powodu w praktyce organów ścigania wypracowano zasady minimalizujące ewentualne niepowodzenia oraz zwiększające prawdopodobieństwo odniesienia sukcesu, jeśli te zasady są przestrzegane[42]. Część z nich wykazuje podobieństwo do klasycznych zasad taktyki kryminalistycznej. Szczególnie warto tu wskazać zasady: tajności oraz organizacji walki. Pierwsza

[39] A. Taracha, *Czynności operacyjno-rozpoznawcze*…, s. 113.

[40] W. Jasiński, *Prawne i kryminalistyczne aspekty wykrywania przestępstwa prania pieniędzy*, w: *Proceder prania pieniędzy i jego implikacje*, E.W. Pływaczewski (red.), Warszawa 2013, s. 204.

[41] W. Jasiński, *Prawne i kryminalistyczne aspekty*…, s. 205.

[42] Obrazuje to następująca opinia: *Przykrywowiec to tylko szpica, na którą pracuje cały zespół ludzi wyposażony w skomplikowaną i drogą infrastrukturę: wynajęte lokale konspiracyjne, samochody kupowane często na potrzeby jednej konkretnej operacji, fikcyjne firmy, ich biura, telefony i cała szpiegowska elektronika*. Zob. szerzej: I.T. Miecik, *Wtyką będę ja* [online], http://www.newsweek.pl/wtyka-bede-ja,49122,1,1.html [dostęp 16 II 2016].

z nich sprowadza się do obowiązku zachowania tajemnicy podejmowanych działań, ewentualne odstępstwa mogą być uzasadnione wymogami proceduralnymi lub określonymi względami taktycznymi[43]. Przykładem przestrzegania zasady tajności w odniesieniu do operacji specjalnej jest akcja ABW o kryptonimie „Gringo", w którą było zaangażowanych około trzystu funkcjonariuszy Agencji. Na potrzeby tej operacji stworzono wewnętrzny system kontroli w celu zapobieżenia przeciekom[44].

Zasada organizacji walki jest w literaturze kryminalistycznej rozumiana jako interakcja w warunkach tzw. kooperacji negatywnej[45]. Operację specjalną można nazwać działaniem opartym na inicjatywie, podstępie, przy czym nie chodzi o zniszczenie przeciwnika (sprawcy, grupy sprawców) w sensie militarnym, a o pozbawienie go kamuflażu, zniszczenie anonimowości i fałszywych argumentów obrony[46]. W. Kulicki podkreśla, że *Walka nierzetelna, w której arogancko stosuje się metody nieetyczne i bezprawne (presję fizyczną, poniżanie godności osobistej, szantaż, udręczenie psychiczne, podżeganie do relacjonowania narzuconych treści, wprowadzanie w błąd co do przysługujących uprawnień), jest, w zestawieniu z zasadami kryminalistycznej taktyki walki, alternatywą nieporównywalnie gorszą*[47]. Zasadę organizacji walki należy zatem interpretować jako prakseologiczną dyrektywę skutecznego działania, którego granice wyznacza nie tylko praw, lecz także etyka zawodowa. Na przykład agenci specjalni FBI składają przyrzeczenie, że podczas realizowanej operacji specjalnej będą przestrzegać kodeksu policyjnego i etycznego, w których kładzie się nacisk na ochronę osób niewinnych[48].

Pierwszą zasadą kształtującą założenia operacji specjalnej jest zasada subsydiarności. Oznacza ona, że inicjowanie tych działań jest zasadne wówczas, gdy nie istnieją lub zostały wyczerpane inne możliwości działań wykrywczych i dowodowych. Z uwagi na wyjątkowość tej techniki śledczej jest ona stosowana w skomplikowanych sprawach o dużym ciężarze gatunkowym, takich jak: handel narkotykami, obrót bronią[49] i materiałami rozszczepialnymi – prowadzonych przez zorganizowane grupy przestępcze – rozpracowywanie organizacji terrorystycznych, pranie pieniędzy i finansowanie terroryzmu. Zasada subsydiarności łączy się także z aspektem finansowym. Ocenia się, że operacja specjalna to najdroższa forma pracy operacyjnej. Podkreślenia wymaga również to, że w USA (…) *wartość odzyskanego, a także skonfiskowanego mienia od osób rozpracowywanych, corocznie 10-krotnie przekracza koszt ich prowadzenia*[50].

Ważną zasadą jest planowanie operacji specjalnej. Jak zauważa W. Jasiński, *Planowanie operacji rozpoczyna się od analizy materiałów zgromadzonych podczas wcześniej realizowanych czynności operacyjno-rozpoznawczych, postępowań przygotowawczych związanych z rozpracowywanymi sprawcami*[51]. Głównym elementem planowania jest wykorzystanie nowoczesnych technik analitycznych stosowanych w ramach analizy kryminalnej. Jest to ciekawe zagadnienie, którego znaczenie podkreślali Jacek Kudła i Piotr Kosmaty. Ich zdaniem (…) *stosowanie metod analitycznych do oceny obszarów*

[43] Zob. szerzej: M. Kulicki, V. Kwiatkowska-Darul, L. Stępka, *Kryminalistyka*…, s. 48.

[44] Zob. szerzej: B. Wróblewski, *Infiltracja, tona koki i polski „general"*, http://wyborcza.pl/1,76842,9357915,Infiltracja_tona_koki_i_polski_general_.html [dostęp 31 I 2017].

[45] M. Kulicki, V. Kwiatkowska-Darul, L. Stępka, *Kryminalistyka*…, s. 48.

[46] Tamże.

[47] Tamże, s. 50.

[48] Zob. szerzej: B. Hołyst, *Psychologia kryminalistyczna*, Warszawa 2009, s. 1252.

[49] Zob. P. Chlebowicz, *Nielegalny handel bronią. Studium kryminologiczne*, Warszawa 2015.

[50] W. Jasiński, D. Potakowski, *Uregulowania prawne*…, s. 85.

[51] W. Jasiński, *Prawne i kryminalistyczne aspekty*…, s. 203.

ryzyka operacyjnego w pełni uzupełni istniejący deficyt informacji, niezbędnych do zapewnienia prawidłowego wszczęcia i prowadzenia czynności[52]. Efektywność planowania wymaga, aby jego zakres objął wszystkie poszczególne elementy operacji specjalnej, takie jak: dotarcie do rozpracowywanej grupy i jej najbliższego otoczenia, taktyka zabezpieczenia policjantów działających pod przykryciem, całokształt spraw związanych z maskowaniem policjantów pod przykryciem (scenariusze „awaryjne", modyfikacja legendy itd.), finansowanie kolejnych etapów operacji, wykorzystywanie materiałów uzyskanych w toku ich przeprowadzania na potrzeby postępowania karnego, rozłożenie odpowiedzialności za poszczególne czynności lub całą operację specjalną[53].

Najważniejszym komponentem operacji specjalnej jest funkcjonariusz Policji, który przenika do struktur przestępczych i prowadzi działania mające na celu zebranie dowodów przestępnej działalności. W praktyce polskiej mianem o p e r a t o r a określa się policjanta pod przykryciem. Warunkiem skuteczności operacji jest nie tylko poziom wyszkolenia, lecz także cechy osobowości „przykrywkowca".

Kolejną przesłanką powodzenia operacji specjalnej jest właściwy dobór zespołu, który ją prowadzi. Głównym zagadnieniem jest problem bezpieczeństwa policjanta pod przykryciem. Jako źródło zagrożeń wymienia się przede wszystkim jego dekonspirację. Zagrożenia wynikają także z możliwości dekonspiracji informatorów, którzy współpracują z przykrywkowcem, możliwości popełnienia przestępstwa wobec kadrowego funkcjonariusza służby policyjnej lub specjalnej, podejmowania przez rozpracowywaną grupę przestępczą działań testujących lojalność policjanta pracującego pod przykryciem, ujawnienie działań Policji wobec grupy stanowiącej cel operacji[54].

Trzeba zwrócić szczególną uwagę na psychologiczne aspekty tego przedsięwzięcia. Koszty psychiczne ponoszone przez policjanta – przykrywkowca, związane z utrzymywaniem tzw. ukrytej tożsamości (ang. *cover identity*), są ogromne. Odnotowywano przypadki załamań psychicznych agentów kończące się alkoholizmem, uzależnieniem od narkotyków, pojawianiem się silnych zaburzeń emocjonalnych, a nawet epizodów psychotycznych. Poważnym problemem obserwowanym w praktyce jest także więź psychiczna, która wytwarza się podczas operacji specjalnej pomiędzy przykrywkowcem a członkami grupy. To zjawisko określa się mianem „tajnego syndromu sztokholmskiego"[55]. Jak stwierdził jeden z praktyków: *To gigantyczna próba charakteru. Potrzebne są nie tylko odwaga, inteligencja czy talent aktorski, ale przede wszystkim wewnętrzna dyscyplina. Wiadomo, młody chłopak plus duża kasa, plus adrenalina równa się kłopoty. Stąd ogromna rola nadzoru, prowadzenia, kontroli. Kaganiec i smycz*[56]. Permanentny stres, który towarzyszy funkcjonariuszowi pod przykryciem, wymaga nie tylko odpowiedniego przygotowania, lecz także właściwej opieki psychologicznej – i to zarówno podczas trwania operacji, jak i po jej zakończeniu.

Podsumowanie

Problematyka dotycząca operacji specjalnych to interesujący obszar badawczy, który zasługuje na uwagę. Podkreślano problemy związane z refleksją naukową w tym

[52] Zob. szerzej: J. Kudła, P. Kosmaty, *Ryzyko w czynnościach operacyjno-rozpoznawczych Policji. Aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2013, s. 39.

[53] W. Jasiński, *Prawne i kryminalistyczne aspekty*…, s. 203.

[54] Tamże, s. 204.

[55] Zob. szerzej: B. Hołyst, *Psychologia*…, s. 1248 wraz z przywołaną literaturą.

[56] I.T. Miecik, *Wtyką będę ja*…

zakresie praktyki kryminalistycznej. Doświadczenia zebrane podczas zakończonej operacji specjalnej powinny być przedmiotem analiz i badań, aby ulepszać rozwiązania taktyczne, eliminować błędy i wyciągać wnioski na przyszłość. Wydaje się, że to zadanie może być realizowane na przykład przez analityków kryminalnych w ramach analizy prowadzenia sprawy[57]. Należy zatem postulować wykorzystanie wiedzy i doświadczeń całego zespołu, który prowadził daną operację. Ta wiedza jest cennym kapitałem, którego właściwe zastosowanie może przełożyć się na efektywność działań wykrywczych służb policyjnych i specjalnych.

Bibliografia:

1. Baczyński S., *Prokurator w postępowaniu operacyjno-rozpoznawczym*, „Prokurator" 2000, nr 3.
2. Błachut J., Gaberle A., Krajewski K., *Kryminologia*, Gdańsk 2001, Arche.
3. Bożek M. i in., *Służby specjalne w strukturze władz publicznych. Zagadnienia prawnoustrojowe*, Warszawa 2014, Wolters Kluwer.
4. Chlebowicz P., *Chuligaństwo stadionowe. Studium kryminologiczne*, Warszawa 2009, Wolters Kluwer.
5. Chlebowicz P., *Nielegalny handel bronią. Studium kryminologiczne*, Warszawa 2015, Wolters Kluwer.
6. Chlebowicz P., Kamińska J., *Operacyjna analiza kryminalna w służbach policyjnych*, Warszawa 2015, Difin.
7. Chrabkowski M., *Metody pracy operacyjnej*, w: *Przestępczość zorganizowana. Fenomen. Współczesne zagrożenia. Zwalczanie. Ujęcie praktyczne*, W. Jasiński, W. Mądrzejowski, K. Wiciak (red.), Szczytno 2013, Wydawnictwo Wyższej Szkoły Policji w Szczytnie.
8. Czeczot Z., Tomaszewski T., *Kryminalistyka ogólna*, Toruń 1996, Comer.
9. Feix G., *Sûreté. Wielkie ucho Paryża*, Katowice 1988, Śląsk.
10. Gołębiewski J., *Praca operacyjna w zwalczaniu przestępczości zorganizowanej*, Warszawa 2008, Wydawnictwa Akademickie i Profesjonalne.
11. Gruza E., Goc M., Moszczyński J., *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2011, Wydawnictwa Akademickie i Profesjonalne.
12. Hołyst B., *Psychologia kryminalistyczna*, Warszawa 2009, LexisNexis.
13. *Instrukcje pracy operacyjnej aparatu bezpieczeństwa (1945–1989)*, T. Ruzikowski (oprac. i wstęp), Warszawa 2004, IPN [Materiały pomocnicze Biura Edukacji Publicznej IPN].
14. Jasiński W., *Prawne i kryminalistyczne aspekty wykrywania przestępstwa prania pieniędzy*, w: *Proceder prania pieniędzy i jego implikacje*, E.W. Pływaczewski (red.), Warszawa 2013, Wolters Kluwer.
15. Jasiński W., *Przeciw szarej strefie. Nowe zasady zapobiegania praniu pieniędzy*, Warszawa 2001, Poltex.
16. Jasiński W., Potakowski D., *Uregulowania prawne dotyczące amerykańskich operacji „pod przykryciem"*, „Prokuratura i Prawo" 1996, nr 11.
17. Koebcke S., *Przyczynek do rozważań o teorii pracy operacyjnej*, „Problemy Kryminalistyki" 1981, nr 150.

[57] Zob. P. Chlebowicz, J. Kamińska, *Operacyjna analiza kryminalna w służbach policyjnych*, Warszawa 2015, s. 182.

18. Kołecki H., *Niespójność kryminalistyki uniwersyteckiej z realiami i potrzebami praktyki zwalczania zorganizowanej przestępczości gospodarczej w Polsce*, w: *Nauka wobec współczesnych zagadnień prawa karnego w Polsce. Księga pamiątkowa dedykowana Profesorowi Tobisowi*, B. Janiszewski (red.), Poznań 2004, Wydawnictwo Poznańskie.
19. Kosmaty P., *Granice tajnej inwigilacji obywateli w demokratycznym państwie prawa*, „Prokurator" 2009, nr 3–4.
20. Kosmaty P., *Prawo operacyjne*, „Prokurator" 2010, nr 1–2.
21. *Kryminalistyka*, Widacki J. (red.), Warszawa 2008, C.H.Beck.
22. Kudła J., Kosmaty P., *Ryzyko w czynnościach operacyjno-rozpoznawczych Policji. Aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2013, Difin.
23. Kulicki M., Kwiatkowska-Darul V., Stępka L., *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2005, Wydawnictwo UMK.
24. Kurzępa B., *Podstęp w toku czynności karnoprocesowych i operacyjnych*, Toruń 2003, Wydawnictwo TNOiK.
25. Michna P., Safjański T., Żelazek J., *Działania kontrwykrywcze zorganizowanych grup przestępczych*, „Przegląd Policyjny" 2006, nr 4.
26. Minkina M., *Sztuka wywiadu w państwie współczesnym*, Warszawa 2014, Rytm.
27. Niemczyk P., *Literatura piękna jako źródło informacji o służbach specjalnych*, „Przegląd Bezpieczeństwa Wewnętrznego" 2015, nr 13.
28. Widacki J., *Współczesny zakres nazwy „kryminalistyka"*, „Studia Prawnicze. Rozprawy i materiały" 2013, nr 1.
29. Wójcik J.W., *Przeciwdziałanie przestępczości zorganizowanej. Zagadnienia prawne, kryminologiczne i kryminalistyczne*, Warszawa 2011, Wolters Kluwer.
30. Pikulski. S., *Działania operacyjne Policji*, „Wojskowy Przegląd Prawniczy" 1996, nr 2.
31. Pływaczewski W., *Gangi motocyklowe – konglomerat motocyklowych pasji, skrajnej ideologii i przestępczości*, w: *Współczesne ekstremizmy. Geneza, przejawy, przeciwdziałanie*, W. Pływaczewski, P. Lubiewski (red.), Olsztyn 2014, Katedra Kryminologii i Polityki Kryminalnej, WPiA, Uniwersytet Warmińsko-Mazurski w Olsztynie.
32. Sifakis C., *Mafia amerykańska. Encyklopedia*, Kraków 2007, Universitas.
33. Taracha A., *Czynności operacyjno-rozpoznawcze. Aspekty kryminalistyczne i prawnodowodowe*, Lublin 2006, Wyd. UMCS.
34. Thorwald J., *Stulecie detektywów. Drogi i przygody kryminalistyki*, Kraków 1971, Znak.
35. Tomaszewski T., *Projekt ustawy o czynnościach operacyjno-rozpoznawczych – analiza krytyczna*, w: *Co nowego w kryminalistyce – przegląd zagadnień z zakresu zwalczania przestępczości*, E. Gruza, M. Goc, T. Tomaszewski (red.), Warszawa 2010, Stowarzyszenie Absolwentów WPiA UW.

Źródła internetowe:

1. http://cba.gov.pl/pl/newsy-serwisu-antykorup/642,Dyrektywy-dotyczace-tajnych-dzialan-FBI.html [dostęp: 17 II 2016].
2. http://inwentarz.ipn.gov.pl/slownik?znak=K [dostęp: 17 II 2016].
3. https://pl.wikipedia.org/wiki/Abscam [dostęp: 17 II 2016].
4. http://wiadomosci.onet.pl/swiat/niemieckie-media-wywiad-pomagal-amerykanom-w-inwigilowaniu-francuzow-i-ke/8ggr9g [dostęp: 23 III 2016].

5. http://www.polskieradio.pl/5/3/Artykul/914697,35-lat-wiezienia-za-przeciek-do-WikiLeaks-Bradley-Manning-skazany [dostęp: 23 III 2016].
6. http://wyborcza.pl/1,76842,9357915,Infiltracja__tona_koki_i_polski__general_.html [dostęp: 17 II 2016].
7. Miecik I.T., *Wtyką będę ja* [online], http://www.newsweek.pl/wtyka-bede-ja,49122,1,1.html [dostęp: 16 II 2016].

Abstrakt

Operacje specjalne stanowią użyteczne narzędzie w zwalczaniu zaawansowanych form przestępczości grupowej, takich jak przestępczość zorganizowana i terrorystyczna. W literaturze przedmiotu podkreśla się trudności związane z badaniami tej sfery działań służb policyjnych i specjalnych. Wynika to nie tylko z ustawowych rygorów dotyczących informacji niejawnych, lecz także z mentalności i kultury organizacyjnej służb odpowiedzialnych za bezpieczeństwo wewnętrzne państwa. Mimo tych ograniczeń, istnieją wystarczające dane, aby spróbować opisać operację specjalną z teoretycznego punktu widzenia.

Artykuł przedstawia charakterystykę operacji specjalnej z punktu widzenia nauki, jaką jest kryminalistyka. Przybliżono tu definicję oraz historyczne uwarunkowania tej instytucji. Podkreślono, że elementy właściwe dla operacji specjalnej były obecne w działaniach już pierwszych formacji policyjnych. W artykule przedstawiono operację specjalną na tle czynności kryminalistycznych oraz zaprezentowano teoretyczną analizę poszczególnych ogniw, które na nią się składają.

Słowa kluczowe: kryminalistyka, operacja specjalna, definicja i typologia operacji specjalnej, funkcjonariusz pod przykryciem.

Abstract

Special operations are useful tool in combating advanced forms of organized crime, like classical organized crime or terrorist activities. In the literature it is stressed that there are many problems with the examination of law enforcement and special services' activities. It is the result of both legal restrictions coming from the legislation on classified information and the mentality and organizational culture of the services responsible for the internal security of the state. Nevertheless there are sufficient data the special operation could be described from the theoretical point of view.

The article provides characteristics of the special operation in the narrow view of forensics. It explains the definition of a special operation and its historical background. It stresses that features of special operations were present in the activities of the first police forces. It also presents a special operation among forensic activities and theoretical analysis of all the links constituting a special operation.

Keywords: forensics, special operation, definition and typology of special operations, undercover agent.

III
RECENZJE

Robert Borkowski

Daniel Estulin, *W imię Allaha. Jak Zachód stworzył, sponsorował i rozpętał piekło islamskiego terroru*[1]

Wzrost politycznego znaczenia terroryzmu w pierwszym dwudziestoleciu XXI w. pociąga za sobą pytania o przyszłość świata, który wpadł w pułapkę nietolerancji, ksenofobii i przemocy. Wielką niewiadomą staje się dziś kierunek ewolucji światowego systemu bezpieczeństwa, w tym rozwój sytuacji na Bliskim Wschodzie. Oddziaływanie fali terroryzmu jest obecnie daleko silniejsze niż kiedykolwiek wcześniej. Powstają uzasadnione obawy o przyszłość demokracji, zagrożonej zaostrzonymi wymogami dotyczącymi bezpieczeństwa państwowego w związku z kampanią antyterrorystyczną. Przyszłość jawi się jako odejście od porządku demoliberalnego na rzecz nieokreślonej jeszcze formy pełzającego stanu wyjątkowego. Konflikt pomiędzy swobodami obywatelskimi a potrzebą zapewnienia bezpieczeństwa publicznego pociąga za sobą pytanie o to, czy w atmosferze strachu, podejrzliwości oraz niechęci rasowej i religijnej będzie możliwe uratowanie demokratycznych wartości. W sytuacji zagrożenia instytucje państwa, a ściślej rzecz biorąc – aparat przymusu (wojsko, policja, a zwłaszcza służby specjalne) – zyskują szczególne prerogatywy i rozciągają nad obywatelami szeroką kontrolę (transakcji finansowych, korespondencji, rozmów, głoszonych poglądów, przekonań politycznych, religijnych itp.). Pojawiają się naciski ze strony służb dotyczące zwiększenia puli środków przeznaczonych na ich działania i na poszerzanie ich uprawnień kosztem swobód obywatelskich.

W ostatnim piętnastoleciu powstało wiele publikacji poświęconych terroryzmowi, fundamentalizmowi islamskiemu i konfliktom na Bliskim Wschodzie. W Polsce problematyka dotycząca terroryzmu i bezpieczeństwa wysunęła się na pierwsze miejsce wśród nauk społecznych. Większość prac jest jednak wtórna i odtwórcza wobec publikacji czołowych badaczy i generuje zjawisko, które można by nazwać pop-nauką. Coraz rzadziej można liczyć na pojawienie się książki, której autor sformułuje nowe problemy badawcze, zaproponuje nowe metody badania terroryzmu lub choćby przedstawi nowatorskie ujęcie perspektywy poznawczej albo ocenę zachodzących współcześnie procesów – odmienne od konformistycznego ogółu.

Ostatni z wymienionych postulatów spełnia niewątpliwie książka Daniela Estulina. Praca tego hiszpańskiego dziennikarza śledczego może wzbudzić silne emocje u czytelników już samym podtytułem polskiego wydania, zawierającym szokującą w istocie tezę: *Jak Zachód wykreował, sfinansował i rozpętał piekło islamskiego terroryzmu*. D. Estulin jest znany z kontrowersyjnych treści swoich książek. Specjalizuje się bowiem w problematyce działań zakulisowych, w tym w opisywaniu działalności grupy Bilderberg[2], co, niestety, owocuje coraz większą fascynacją autora teoriami spiskowymi. Samo pisarstwo Estulina stało się już przedmiotem dociekań naukowych na gruncie rodzimego medioznawstwa[3].

---

[1] D. Estulin, *W imię Allaha. Jak Zachód stworzył, sponsorował i rozpętał piekło islamskiego terroru*, tłum. z jęz. ang. M. Potulny, Katowice 2016, Sonia Draga, 333 s.

[2] D. Estulin, *Prawdziwa historia Klubu Bilderberg*, Katowice 2015 oraz tegoż: *Władcy cienia*, Katowice 2012.

[3] Zob. D.U. Popielec, *Charakterystyka dziennikarstwa śledczego Daniela Estulina*, „Naukowy Przegląd

Trzeba zauważyć, że polska opinia publiczna jest kształtowana w kwestiach bliskowschodnich jednostronnie, i to w sposób bardzo uproszczony. Wobec braku wiedzy historycznej, geograficznej, religioznawczej i politologicznej (problematyka orientalistyczna właściwie nie jest poruszana w programach edukacyjnych w naszym kraju) daje to stereotypowe postrzeganie tego regionu świata i jego problemów. Każda informacja, która będzie odmienna od dominującego przekazu mainstreamowych mediów oraz znacznej części literatury spod znaku pop-nauki, wzbudzi zdziwienie graniczące u większości czytelników wręcz z dysonansem poznawczym. Nie wydaje się, aby możliwa była polska edycja książki Noama Chomsky'ego – skrajnie krytycznej wobec „wojny z terroryzmem"[4]. Nakłada się embargo na informacje o dwuznacznej roli Arabii Saudyjskiej, Kataru i Kuwejtu wobec zbrojnego dżihadyzmu[5]. W Polsce są publikowane tylko pojedyncze prace na ten temat[6], chociaż tajemnicą poliszynela jest to, że dla rozwoju globalnego dżihadyzmu sunnickiego ogromne znaczenie miała polityka Królestwa Arabii Saudyjskiej, którego państwową religią i zarazem ideologią jest wahabityzm, inspirujący ruchy fundamentalistyczne.

Lekcja afgańska dowiodła, jak wielkie zagrożenie tkwi w ruchach zbrojnych wywołanych przez zachodni interwencjonizm i pozostawienie bez kontroli tysięcy mężczyzn, uzbrojonych i zdemoralizowanych wojną. Dziś jej powtórką, z groźnymi konsekwencjami dla Unii Europejskiej, jest lekcja syryjsko-iracko-libijska. Uświadamia ona prawdziwość geopolitycznej perspektywy postrzegania terroryzmu jako przemocy będącej odbiciem tej, którą wcześniej wygenerowały centra cywilizacyjne wobec peryferii[7]. Jednocześnie USA wzywają sojuszników z NATO do powtórnego zaangażowania się w Afganistanie. Narastają bowiem obawy o to, że Hamid Karzaj podzieli los Mohammada Nadżibullaha. Efekty dotychczasowej polityki i działań zbrojnych Zachodu nie są tak spektakularne, jak przedstawiają to przywódcy państw koalicji antyterrorystycznej, generalicja i mass media. A przecież na świecie – w tym głównie w USA – ukazało się wiele publikacji prezentujących bardziej zróżnicowany obraz genezy ruchów zbrojnych i organizacji terrorystycznych, a także meandrów amerykańskiej polityki zagranicznej wobec Bliskiego Wschodu i jej rezultatów[8].

Wydawnictwo Sonia Draga już wcześniej udostępniło polskiemu czytelnikowi prowokacyjną książkę Morgana Spurlocka[9], a tym razem wypuściło na rynek pozycję wyraźnie kontrastującą z rosnącym zalewem książek poświęconych Państwu Islamskiemu. Recenzowana publikacja jest złożona z prologu oraz czterech rozdziałów poświęconych kolejno: historii islamskiego fundamentalizmu; polityce mocarstw zachodnich wobec Bliskiego Wschodu; zawiłościom współczesnej polityki bliskowschodniej i roli, jaką odgrywa w regionie monarchia saudyjska; działaniom ISIS oraz innych organizacji terrorystycznych; zamachom terrorystycznym w Brukseli i Paryżu oraz ich daleko idącym

Dziennikarski/Journalism Research Review Quarterly" 2014, nr 3, s. 33–40.

[4] N. Chomsky, *Hegemony or Survival: America's Quest for Global Dominance*, New York 2003.

[5] L. Murawiec, *Princes of Darkness: the Saudi Assault on the West*, Lanham 2005 oraz tegoż: *The Mind of Jihad*, Cambridge 2008.

[6] S. Marchand, *Arabia Saudyjska – zagrożenie*, Warszawa 2004.

[7] Por. C. Flint, *Wstęp do Geopolityki*, Wydawnictwo Naukowe PWN, Warszawa 2008.

[8] Zob. np. R. Dreyfuss, *Devil's Game: How the United States Helped Unleash Fundamentalist Islam,* New York 2005, W. Madsen, J.Ch. Brisard, G. Dasquie, *Forbidden Truth: U.S.-Taliban Secret Oil Diplomacy, Saudi Arabia and the Failed Search for bin Laden*, New York 2002, jak również W. Madsen, *ISIS IS US: The Shocking Truth Behind the Army of Terror*, San Diego Ca 2016 oraz tegoż: *Unmasking ISIS: The Shocking Truth*, San Diego Ca 2016.

[9] M. Spurlock, *Gdzie u diabła jest Osama bin Laden?*, Katowice 2008.

konsekwencjom w polityce współczesnych państw. D. Estulin opisuje, jak zachodnia cywilizacja ze Stanami Zjednoczonymi, NATO oraz ich sojusznikami, takimi jak Izrael, Arabia Saudyjska i Katar na czele, doprowadziła do wykreowania islamskiego terroryzmu. Wskazuje beneficjentów tego konfliktu oraz główny cel obecnej polityki – zmianę porządku na Bliskim Wschodzie. Tę politykę nazywa *jawną próbą „bałkanizacji" krajów islamskich* (s. 12 oraz 82–90). Zdaniem D. Estulina procesy, których jesteśmy obecnie świadkami, to nie tyle wojna religijna, ile pierwsze symptomy wielkich geopolitycznych zmian o długotrwałych konsekwencjach. Już na pierwszych stronach prologu (10 stron) autor nakreśla zasadnicze tezy konstruujące jego perspektywę postrzegania współczesnej sytuacji globalnej. Pisze, że wojna z terroryzmem jest mitem służącym legitymizacji prowadzenia polityki ekspansji i głównym uzasadnieniem amerykańskiej doktryny wojskowej (s. 9), gdyż (…) *w drugiej połowie lat 70. XX wieku nastąpił w polityce międzynarodowej zainicjowany przez Stany Zjednoczone zwrot: wsparto finansowo i zbrojnie fanatycznych dżihadystów z całego Bliskiego Wschodu, którzy mieli prowadzić świętą wojnę z niewiernymi „komunistami" w Afganistanie* (s. 7).

Rozdział pierwszy – *Szatańska rozgrywka* (80 stron) – autor rozpoczyna od rozważań na temat islamskich sekt oraz ich wykorzystywania w imperialnych interesach przez brytyjski wywiad w Egipcie, a także od związanej z tym genezy Braci Muzułmanów (s. 27). Jednak religioznawczy aspekt jego wywodów jest dość niejasny, zwłaszcza w odniesieniu do sufizmu. Na kartach książki pojawiają się postacie Lawrence'a z Arabii i Gertrudy Bell oraz Arnolda Toynbee'ego, którym D. Estulin przypisuje ogromną moc sprawczą w kształtowaniu historii Arabów. Kolejną kwestią omawianą w tej części książki jest szok naftowy z 1973 r., na którego temat autor ma poglądy oryginalne. Twierdzi, że ów kryzys został sztucznie wywołany przez światową oligarchię finansową i doprowadził do wielkiej transformacji globalnej gospodarki (s. 29–39). W dalszym ciągu rozdziału snuje rozważania na temat roli służb wywiadowczych Wielkiej Brytanii i USA w wywieraniu wpływu na przebieg rewolucji irańskiej. D. Estulin cytuje w tej części książki poglądy Bernarda Lewisa i jego ocenę anglosaskiego uderzenia na Irak oraz wywołania wojny domowej w Syrii jako *upadek pan-Arabii*, czyli fiasko projektów nacjonalistycznych. Słuszna jest teza, że narastanie islamskiego radykalizmu można tłumaczyć nie tylko frustracją społeczną wywołaną ubóstwem i korupcją rządów, lecz także efektem próżni ideologicznej. Miejsce nieudanych eksperymentów doktrynalnych, takich jak arabski nacjonalizm (Egipt, Syria, Irak) czy arabski socjalizm (Egipt, Libia) zajął islamski fundamentalizm. Swoją drogą mesjanizm dżihadystów wykazuje podobieństwo do mesjanizmu robotniczego – obraz Zachodu jest wręcz tożsamy ze stereotypem kapitalizmu przedstawianym w marksistowskich pismach propagandowych.

W dalszym ciągu autor wskazuje zasadniczy cel Zachodu, jakim jest doprowadzenie do upadku państw nacjonalistycznych, co (…) *oddala groźbę rozwoju przemysłowego Bliskiego Wschodu i niepodległości państw w tym regionie* (s. 91). Jednocześnie podkreśla, że konflikty zbrojne wybuchały w krajach, które wcześniej były klientami ZSRR. D. Estulin nazywa Libię, Syrię (*krojenie Syrii na plasterki* – s. 90) oraz Irak socjalistycznymi – co jednak jest dyskusyjne. Słusznie wskazuje, że uderzenie na Irak leżało głównie w interesie państw, które od kilkudziesięciu lat są najważniejszymi klientami USA w regionie i które czuły się zagrożone irackim potencjałem wojskowym, tj. Arabii Saudyjskiej i Izraela.

Rozdział drugi, zatytułowany *Saudyjczycy* (112 stron), to prawdziwa *crème de la crème* dla czytelnika pasjonującego się tematyką bliskowschodnią. Autor konsekwentnie

stara się tu dowieść, że źródłem sunnickiego terroryzmu jest polityka Arabii Saudyjskiej. To państwo bowiem od półwiecza pełni najważniejszą rolę w szerzeniu ekstremizmu na Bliskim Wschodzie, finansując za pośrednictwem swoich banków wahabickie meczety i medresy na całym świecie, a za pośrednictwem organizacji charytatywnych – także radykalne ruchy zbrojne (s. 116). Wahabityzm (autor pisze wahabizm) jako najbardziej rygorystyczna odmiana purytanizmu jest w islamie trafnie określany za C. Winsorem mianem „teofaszymu". Zdaniem autora władze Stanów Zjednoczonych zdają sobie sprawę z roli Arabii Saudyjskiej we wspieraniu międzynarodowego terroryzmu, ale w imię wyższych racji politycznych zachowują milczenie (s. 118). Ogromne znaczenie ma również niejawna współpraca Rijadu z Londynem, a podkreślanie wagi zakulisowych działań perfidnego Albionu jest jedną z podstawowych obsesji autora (s. 155–201).

Wojna radziecko-afgańska zmobilizowała tysiące młodych, fanatycznych muzułmanów do walki za wiarę. Fundamentalistyczne, sunnnickie ugrupowania pasztuńskich mudżahedinów uzyskały pomoc finansową ze strony Arabii Saudyjskiej za pośrednictwem pakistańskich służb specjalnych przy wsparciu CIA. Celem Rijadu było szerzenie wahabityzmu i powstrzymywanie wpływów szyickiego Iranu oraz ekspansji Sowietów. Antysowiecki „dżihad" stał się impulsem do wstępowania w szeregi bojowników w imię Allaha. Po zdobyciu Kabulu w 1992 r. weterani (*Afghan Arabs*) walk przeciwko Armii Radzieckiej stali się zbrojną awangardą nowej rewolucji. Z kolei założenie ruchu talibów miało na celu stworzenie wahabickiego przyczółku blisko granic Rosji (s. 104). Dużą część rozdziału poświęcono przestępczości narkotykowej powiązanej z organizacjami terrorystycznymi, której działalność jest związana z rosnącą produkcją opium w Afganistanie.

W rozdziale trzecim – *ISIS i inni* (94 strony) – D. Estulin zawarł opis współczesnego dżihadu, a więc aktualnych wydarzeń na Bliskim Wschodzie oraz na Kaukazie. To rozdział dość rzetelnie napisany, jeśli chodzi o faktografię. Autor wzmiankuje tu o znaczeniu kolorowych rewolucji (s. 215–216) oraz o tzw. arabskiej wiośnie. W odniesieniu do grup zbrojnych w Iraku i Syrii D. Estulin uważa pojęcie umiarkowani rebelianci wręcz za oksymoron i pisze, że są to po prostu (…) *salafickie bojówki, najemnicy, zabójcy do wynajęcia* (s. 230). W końcowej części rozdziału omawia politykę Arabii Saudyjskiej, Izraela, Turcji i innych państw wobec kampanii toczonych przez ISIS, rysując ponury obraz niebywałego zagmatwania i konfliktu rozmaitych interesów. Stawia pytania o to, dlaczego cywilizowany świat nie jest w stanie powstrzymać ruchu zbrojnego, który pojawił się rzekomo znikąd, (…) *od razu jako armia uzbrojonych* (...) *dobrze zorganizowanych i profesjonalnie wyszkolonych żołnierzy, poruszających się konwojami identycznych, fabrycznie nowych toyot* (s. 262).

Rozdział czwarty – *Paryż – Paryż – Bruksela* (19 stron) – skromny objętościowo i zamykający książkę, zawiera zwięzły opis zamachów w Paryżu i Brukseli oraz refleksję nad możliwymi scenariuszami rozwoju sytuacji w Europie. Autor przytacza tu wiele opinii krytycznych wobec francuskich i belgijskich służb specjalnych oraz podważających oficjalną wersję wydarzeń. Stawia pytanie, dlaczego zachodnie służby wypuszczały na wolność zatrzymywanych wcześniej terrorystów. Przytacza tezę Stevena MacMillana, że zachodnim elitom (…) *nie chodzi o zwycięstwo w „wojnie z terrorem", bo „wojna z terrorem" została wymyślona jako trwały stan*, widząc w niej potwierdzenie poglądów George'a Orwella z *Roku 1984*[10], że (…) *liczy się sam fakt ciągłego stanu zagro-*

[10] G. Orwell, *Rok 1984*, Warszawa 2013.

żenia (s. 304), co jest siłą napędową rozwoju nowych technologii służących inwigilacji oraz wprowadzaniu w Europie metod państwa policyjnego. Tym samym globalną wojnę z terroryzmem można interpretować jako projekt globalnej paniki moralnej. To zjawisko, opisane przez psychologów społecznych i socjologów, istnieje dzięki ludzkim emocjom związanym z lękiem i niepewnością. Przeważnie jest ono inicjowane i sterowane przez przedstawicieli władzy lub grupy interesu, których partykularnym celem jest doprowadzenie do zmiany społecznej, często związanej ze zmianą regulacji prawnych[11].

Źródła wykorzystane przez autora książki *W imię Allaha…* zostały wykazane w 740 przypisach. Aż w 132 przypadkach D. Estulin przywołuje wyłącznie artykuły zamieszczane w czasopismie „EIR" („Executive Intelligence Review") wydawanym przez ruch Lyndona LaRouche'a. W publikacji jest dużo odniesień do poważnych źródeł prasowych, takich jak „The Guardian", „Der Spiegel", „Newsweek", „The Times", „The Economist", „The Washington Post", „Los Angeles Times", „Le Monde", „The New York Times", a także do stacji telewizyjnych: CNN, BBC i al Dżazira. Sporadycznie tylko autor sięga do czasopism naukowych, takich jak „Foreign Policy Magazine", „Foreign Affairs", „New Middle East" czy „Armed Forces Journal". Zaledwie pięć razy odwołuje się do źródeł rosyjskich (w tym do „Sputnika" – tylko raz). Najczęściej cytowani przez D. Estulina autorzy to: Peter Goodgame (protestancki publicysta głoszący idee antykapitalistyczne i apokaliptyczne, autor książki *The Globalists & the Islamists: Fomenting the „Clash of Civilizations"*), Robert Baer (były oficer CIA i znawca problematyki bliskowschodniej, autor kilku książek na temat terroryzmu, w tym *Sleeping with the Devil*, na której kanwie powstał scenariusz filmu „Syriana" w reż. Stephena Gaghana), Robert Dreyfuss (dziennikarz śledczy, redaktor najstarszego amerykańskiego tygodnika „The Nation" popierającego w ostatnich wyborach prezydenckich kandydaturę Berniego Sandersa), Barry Rubin (izraelski naukowiec specjalizujący się w problematyce dotyczącej bezpieczeństwa Bliskiego Wschodu) i Thierry Lalevée (francuski publicysta, znawca Bliskiego Wschodu, zaangażowany w ruch Lyndona LaRouche'a). Skromnie natomiast przedstawia się liczba źródeł poważniejszych – zaledwie kilkanaście monografii (w tym bardzo nieliczne na temat Bliskiego Wschodu) wykorzystanych podczas pisania pracy nie robi dobrego wrażenia.

Książka zawiera szesnastostronicową wkładkę z ilustracjami (fotografie, dokumenty, mapy) oraz – jako załącznik – jedenastostronicowy wykaz organizacji terrorystycznych oparty na skrócie opracowania z Uniwersytetu Stanforda. Tego rodzaju aneks nie ma jednak większej wartości, zważywszy na publikacje, które ukazały się ostatnio w Polsce, w tym przede wszystkim *Leksykon organizacji i ruchów islamistycznych* opracowany przez Krzysztofa Izaka[12].

O atrakcyjności omawianej lektury stanowią znajomość historii politycznej Bliskiego Wschodu, żywa narracja oraz dobry warsztat pisarski (duża w tym zasługa tłumacza). Jednak po jej zgłębieniu należy postawić pytanie o rzeczywiste motywy jej powstania. Można sformułować cztery hipotezy w odniesieniu do osoby samego autora i znaczenia jego twórczości. Po pierwsze można uznać, że Daniel Estulin jest *whist-*

[11] Zob. I. Sakson-Szafrańska, *Dewiacja czy norma – rola paniki moralnej i syndromu Nagasaki w postrzeganiu prawa do użycia i sankcjonowania przemocy zbiorowej,* „Normy, dewiacje i kontrola społeczna" 2014, nr 15, s. 144–176.

[12] Por. K. Izak, *Leksykon organizacji i ruchów islamistycznych*, wyd. I – Emów 2014, Agencja Bezpieczeństwa Wewnętrznego, Centralny Ośrodek Szkolenia; wyd. II – Warszawa 2016, Wydawnictwo Akademickie Dialog, a także: *Atlas radykalnego islamu*, Warszawa 2011, oraz wcześniejsze: *Leksykon współczesnych organizacji terrorystycznych*, P. Ebig i in. (red.), Poznań 2007.

blowerem, niezależnym dziennikarzem śledczym, który w sposób bezkompromisowy tropi niegodziwości w polityce mocarstw. Zatem jego motywacja jest natury poznawczej i etycznej. Po drugie można przyjąć, że autor jest przede wszystkim celebrytą, który opanował sztukę pisania książek prowokujących swymi sensacyjnymi tezami, co przynosi piszącemu oraz jego wydawcom znaczne dochody, a więc jego motywacja jest natury finansowej. Po trzecie można uznać, że D. Estulin cierpi na przymus pisania prowokacyjnych tekstów i jako sympatyk ruchu Lyndona LaRouche'a jest owładnięty obsesją światowych spisków, a to oznaczałoby, że jego motywacja ma charakter wewnętrzny i psychiczny. Po czwarte wreszcie można postawić hipotezę, że autor nie jest bynajmniej niezależny i że jego twórczość ma swoje źródła w inspiracji ukrytych mocodawców. Zatem jego motywacja miałaby charakter zewnętrzny, a teksty jego kontrowersyjnych książek miałyby wywierać wpływ na światową opinię publiczną. Pisarstwo D. Estulina byłoby więc przejawem globalnej walki informacyjnej między państwami, a sam autor – agentem dezinformacji.

Choć w ostatnich latach pojawiło się w Polsce dość dużo opracowań na temat walki informacyjnej, to mają one różną wartość. A przecież wystarczy zdrowy rozsądek oraz znajomość prac z zakresu kulturoznawstwa i medioznawstwa, aby zrozumieć istotę problemu. Odbiorcy wiadomości pozostają w polu oddziaływania wielu dyskursów, z których część nawzajem się uzupełnia i wzmacnia, część zaś stoi w sprzeczności i blokuje oddziaływanie innych dyskursów[13]. Obecny kierunek polityki zagranicznej i bezpieczeństwa państwa jest uzasadniany propagandowym przekazem medialnym, w którym władza dąży do ujednolicenia treści tego przekazu (panowanie informacyjne). Każda wiadomość, która znacząco odbiega od mainstreamu, zaczyna więc być traktowana jako przejaw „walki informacyjnej", „informacyjnych ataków przeciwnika", „trollowania" itd., nawet jeśli jest prawdziwa. To jest prosta droga do makkartyzmu. Tymczasem szerzenie podejrzliwości i politycznej paranoi jest poważnym zagrożniem dla demokracji i społeczeństwa, a w konsekwencji – dla państwa[14]. W walce informacyjnej nie powinno chodzić o to, by w krajowych mediach był rozpowszechniany tylko jeden rodzaj opinii, jeden pogląd i aby była prezentowana tylko jedna kanoniczna wersja politycznej prawdy, chroniona przez cenzurę[15], jak to było w państwach totalitarnych i nadal jest w autorytarnych dyktaturach. Metaforycznie rzecz ujmując, walka informacyjna to nie zmasowane naloty dywanowe z użyciem jednego rodzaju bomb w maksymalnych ilościach, a, niestety, przez wielu rodzimych specjalistów (szczególnie o proweniencji wojskowej) tak właśnie jest rozumiana. Doświadczenia historyczne pokazują, do jakich rezultatów doprowadza długofalowo polityka propagandowa „jedności ideowo-politycznej narodu". Im bardziej jest ujednolicony przekaz informacji sterowany przez władze, tym wywieranie wpływu przez nie może summa summarum okazać się słabsze i dysfunkcyjne dla siły państwa. W sytuacji zamętu, kryzysu czy konfliktu bowiem silniejsze staje się oddziaływanie dyskursów alternatywnych. Stąd tak znacząca siła oddziaływania teorii spiskowych i sukcesy rynkowe książek takich autorów, jak Daniel Estulin.

[13] Por. J. Storey, *Studia kulturowe i badanie kultury popularnej*, Kraków 2003, s. 23.

[14] Jak dotąd, w Polsce ukazały się, tylko dwie dobre prace na ten temat, zob. D. Pipes, *Potęga spisku – wpływ paranoicznego myślenia na dzieje ludzkości*, Warszawa 1998 oraz R.S. Robins, J.M. Post, *Paranoja polityczna – psychologia nienawiści*, Warszawa 1997.

[15] Np. według N. Chomsky'ego cenzura jest warunkiem skuteczności perswazji medialnej, por. tegoż: *Media Control* [online], http://library.uniteddiversity.coop/Media_and_Free_Culture/Media_Control-The_Spectacular_Achievements_of_Propaganda-Noam_Chomsky.pdf. [dostęp: 22 II 2016].

M. Świerczek

S. Wojciechowski, *Triest. Wospominanija*[1] czyli wspomnienia „pożytecznego idioty"

„Pożytecznymi idiotami"[2] W. Lenin nazywał podobno zachodnich dziennikarzy, którzy bezkrytycznie głosili pochwałę sowieckiej rewolucji i tym samym przyczyniali się jego zdaniem do samozagłady burżuazji gotowej „sprzedać komunistom sznur, na którym ci ich potem powieszą"[3]. Ta kategoria osób została później rozszerzona w antykomunistycznej publicystyce na wszystkich tych, którzy powtarzali tezy radzieckiej propagandy, nie dostrzegając ukrytych za nimi faktów. W znaczeniu zawężonym, w odniesieniu do teorii dezinformacji, używa się tego wyrażenia do określenia osób niezwiązanych z wywiadem prowadzącym akcję inspiracyjną, lecz z powodu swojej niewiedzy lub emocjonalnego zadurzenia uwiarygodniających tego typu działania.

Rzadko się zdarza, aby „pożyteczny idiota" opisywał swój w udział w operacji już po jej ujawnieniu. Zwykle bowiem ludzie wstydzą się tego, że z powodu braku zdrowego rozsądku padli ofiarą oszustów lub intrygantów. Dlatego też książka Siergieja Wojciechowskiego ma ogromną wartość – autor napisał ją ponad 45 lat po ostatecznej dekonspiracji sowieckiej intrygi, zwanej w literaturze „aferą Trust". Potrzebował niemal pół wieku, żeby znaleźć w sobie odwagę do publicznej analizy swoich przekonań i złudzeń, które pozwoliły bolszewikom zmienić go w bezwolne narzędzie. Co ciekawe, w latach 1923–1927 S. Wojciechowski odgrywał podwójną rolę: uwiarygadniał sowiecką dezinformację i jednocześnie był bolszewickim szpiegiem, choć podobno nie zdawał sobie sprawy z tego, że jego raporty docierają na Łubiankę[4]. Mimo że nienawidził bolszewików, to pracował dla nich i realizował zadania, które zlecali mu bezpośrednio Feliks Dzierżyński, a potem Wiaczesław Mienżyński, i do końca zachowywał wiarę, że działa na rzecz samodzierżawnej Rosji[5].

Wojciechowski przyjechał do Polski po ewakuacji „białych" wojsk z Krymu. Miał tu znajomych jeszcze z czasów przedwojennych, w Gdańsku posiadał mieszkanie, które wynajmował. Szybko stał się korespondentem emigracyjnej agencji prasowej RUSPRESS. Był zdolnym dziennikarzem, zaangażowanym w działalność „białej" emigracji, a przy tym nieprzejednanym wrogiem *bolszewii* przekonanym o konieczności aktywnej walki z Rosją Sowiecką w celu odbudowy dawnego imperium. Co ciekawe, Polska w jego czarnosecinnym światopoglądzie mieściła się jedynie jako – być może autonomiczny – Kraj Przywiślański, ściśle powiązany z rosyjskim domem panującym[6]. Wraz

[1] S. Wojciechowski, *Triest. Wospominanija*, Kanada 1974, bmw.

[2] Ros. *полезный идиот*.

[3] *Kapitaliści sprzedadzą nam sznurek, na którym ich powiesimy*, cyt. za: T. Gospodarek, *Aspekty złożoności i filozofii nauki w zarządzaniu*, Wałbrzych 2012, s. 175.

[4] Wojciechowski przyznał się do napisania 85 raportów, nazywanych przez niego *obzorami*, por. W. Michniewicz, *Wielki bluff sowiecki*, Chicago 1991, s. 260.

[5] O szczerości przekonań kultywowanych w rodzinie Wojciechowskich może świadczyć to, że brat Siergieja – Jurij – w maju 1928 r. dokonał w Warszawie zamachu na przedstawiciela handlowego Rosji Sowieckiej, Lizariewa.

[6] Por. W. Michniewicz, *Wielki bluff*…, poszczególne fragmenty charakterystyki Wojciechowskiego w różnych miejscach.

z innymi monarchistami współpracującymi z polskim wywiadem starał się wmawiać Polakom, że odbudowana po spodziewanym przewrocie carska Rosja zaakceptuje ustalenia traktatu ryskiego, choć było wiadomo, że monarchiści stali na stanowisku *jedinoj i niedielimoj Rossiji.* O jego stosunku do państwa polskiego i Polaków świadczy też praca w czasie niemieckiej okupacji w *Russkom Komitetie* w Warszawie, który ściśle współpracował z władzami okupacyjnymi i odgrywał rolę pośrednika między kolaboracyjnie nastawionymi Polakami a Niemcami (np. wystawiał Polkom chcącym legalnie wyjść za mąż za żołnierzy armii okupacyjnej świadectwa potwierdzające ich rosyjską narodowość). Z uznaniem wyraża się o niemieckich urzędnikach, którzy *nie utracili niemieckiego honoru*.

Warto zauważyć, że S. Wojciechowski, pisząc o akcjach polskiego podziemia, konsekwentnie nazywa żołnierzy ruchu oporu „terrorystami". Z nienawiścią opisuje antyrosyjską działalność F.S. Składkowskiego, W. Dziadosza – wojewody kieleckiego, a nawet ruchu prometejskiego, który w jego mniemaniu nie był antysowiecki, ale antyrosyjski i zmierzał do podcięcia podstaw rosyjskiego imperium. Innymi słowy, S. Wojciechowski był typowym przedstawicielem rosyjskiej emigracji monarchistycznej, łączącej wiarę w mocarstwowo-słowianofilską rolę Rosji z nienawiścią do bolszewików, którzy zniszczyli imperium Romanowów, doprowadzili do stworzenia na jego gruzach państw „limitrofowych" i upokorzenia Rosji przegraną wojną z *Polszą*, którą traktowali jak zbuntowanego wasala[7]. W tym samym stopniu, co W. Szulgin[8] i reszta działaczy emigracyjnych, był przekonany o *śmierci Rosji* zniszczonej przez żydowskich rewolucjonistów[9] i marzył o powrocie do ojczyzny w jej przedwojennych granicach, z batiuszką carem na kremlowskim tronie. Jedyne, co różniło go od aktywistów emigracyjnej Najwyższej Rady Monarchicznej (Wysszego Monarchiczeskogo Sowieta), było przekonanie, że przewrót w Rosji dokona się za pomocą sił wewnętrznych i że części rewolucyjnych zmian cofnąć się nie da. To niewielkie odstępstwo wystarczyło, aby bolszewiccy manipulanci odkryli w nim potencjalną ofiarę.

Po przyjeździe do Polski Wojciechowski obracał się w kręgach „białej" emigracji oraz wśród Polaków – rusofilów kultywujących swoje przywiązanie do idei wielonarodowej monarchii rosyjskiej, takich jak Antoni Korniecki, który (tuż po wojnie 1920 r. skutkującej powszechną rusofobią) miał na ścianach swego adwokackiego gabinetu fotografie carskich oficerów i był znanym przyjacielem rosyjskich emigrantów[10]. Przez niego poznał Dmitrija Andrę, związanego z *tajną organizacją monarchistyczną Trust*, której utworzenie posłużyło de facto do przeprowadzenia sowieckiej prowokacji. Andro z kolei poznał go z agentem GPU Jurijem Artamonowem – łącznikiem Trustu z polskim wywiadem.

Pozyskanie S. Wojciechowskiego przez Artamonowa do pracy w Truście (czyli w istocie jego werbunek do pracy na rzecz GPU) jest majstersztykiem pracy operacyjnej. Artamonow podzielał przekonania Wojciechowskiego dotyczące roli sił wewnętrznych w obaleniu Sowietów. Powiedział, że taka wewnętrzna, antysowiecka

[7] Warto przypomnieć, że w wojnie 1920 r. po stronie bolszewickiej ochotniczo uczestniczyło kilkadziesiąt tysięcy oficerów byłej armii carskiej.

[8] W czasie rewolucji lutowej 1917 r. współtwórca Rządu Tymczasowego. Od 1921 r. na emigracji. W latach 1925–1926, na zaproszenie Trustu, odbył podróż po ZSRS. Jej wynikiem była powieść o chrakterze reportażowym pod tytułem *Tri stolicy.* To zostało wykorzystane przez OGPU do uwiarygodnienia prowadzonej akcji dezinformacyjnej. W 1944 r. aresztowany w Jugosławii i do 1956 r. więziony w ZSRR.

[9] Por. W. Szulgin, *Tri stolicy*, Moskwa 1991.

[10] S. Wojciechowski, *Triest*…, s. 17.

walka trwa już od 1918 r., a on sam jest przedstawicielem grupy, która jest w nią zaangażowana. Jako na twórcę tej konspiracji wskazał na powszechnie szanowanego w carskiej Rosji generała Zajonczkowskiego[11]. Żeby ostatecznie przekonać swego rozmówcę o znaczeniu tej grupy spiskowców, pokazał mu zaświadczenie wystawione podobno przez Oddział II polskiego Sztabu Generalnego, które potwierdzało, że Artamonow działa w RP za wiedzą i zgodą polskiego wywiadu. Rosjanin postępował niezwykle precyzyjnie i delikatnie. Wiedział, że ma do czynienia z przedstawicielem klasy społecznej, dla której honor i służba carowi były wartościami nadrzędnymi. Dlatego nie żądał od S. Wojciechowskiego przysiąg, nie werbował go, a jedynie poprosił o pomoc w zrozumieniu polskich realiów, aby móc jak najlepiej wypełnić swój *graždanskij dołg*[12], pracując dla Trustu. To odwoływanie się do systemu wartości pomogło w zbudowaniu całkowitego zaufania między Artamonowem i Wojciechowskim, który szybko stał się jego najbliższym współpracownikiem. Wiara Wojciechowskiego w przyjaciela była tak wielka, że jeszcze w 1974 r. podkreślał, iż Artamonow padł – jak on sam – ofiarą sowieckich szpiegów, nie będąc z nimi w żaden sposób powiązanym. Stało się tak dlatego, że podobnie jak wszyscy przedstawiciele carskiej inteligencji wierzył w nienaruszalność słowa danego przez rosyjskiego oficera. Na tym zaufaniu żerował także F. Dzierżyński, kiedy powierzył funkcję kierowania operacją „Trust" byłym generałom armii carskiej: N. Potapowowi[13] i A. Zajonczkowskiemu, których osobiście znał jako działaczy rosyjskiej emigracji na Zachodzie, oraz generałom P. Wranglowi i A. Kutiepowowi. W dodatku gen. Potapow cieszył się opinią nieprzejednanego wroga urzędniczej korupcji i w przeszłości narażał własną karierę przez wyrażanie sprzeciwu wobec rozkradania carskich funduszy przez spokrewnionego z rodziną carską władcę Czarnogóry, w której Potapow przed wojną był attaché wojskowym[14]. W ten sposób, jak pisał Wojciechowski, bolszewicy – pozbawieni honoru i poczucia własnej godności – wykorzystali właśnie te cechy „umarłej klasy", które nie pozwalały jej przedstawicielom na przyjęcie do wiadomości tego, że są tylko ofiarami podstępnej intrygi. Zdaniem Wojciechowskiego postawienie na czele prowokacyjnej organizacji dwóch szanowanych generałów oraz byłego wysokiego rangą urzędnika carskiego o nieposzlakowanej opinii – zagorzałego monarchisty A. Jakuszewa[15] – zablokowało zdolność logicznego myślenia.

S. Wojciechowski z goryczą konstatuje, że jego ówczesny system wartości wykluczał to, że carski oficer może kłamać i szargać swój honor. Wyciąga także niepokojąco aktualny wniosek, że rosyjska emigracja wychowana w kulcie posłuszeństwa wobec autorytetów nie była w stanie dać wyrazu wątpliwościom, kiedy jej przywódcy i moralni przewodnicy wystawiali bolszewickim prowokatorom świadectwa moralności i najwyższego uznania.

[11] Andriej M. Zajonczkowski – dowodził 30 rosyjsko-rumuńską armią broniącą Dobrudży w 1916 r.; po wybuchu rewolucji lutowej przeszedł na emeryturę. W 1918 r. przyłączył się jednak do Armii Czerwonej i zajmował kierownicze stanowiska w Sztabie Generalnym. Po wojnie z Polską podjął pracę jako wykładowca wojskowy. Napisał m.in. dwutomową historię I wojny światowej. Pracował dla CzKa i GPU. Zmarł w 1926 r.

[12] Obowiązek obywatelski – przyp. red.

[13] Nikołaj M. Potapow – od 1901 r. służył w rosyjskim wywiadzie wojskowym, najpierw jako pomocnik attaché wojskowego w Wiedniu, a następnie jako attaché wojskowy w Czarnogórze. W 1916 r. wrócił do Rosji. Po rewolucji październikowej został mianowany szefem Sztabu Generalnego. Od 1918 r. służył w Komisariacie Wojny. Zmarł w 1946 r.

[14] Por. L. Nikulin, *Miortwaja zyb'*...

[15] Najważniejsza postać sowieckiej prowokacji – były wysoki urzędnik carski, który na początku lat 20. XX w. podjął współpracę z CzKa i GPU oraz nawiązał kontakt z rosyjską emigracją i sztabami europejskimi jako emisariusz Trustu. Dokładne okoliczności jego śmierci, jak też motywy współpracy z GPU, są nieznane.

Wojciechowski pisze o tym z zadziwieniem, jakby wciąż nie mógł uwierzyć we własną naiwność. Najbardziej boli go to, że widział symptomy oszustwa. Zachowanie agentów Łubianki nie było wcale szczytem profesjonalizmu – Jakuszew i Potapow odbywali długie podróże po Europie jako rzekomi urzędnicy na bolszewickiej służbie. Zapytani, dlaczego nikogo w Rosji nie interesuje, co się z nimi przez ten czas dzieje, zbywali rozmówców stwierdzeniem, że Trust jest potężny i daje im długie delegacje lub urlopy w syberyjskich lasach na polowania.

Obaj, będąc ponoć emisariuszami podziemnej organizacji, spotykali się z oficerami polskiego Oddziału II SG w modnych warszawskich lokalach (i to w mieście, w którym znajdowała się największa rezydentura sowieckiego wywiadu w Europie). Wojciechowski zadawał sobie pytania: Jak to możliwe, że emisariusze Trustu nie troszczą się o swoje bezpieczeństwo, nie konspirują i nie boją się OGPU, które u reszty społeczeństwa budziło paraliżujący strach?

Jakim cudem tak rzekomo dużej organizacji, jaką był Trust, udało się uniknąć wykrycia? Dlaczego przez cztery lata podziemnej działalności nie tylko niczego nie osiągnęła, lecz także niemal jawnie paraliżowała wszelką aktywność środowisk „białej" emigracji? Czy możliwe było pominięcie milczeniem tak oczywistych wpadek osób uważanych przez bolszewików za zbyt groźne , jak Reilly[16] i Sawinkow[17], aby pozwolić im na powrót z „konspiracyjnych" podróży po Rosji?

Wojciechowski dostrzegał wiele oznak czyjejś złej, podstępnej woli, ale nie dopuszczał do siebie wniosków. Sądził, że skoro Trustowi wierzą tak zasłużeni działacze emigracji, jak gen. Kutiepow[18], gen. Wrangel[19], Szulgin, wielki książę Mikołaj Mikołajewicz[20] i wreszcie oficerowie polskiego wywiadu, to jemu – szaremu działaczowi emigracyjnemu – nie wolno nie wierzyć. Nawet jeśli zachowania tych autorytetów były całkowicie bezmyślne.

Bolszewicy robili przy tym wszystko, aby ten „stan autorytarnego transu" umacniać u swoich ofiar. Jakuszew pisał listy do swoich europejskich współpracowników, dbając o zachowanie wszystkich form stosowanych w najlepszych latach monarchii[21]. Nosił monokl i ubierał się, jakby wciąż był pracownikiem carskiego ministerstwa w 1914 r. Potapow podczas wizyt w Warszawie chodził ze swoimi gospodarzami po Łazienkach,

[16] Właśc. Sigmund Grigorjewicz Rosenbaum. Po wyjeździe z Rosji, od 1895 r., podjął pracę dla brytyjskiego wywiadu. W 1918 r. był współorganizatorem tzw. spisku Lockharta zmierzającego do obalenia bolszewickiej władzy. W 1925 r. został zwabiony przez przedstawicieli Trustu do ZSRR, gdzie po aresztowaniu i przesłuchaniu został zamordowany.

[17] Boris Wiktorowicz Sawinkow, jako członek Organizacji Bojowej Socjalistów-Rewolucjonistów, organizował zamachy na carskich notabli. Po rewolucji październikowej stał się wrogiem bolszewików – m.in. współdziałał z J. Piłsudskim w tworzeniu Rosyjskiej Armii Ludowej, która walczyła w 1920 r. przeciwko Armii Czerwonej. W 1925 r. został zwabiony przez GPU do ZSRR, gdzie po aresztowaniu i skazaniu na więzienie zginął w niejasnych okolicznościach.

[18] Aleksander Pawłowicz Kutiepow – generał armii carskiej uczestniczący aktywnie w wojnie domowej przeciwko bolszewikom. Po ewakuacji „białych" armii stał się aktywnym działaczem emigracyjnym; z czasem został liderem Rosyjskiego Związku Ogólnowojskowego. W 1930 r. we Francji został porwany i zamordowany przez OGPU.

[19] Piotr Nikołajewicz Wrangel – jeden z najwybitniejszych przywódców „białego ruchu" walczącego z bolszewikami. Po ewakuacji „białych" armii osiadł we Francji, gdzie aż do śmierci stał na czele Rosyjskiego Związku Ogólnowojskowego. Zmarł w 1928 r., najprawdopodobniej otruty przez OGPU.

[20] Mikołaj Mikołajewicz Romanow – głównodowodzący armii rosyjskiej podczas I wojny światowej. Po rewolucji październikowej – na emigracji, gdzie był przewodniczącym Rosyjskiego Związku Ogólnowojskowego. Zmarł w 1929 r.

[21] Por. L. Nikulin, *Miortwaja zyb'*…

gdzie sentymentalnie przystawał pod wybranym drzewem, z którym, rzecz jasna, była związana jakaś rzewna historia bliska duszy rosyjskiego oficera; chodząc po alejkach, deklamował wiersze i obiecywał przewrót w Rosji za jedyne 25 milionów amerykańskiej pożyczki. Jednocześnie Trust przysyłał z Moskwy materiały do opublikowania w emigracyjnej prasie, poświęcone np. tkliwym wrażeniom wywołanym u rzekomego monarchisty podczas wizyty w Carskim Siole (Potapow podobno przeżywał najgłębsze wzruszenie strasznym losem batiuszki – ojca narodu).

Ta komedia odwołująca się do ukształtowanych nawyków reagowania na świat ofiar autorytarnego, carskiego wychowania wystarczyła, aby sparaliżować wszelki krytycyzm. Wojciechowski nie dzielił się swoimi wątpliwościami z nikim, aby nie wydać się małodusznym, pozbawionym patriotycznych uczuć czy też pesymistycznym malkontentem. Jak inni emigranci ukrywał swoją niewiarę i poczucie absurdu, wywołane bezmyślnością emigracyjnego kierownictwa lub brakiem profesjonalizmu polskiego wywiadu, z którym współpracował. Nakładał maskę przekonanego monarchisty, głęboko wierzącego w triumfalny powrót samodzierżawia na Kreml – może tylko nieco zmodyfikowanego przez bolszewicki totalitaryzm. I ta poza, która miała maskować własne wątpliwości, była zabójcza, gdyż inni zapewne też widzieli, że coś zgrzyta w tym mechanizmie entuzjastycznie przygotowywanego przewrotu. Tyle, że – jak Wojciechowski – chcieli wierzyć swoim przywódcom i uniknąć utraty twarzy „szczerych, rosyjskich patriotów".

W tym właśnie zawiera się największa wartość książki S. Wojciechowskiego. Autor mimowolnie nakreślił zjawisko występujące zapewne powszechnie, bez względu na szerokość geograficzną czy narodowość aktorów. Chęć wiary w cudze wskazówki oraz obawa przed tym, aby nie wydać się paranoikiem lub człowiekiem małodusznym potrafią nawet z najbystrzejszych obserwatorów zrobić ślepców.

Podobne procesy (choć na mniejszą skalę) zachodziły w szpiegowskich sprawach Kima Philby'ego i Aldricha Amesa. Ich koledzy nie chcieli widzieć faktów. Woleli udawać, że wszystko jest w porządku, nawet jeśli poszlaki były dla każdego oczywiste. W makroskali historii procesy zaprzeczania faktom są chyba jeszcze bardziej jaskrawe, czego najlepszą ilustracją jest słynne zdanie jednego z szefów sowieckiego wywiadu, który na pytanie, jak to możliwe, że dziesiątki meldunków szpiegowskich o przygotowywanej agresji hitlerowskiej na ZSRS są ignorowane – odpowiedział: (…) *towarzysz Stalin wie lepiej!*

Zapewne tak długo, jak długo ludzie nie będą podejmować wysiłku samodzielnego myślenia, zgodnego z dewizą Kanta: *sapere aude* [22], lecz będą zdawać się na autorytety, będzie się powtarzać opisane przez Wojciechowskiego zjawisko, tak chętnie wykorzystywane przez zawodowych manipulantów.

[22] Z łac.'miej odwagę być mądrym' – przyp. red.

IV
PRZEGLĄD
PRAC KONKURSOWYCH

Szósta edycja ogólnopolskiego konkursu Szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa

Edycja 2015/2016 – wyniki konkursu

Na konkurs dla absolwentów studiów I i II stopnia ogłoszony przez Szefa Agencji Bezpieczeństwa Wewnętrznego wpłynęło 40 prac obronionych w roku akademickim 2015/2016.

Komitet konkursowy, po dokonaniu oceny nadesłanych prac, zdecydował przyznać następujące nagrody:

miejsce I – p. Dorian Duda (Uniwersytet im. Adama Mickiewicza w Poznaniu, Wydział Prawa i Administracji), *Operacyjne metody zwalczania terroryzmu w świetle polskiego i niemieckiego procesu karnego*,

miejsce II – p. Jakub Sałek (Uniwersytet Jagielloński, Wydział Prawa i Administracji), *Nielegalność czynności operacyjno-rozpoznawczych a możliwość ich procesowego wykorzystania w postępowaniu dowodowym*,

miejsce III – p. Krystian Radziejewski (Uniwersytet Warszawski, Wydział Dziennikarstwa i Nauk Politycznych), *Cyberbezpieczeństwo w administracji rządowej w Rzeczypospolitej Polskiej*,

wyróżnienia:

- p. Kamil Gefert (Wojskowa Akademia Techniczna, Wydział Cybernetyki), *Terroryzm lotniczy. Istota i zwalczanie*,
- p. Emilian Kaufman (Katolicki Uniwersytet Lubelski JP II, Wydział Prawa, Prawa Kanonicznego i Administracji), *Ochrona praw człowieka przy realizacji uprawnień służb specjalnych*,
- p. Mateusz Rakowski (Akademia im. Jana Długosza w Częstochowie, Wydział Filologiczno-Historyczny), *„Nowe wojny" – wybrane aspekty konfliktów w cyberprzestrzeni.*

Ogólnopolski konkurs Szefa ABW na najlepszą pracę doktorską, magisterską lub licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa.
Edycja VII – 2016/2017
Ogłoszenie i warunki konkursu

Organizatorem konkursu jest Szef Agencji Bezpieczeństwa Wewnętrznego. Celem konkursu jest promocja i upowszechnianie problematyki bezpieczeństwa wewnętrznego państwa wśród studentów i kadry akademickiej, zwiększenie świadomości społecznej w tym zakresie oraz profilaktyka i edukacja na rzecz bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.

Tematy konkursu:

1. Rola i zadania służb specjalnych w demokratycznym państwie prawa i w państwach autorytarnych.
2. Konstytucyjne prawa obywateli a uprawnienia służb specjalnych.
3. Służby specjalne – historia, teraźniejszość.
4. Bezpieczeństwo Polski i Europy w XXI wieku – zagrożenia i wyzwania.

Nagrody w konkursie:

miejsce I – nagroda finansowa w wysokości 3000 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego",

miejsce II – nagroda finansowa w wysokości 2500 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego",

miejsce III – nagroda finansowa w wysokości 2000 zł oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego",

wyróżnienie – nagroda rzeczowa oraz publikacja fragmentów pracy w „Przeglądzie Bezpieczeństwa Wewnętrznego".

Warunki:

Do konkursu uczestnicy zgłaszają własną pracę doktorską (I kategoria) napisaną w języku polskim i obronioną w latach 2007–2017 oraz pracę magisterską lub licencjacką (II kategoria) napisaną w języku polskim i obronioną na **oceną bardzo dobrą** w roku akademickim 2016/2017 lub poprzednim.

Organizator informuje, że prace będą oceniane w dwóch odrębnych kategoriach:

kategoria I – prace doktorskie,
kategoria II – prace magisterskie i licencjackie.

Prace wraz z wymaganymi dokumentami powinny zostać przesłane zarówno w wersji papierowej, jak i elektronicznej.

Dokumenty, które należy załączyć:

1. Wypełniony i podpisany formularz zgłoszenia do konkursu (plik do pobrania ze strony głównej Agencji Bezpieczeństwa Wewnętrznego).
2. Opinia promotora lub/i recenzenta.
3. Pisemna zgoda autora opinii/recenzji na jej wykorzystanie do celów konkursu.

Adres, na który należy przesłać pracę wraz z załącznikami:

Gabinet Szefa ABW
00-993 Warszawa
ul. Rakowiecka 2a

z dopiskiem na kopercie „KONKURS"

Adres e-mail, na który należy przesłać wersję elektroniczną pracy oraz skany załączników: redakcja.pbw@abw.gov.pl

Terminy:

Prace należy przesłać do 30 września 2017 roku (decyduje data stempla pocztowego).

Prace będzie oceniać Komitet Konkursowy powołany przez Szefa ABW, który wyłoni laureatów konkursu w terminie do 31 stycznia 2018 r.

Wyniki konkursu zostaną opublikowane na stronie internetowej www.abw.gov.pl w ciągu 14 dni od momentu wyboru laureatów przez Komitet Konkursowy. Laureaci otrzymają zawiadomienie o wynikach konkursu telefonicznie oraz drogą elektroniczną.

W formularzu zgłoszeniowym uczestnik akceptuje warunki konkursu oraz wyraża zgodę na:

1) upowszechnienie treści zawartych w ich pracy do celów promocji tematyki bezpieczeństwa państwa oraz do celów służbowych ABW,
2) gromadzenie i przetwarzanie swoich danych osobowych i ma prawo dostępu do ich treści oraz ich poprawiania zgodnie z przepisami ustawy z 29 sierpnia 1997 r. o ochronie danych osobowych (Dz.U. z 2002 r. Nr 101 poz. 926, ze zm.).

Dorian Duda

Operacyjne metody zwalczania terroryzmu w świetle polskiego i niemieckiego procesu karnego[1]

Wstęp

Kres drugiej wojny światowej rozpoczął zmiany w postrzeganiu wojny jako zjawiska. Stopniowo zaczęły tracić na znaczeniu międzypaństwowe konfrontacje, poprzedzane deklaracjami czy ultimatami. Coraz większą rolę zaczęły odgrywać organizacje militarne, które, korzystając z mniej lub bardziej konwencjonalnych metod, usiłują zbrojnie osiągać swoje cele. Dowodem na ich wzrastające znaczenie jest m.in. rozszerzenie interpretacji artykułu 51 Karty ONZ i uznanie niezbywalnego prawa państw do samoobrony także w przypadku napaści zbrojnej przez podmioty niepaństwowe. Tradycyjny termin w o j n a ustępuje miejsca pojęciu k o n f l i k t z b r o j n y, w którym próbuje się odzwierciedlić przekształcenia, z jakimi mierzą się instytucje dbające o zewnętrzne i wewnętrzne bezpieczeństwo państwa.

Złożoną wojnę hybrydową, która łączy elementy psychologiczne z niekonwencjonalnymi działaniami partyzanckimi, destrukcyjnym penetrowaniem cyberprzestrzeni, a także konwencjonalnymi działaniami militarnymi prowadzą ugrupowania terrorystyczne. Taka aktywność nie może zostać przypisana podmiotom państwowym i nie jest prowadzona na zasadach *iuris in bello*. W wielu wypadkach mechanizmy reagowania sprowadzają się zatem do wykorzystania istniejących przepisów prawa krajowego. Materialne prawo karne typizuje przestępstwa o charakterze terrorystycznym i przewiduje ich penalizowanie post factum. Dla bezpieczeństwa państwa ważniejsze są jednak możliwości, jakie w zakresie przeciwdziałania terroryzmowi i zapobiegania tym przestępstwom mają instytucje państwowe.

W niniejszym opracowaniu zostaną poddane analizie metody operacyjne służące zwalczaniu terroryzmu pre factum, wykorzystywane przez służby polskie i niemieckie. Należy zwrócić uwagę na to, że tego rodzaju narzędzia są uważane za swoistą „szarą strefę" i że niejednokrotnie ich charakter bywa podważany. Dzieje się tak dlatego, że działania operacyjne nie są precyzyjnie zdefiniowane, trudno je w sposób jednoznaczny zakwalifikować do danej dziedziny prawa, a ich podejmowanie niekiedy balansuje na granicy bezprawia i jest realizowane niejawnie. Metody, które są wykorzystywane do zminimalizowania takich zagrożeń, jak infiltracja środowisk religijnych, radykalizacja mniejszości narodowych czy zamachy terrorystyczne, stanowią zespół działań o charakterze wywiadowczym, analitycznym, informatycznym i policyjnym. W polskim systemie prawnym czynności operacyjno-rozpoznawcze są w doktrynie ujmowane tradycyjnie jako element postępowania karnego sensu largo. Jest to stanowisko sporne, gdyż z jednej strony są

[1] Fragmenty pracy magisterskiej pt. *Operacyjne metody zwalczania terroryzmu w świetle polskiego i niemieckiego procesu karnego*, która zajęła I miejsce w konkursie Szefa ABW na najlepszą pracę magisterską/licencjacką z dziedziny bezpieczeństwa wewnętrznego państwa (edycja 2015/2016). Autor jest absolwentem Uniwersytetu im. Adama Mickiewicza w Poznaniu i Uniwersytetu Europejskiego Viadrina we Frankfurcie nad Odrą oraz aplikantem adwokackim przy ORA we Wrocławiu. Redakcja dokonała w tekście niezbędnych poprawek oraz zmian numeracji przypisów (przyp. red.).

to działania na przedpolu procesu, z drugiej zaś – ich rezultat stanowią nierzadko przełomowe wskazówki lub nawet dowody w postępowaniu. W niniejszej pracy zostanie położony merytoryczny nacisk na karnoprocesowe aspekty owych metod.

Określenie zwalczanie terroryzmu użyte w tytule pracy należy rozumieć w dwojaki sposób. Po pierwsze – ma ono podkreślać prewencyjny charakter metod operacyjnych, czyli ich stosowanie przed zaistnieniem (lub w trakcie stadium przygotowawczego) czynu przestępnego spełniającego materialne przesłanki zawarte w kodeksie karnym. W tym sensie należy odróżnić zwalczanie terroryzmu od ścigania przestępstw o charakterze terrorystycznym, które ma charakter represyjny. Po drugie – termin zwalczanie (niem. *Bekämpfung*) jest szeroki. Zwalczanie operacyjne jest rozumiane nie tylko jako pojęcie dotyczące działań związanych z rozpoznawaniem zagrożeń (niem. *Aufklärung*) i zapobieganiem im (niem. *Verhütung*), lecz także wkracza w sferę zaistniałą po wystąpieniu zagrożenia, ale przed podjęciem ścigania, i obejmuje wykrywanie przestępstw (niem. *Aufdeckung*). Każdy z tych elementów ma charakter przedprocesowy i dotyczy działań podjętych przed popełnieniem przestępstwa lub przed wszczęciem postępowania. W odróżnieniu od nich – ze względu na swój represyjny, jawny i procesowy charakter – ściganie karne (niem. *Verfolgung*) trudno włączyć do takiej definicji w sensie operacyjnym, choć jego cele związane z prewencją ogólną i szczególną z pewnością można przypisać „zwalczaniu" sensu largo.

Zakres pracy został zawarty w czterech rozdziałach. W rozdziale pierwszym skatalogowano działania operacyjne w obrębie systemów (rozumianych szeroko) ścigania karnego Polski i Niemiec. Wyjaśniono charakter przestępstw terrorystycznych w każdym z państw, podjęto próbę zdefiniowania działań operacyjnych oraz przedstawiono problematykę ich rozgraniczenia w odniesieniu do typowych czynności wywiadowczych i procesowych. W rozdziale drugim przedstawiono analizę poszczególnych czynności operacyjnych na podstawie wybranych ustaw i ukazano podobieństwa i różnice w metodach zwalczania terroryzmu w Polsce i w Niemczech. Porównano też zdolności operacyjne Agencji Bezpieczeństwa Wewnętrznego oraz Federalnego Urzędu Kryminalnego (niem. *Bundeskriminalamt* – BKA). W rozdziale trzecim opisano wpływ metod operacyjnych na postępowanie karne oraz skoncentrowano się na wartości dowodowej wyników pracy operacyjnej w procesie karnym. Wskazano też na możliwości transgranicznego wykorzystania materiałów operacyjnych.

Rozdział czwarty poświęcono roli instytucji dbających o bezpieczeństwo Polski i Niemiec w świetle polsko-niemieckiej umowy o współpracy służb policyjnych, granicznych i celnych oraz współpracy międzynarodowej, a także w odniesieniu do prawa Unii Europejskiej. Opracowanie jest zakończone prawnoporównawczymi wnioskami i rozważaniami *de lege ferenda* dotyczącymi czynności operacyjno-rozpoznawczych i perspektyw ich wykorzystania w walce z międzynarodowym terroryzmem.

W niniejszej pracy wykorzystano polsko- i niemieckojęzyczną literaturę z zakresu procesowego prawa karnego oraz prawa policyjnego. Oparto się tu zarówno na komentarzach do ustaw, jak i artykułach z czasopism naukowych i monografiach tematycznych. Natomiast praca nie odnosi się kompleksowo do metod operacyjnych; poza zainteresowaniem pozostają takie sprawy, jak ochrona praw jednostki przy wykonywaniu czynności operacyjnych czy przegląd wszystkich instytucji policyjnych krajów związkowych oraz sposób ich operacyjnego współdziałania. Opracowanie odpowiada stanowi prawnemu na dzień 11 lipca 2016 r. i uwzględnia: *Ustawę z dnia 15 stycznia 2016 r. o zmia-*

nie ustawy o Policji oraz niektórych innych ustaw[2], *Ustawę z dnia 10 czerwca 2016 r. o działaniach antyterrorystycznych*[3] oraz wyrok Federalnego Trybunału Konstytucyjnego (niem. *Bundesverfassungsgericht* – BVerfG) z 20 kwietnia 2016 r.[4] dotyczący uprawnień Federalnego Urzędu Kryminalnego w ramach zwalczania terroryzmu. Całość ma charakter prawnoporównawczy, jednak zastosowana metodologia jest różna w zależności od opracowywanej problematyki.

W celu podkreślenia specyfiki związanej ze zróżnicowaną formą organizacji państwa, w pierwszym rozdziale zawarto osobne opracowania dla Polski i Niemiec. Tematyka drugiego i trzeciego rozdziału zezwala w większości na prowadzenie równoległych porównań, przepisy omawiane w rozdziale czwartym zaś są wspólne dla obydwu jurysdykcji.

Niniejsze opracowanie jest fragmentem pracy magisterskiej obronionej w ramach polsko-niemieckich studiów prawniczych prowadzonych przez Uniwersytet Europejski Viadrina we Frankfurcie nad Odrą we współpracy z Uniwersytetem im. Adama Mickiewicza w Poznaniu. Dokonanie analizy nie byłoby możliwe bez zaplecza naukowego i wsparcia dydaktycznego ze strony obydwu instytucji naukowych. Ich wieloletnie współdziałanie jest przykładem efektywnej współpracy polsko-niemieckiej, która powinna być inspiracją także dla podmiotów przeciwdziałających coraz bardziej niebezpiecznym zagrożeniom współczesnego, wielokulturowego społeczeństwa.

Rozdział I. Operacyjne zwalczanie terroryzmu a system bezpieczeństwa państwa

1. Uwagi wstępne

Rola i miejsce metod operacyjnych w strukturze systemu bezpieczeństwa państwa (systemu ścigania karnego sensu largo, nieograniczającego się wyłącznie do ścigania przestępstw już popełnionych) nie są oczywiste. Instrumenty, jakimi posługują się wybrane służby, aby zapobiec przestępstwom terrorystycznym, nie są ujęte tradycyjnie jako kodeksowe czynności procesowe. Już definicja metod operacyjnych sprawia trudności interpretacyjne i nie jest jednolita. Na potrzeby niniejszej pracy należy przez nie rozumieć uprawnienia i sposoby wykonywania czynności podejmowanych niejawnie przez powołane do tego służby państwowe. Metody, o których mowa, są związane z pozyskiwaniem danych o jednostkach oraz ich sposobie działania – w celu zwalczania (przede wszystkim rozpoznawania i zapobiegania, a także wykrywania i ścigania) przestępstw przed wszczęciem postępowania karnego. W niniejszym rozdziale przedstawiono charakterystykę różnych metod operacyjnych stosowanych na poszczególnych etapach zwalczania zagrożeń terrorystycznych oraz ich znaczenie w procesowym prawie karnym Polski i Niemiec. Ze względu na różnice w strukturze organizacyjnej państwa, a także czynniki historyczne mające wpływ na kształtowanie ram prawnych, najpierw przedstawiono złożony system Niemiec jako państwa federalnego, a następnie model znajdujący zastosowanie w państwie unitarnym, jakim jest Polska. (…)

[2] Dz.U. z 2016 r. poz. 147.

[3] Dz.U. z 2016 r. poz. 904.

[4] BVerfG, wyrok z 20 IV 2016 r. (1 BvR 966/09, 1 BvR 1140/09), „Neue Juristische Wochenschrift" (NJW) 2016, s. 1781.

3. Niemiecki model bezpieczeństwa państwa

3.1. Podział wertykalny – zasada państwa federalnego a rozdział kompetencji

Decentralizacja władzy i podział kompetencji w Republice Federalnej Niemiec mają istotny wpływ na strukturę systemu ścigania karnego i zwalczania zagrożeń bezpieczeństwa państwa oraz krajów związkowych. Zgodnie z kompetencją generalną (art. 70 GG[5]) to właśnie poszczególne kraje związkowe są w pierwszej linii uprawnione do stanowienia prawa, chyba że ustawa zasadnicza przyznaje kompetencje ustawodawstwu federalnemu. Te uprawnienia mogą mieć charakter wyłączny lub konkurencyjny, a operacyjne metody zwalczania terroryzmu można sklasyfikować w ramach wszystkich tych kategorii.

Do wyłącznej kompetencji ustawodawstwa federalnego należy (przez dodanie w 2006 r. ustępu 9a do art. 73 GG[6]) przeciwdziałanie zagrożeniom związanym z międzynarodowym terroryzmem przez Federalny Urząd Kryminalny w przypadkach niebezpieczeństw, które przekraczają ramy jednego kraju związkowego, gdy nie jest rozpoznana właściwość policji krajowej lub na wniosek najwyższych organów krajów związkowych. Zgodnie z art. 73 ust. 2 GG ustawy regulujące to zagadnienie są przyjmowane jako *Zustimmungsgesetz*, czyli w procedurze ustawodawczej wymagającej wyrażenia zgody przez izbę niższą parlamentu (niem. *Bundesrat*). Przepis art. 73 ust. 10 GG uprawnia ustawodawstwo centralne do uchwalania aktów prawnych odnoszących się do współpracy Federacji i krajów związkowych w ramach pracy policji kryminalnej (lit. a), ochrony konstytucji (lit. b) oraz ochrony przed działaniami zagrażającymi interesom zagranicznym federacji (lit. c), a także do utworzenia Federalnego Urzędu Kryminalnego i zwalczania przestępstw międzynarodowych (*in fine*). Na podstawie wymienionych przepisów ustawy zasadniczej uchwalono na szczeblu federalnym wiele ustaw, które konstytuują poszczególne służby oraz katalogują normy kompetencyjne zawierające poszczególne instrumenty operacyjne. Do najważniejszych aktów prawnych należą: ustawa o Federalnym Urzędzie Kryminalnym (niem. *Bundeskriminalamtgesetz* – BKAG[7]), ustawa o Federalnej Służbie Wywiadu (niem. *Gesetz über den Bundesnachrichtendienst* – BNDG[8]), ustawa o współpracy w sprawach ochrony konstytucji (niem. *Bundesverfassungsschutzgesetz* – BVerfSchG[9]) oraz ustawa o Urzędzie Kontrwywiadu Wojskowego (niem. *Gesetz über den militärischen Abschirmdienst* – MADG[10]).

W przypadku ustawodawstwa konkurencyjnego kraje związkowe dysponują kompetencją do stanowienia prawa na tyle, na ile nie skorzystała z niej Federacja. Materia niemieckiego prawa procesowego, bez rozróżnienia na dziedziny, a więc także materia postępowania karnego (art. 74 ust. 1 nr 1 GG), leży właśnie w tego rodzaju

[5] *Grundgesetz für die Bundesrepublik Deutschland* – ustawa zasadnicza Republiki Federalnej Niemiec (przyp. red.).

[6] Art. 1 nr 6 lit. a sublit. cc ustawy o zmianie Ustawy Zasadniczej (*Gesetz zur Änderung des Grundgesetzes*), z 28 VIII 2006 r. (BGBl. I S. 2034).

[7] Ustawa o Federalnym Urzędzie Kryminalnym oraz współpracy Federacji i krajów związkowych w sprawach policji kryminalnej (*Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten*) z 7 VII 1997 r. (BGBl. I S. 1650, ze zm.).

[8] Ustawa z 20 XII 1990 r. (BGBl. I S. 2954, 2979, ze zm.).

[9] Ustawa o współpracy Federacji i krajów związkowych w sprawach ochrony konstytucji oraz o Federalnym Urzędzie Ochrony Konstytucji (*Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz*) z 20 XII 1990 r. (BGBl. I S. 2954, 2970, ze zm.).

[10] Ustawa z 20 XII 1990 r. (BGBl. I S. 2954, 2977, ze zm.).

kompetencji konkurencyjnej. W rezultacie uchwalenia kodeksu postępowania karnego (niem. *Strafprozessordnung* – StPO[11]) na szczeblu federalnym oraz uznania go przez Federalny Sąd Najwyższy za wyczerpującą i zamkniętą regulację uniemożliwiono krajom związkowym uchwalanie aktów prawnych w tej materii[12]. Ten kodeks zawiera wykaz czynności procesowych oraz czynności o charakterze operacyjnym, wykorzystywanych w ramach ścigania sprawców przestępstw. Nad postępowaniem czuwa prokuratura kierująca czynnościami o charakterze represyjnym, podejmowanymi przez policję. Ściganie większości przestępstw konwencjonalnych leży w domenie odpowiedniej policji krajowej; jedynie w kilku wyjątkowych przypadkach właściwą instytucją policyjną jest Federalny Urząd Kryminalny. Ściganie przestępstw terrorystycznych o charakterze międzynarodowym (§ 4 ust. 1 nr 3 BKAG) lub popełnionych za granicą (nr 4) należy właśnie do takich przypadków.

Pozostałe uprawnienia operacyjne niemające charakteru procesowego (represyjnego), w związku z brakiem ograniczeń podyktowanych ustawą zasadniczą, są uchwalane zgodnie z art. 70 GG na szczeblu krajów związkowych. Uprawnienia, o których mowa, są zawarte przede wszystkim w wielu krajowych ustawach policyjnych oraz krajowych ustawach dotyczących ochrony konstytucji. Ich przepisy są stosowane, gdy wykorzystanie metod operacyjnych nie leży w gestii organów federalnych. Ze względu na wielość regulacji oraz dominującą, w przeważającej liczbie przypadków, kompetencję Federacji w zakresie zwalczania terroryzmu międzynarodowego – przepisy ustaw krajowych nie będą szczegółowo poruszane w niniejszej pracy.

3.2. Podział horyzontalny – charakterystyka modelu

W niemieckim systemie szeroko rozumianego przeciwdziałania przestępczości, niezależnie od podziału pionowego, można wyróżnić trzy reżimy, w których Federacja i kraje związkowe podejmują określone działania. Po pierwsze, służby wywiadowcze i kontrwywiadowcze zbierają i opracowują informacje o potencjalnych zagrożeniach bezpieczeństwa państwa i poszczególnych krajów. Po drugie, służby policyjne mają za zadanie zapobiegać przestępstwom, zanim zostaną one popełnione. Po trzecie, gdy prewencja zawiedzie, sprawców zaistniałych przestępstw ściga prokuratura.

Mimo teoretycznie jasnego podziału kompetencji, rozgraniczenie zadań między wyżej wymienionymi organami stwarza kilka problemów. W obliczu uwarunkowań historycznych niemieckie prawo ustanowiło specyficzną zasadę rozdziału instytucjonalnego między służbami wywiadowczymi a policyjnymi. Współpraca między nimi, która wydaje się oczywista dla sprawnego funkcjonowania aparatu bezpieczeństwa państwa i prewencji terrorystycznej, jest dużo bardziej skomplikowana, niż w innych państwach. Jak wyjaśniono, ściganie karne sensu stricto podlega rygorowi kodeksu postępowania karnego, który jest jednolitą regulacją dla całego państwa. Inaczej jest w przypadku policyjnych działań prewencyjnych, których ramy prawne znajdują się przynajmniej w 16 ustawach policyjnych, odrębnych dla każdego kraju związkowego, co niesie za sobą zróżnicowanie uprawnień[13]. Przyporządkowanie instrumentów operacyjnych do

[11] Kodeks postępowania karnego (*Strafprozeßordnung*) z 7 IV 1987 r. (BGBl. I S. 1074, 1319, ze zm.).

[12] BGH (*Bundesgerichtshof* – Federalny Sąd Najwyższy – przyp. red.), wyrok z 23 II 1962 r. (4 StR 511/61), NJW 1962, s. 1020.

[13] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 27.

konkretnego reżimu jest niezbędne przy analizie uprawnień danego organu. Co ważniejsze, umożliwia to również zdefiniowanie odpowiedniej drogi odwoławczej: administracyjnej – w przypadku czynności prewencyjnych oraz karnoprocesowej – wobec czynności podejmowanych na polecenie prokuratury.

3.2.1. Konsekwencje konstytucyjnego rozdziału między służbami wywiadowczymi a policją

Przyczynkiem do wprowadzenia zasady rozdziału między służbami wywiadowczymi a policyjnymi (niem. *Trennungsgebot*) był tzw. list policyjny gubernatorów militarnych do prezydenta Rady Parlamentarnej z 14 kwietnia 1949 r.[14] Określał on zakaz nadawania uprawnień policyjnych instytucjom pozyskującym i opracowującym informacje wywiadowcze. Ten rozdział ma znaczenie zarówno kompetencyjne, jak i organizacyjne[15], a jego genezą są gorzkie doświadczenia związane z drugą wojną światową i rolą Gestapo (niem. *Geheime Staatspolizei*) oraz Głównym Urzędem Bezpieczeństwa Rzeszy (niem. *Reichssicherheitshauptamt*), które łączyły w sobie uprawnienia wykonawcze i wywiadowcze[16]. Wraz z uchwaleniem konstytucji, w związku z brakiem jednoznacznej normy potwierdzającej tę zasadę, zaczęto wywodzić ją z przepisu art. 87 ust. 1 zd. 2 GG lub z zasady państwa prawa (art. 20 ust. 3 GG). W rezultacie przeważająca część literatury nadaje jej rangę konstytucyjną, choć często spotyka się opinie odrębne[17].

Trennungsgebot z pewnością znajduje jednak przynajmniej częściowe odzwierciedlenie w materii ustawowej. Przepisy wskazujące na to zjawisko znajdują się w każdym z aktów normatywnych ustanawiających służby specjalne[18]. Natomiast działania wywiadowcze podejmowane przez policję operacyjne są nazywane środkami wywiadowczymi (niem. *nachrichtendienstliche Mittel*) i nie mają charakteru wykonawczego, a jedynie informacyjny. Służbom specjalnym wyraźnie nie przysługują imperatywne uprawnienia związane ze stosowaniem przymusu (jak np. prowadzenie przesłuchań, przeszukań czy dokonywanie zajęcia mienia)[19]. Działają one na przedpolu zagrożeń

[14] Tzw. *Polizeibrief der Alliierten Militärgouverneure vom 14. April 1949*, w: *Deutscher Bundestag/Bundesarchiv*, Der Parlamentarische Rat 1948–1949, Bd. 8, s. 230 i nast.

[15] N. Gazeas, *Übermittlung nachrichtendienstlicher Erkentnisse an Strafverfolgungsbehörden*, Berlin 2014, s. 58 i nast.

[16] M. Ostheimer, *Verfassungsschutz nach der Wiedervereinigung*, Frankfurt am Main 1994, s. 63.

[17] Przeciwnicy podkreślają absurd argumentacji wywodzonej z art. 87 ust. 1 zd. 2 GG, a polegającej na tym, że wyszczególnienie policji i służb wywiadowczych jako dwóch różnych instytucji w jednym przepisie absolutnie nie musi prowadzić do tego, że należy te służby postrzegać jako niezwiązane ze sobą. Posiadanie uprawnień policyjnych przez służby wywiadowcze w innych krajach nie stoi w sprzeczności z zasadą państwa prawa. Przeciw randze konstytucyjnej argumentuje Kay Nehm, *Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur*, NJW 2004, s. 3290; innego zdania są Fredrik Roggen i Nils Bergemann, *Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland – Anti-Terror-Datei, gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz*, NJW 2007, s. 876.

[18] Zarówno federalne: § 1 ust. 1 w zw. z § 2 ust. 3 BNDG, § 2 ust. 1 w zw. z § 8 ust. 3 BVerfSchG, § 1 ust. 4 w zw. z § 4 ust. 2 MADG, jak i krajowe (niektóre przykłady): § 2 ust. 2 w zw. z § 6 ust. 4 BbgVerfSchG (*Brandenburgisches Verfassungsschutzgesetz* – przyp. red.), § 2 ust. 1 w zw. z § 8 ust. 7 VSG Bln (*Verfassungsschutzgesetz Berlin* – przyp. red.), art. 1 ust. 4 BayVSG (*Bayerisches Verfassungsschutzgesetz* – przyp. red.), § 2 ust. 1 w zw. z § 5 ust. 9 VSG NRW (*Verfassungsschutzgesetz Nordrhein-Westfalen* – przyp. red.). W każdym przypadku są to przepisy zabraniające włączania służb w struktury policyjne oraz nadawania im uprawnień policyjnych lub kierowniczych względem policji.

[19] F. Roggen, N. Bergemann, *Die „neue Sicherheitsarchitektur" der Bundesrepublik Deutschland – Anti-Terror-Datei*, *gemeinsame Projektdateien und Terrorismusbekämpfungsergänzungsgesetz*,

(niem. *Gefahrenvorsorge*), w odróżnieniu od policji, która ma za zadanie je odpierać (niem. *Gefahrenabwehr*)[20].

Wywodzona z konstytucji zasada rozdziału powinna znajdować zastosowanie w obydwu kierunkach; ustawodawstwo administracyjne jednak nie odmawia służbom policyjnym uprawnień quasi-wywiadowczych. Instrumenty policyjne służące odpieraniu zagrożeń są uregulowane w przeważającej części w przepisach krajów związkowych i określa się je mianem środków przymusowych (niem. *polizeiliche Zwangsmaßnahmen*), mimo że wiele z nich nie ma stricte przymusowego charakteru[21]. W większości przypadków policja nie byłaby w stanie skutecznie wypełniać swoich zadań, jeśli musiałaby pozostać bezczynna aż do momentu powstania zagrożenia[22]. Wzrost znaczenia przestępczości zorganizowanej oraz wyzwania stawiane przez terroryzm powodują, że zbieranie i analizowanie informacji często decydują o późniejszym powodzeniu operacji neutralizujących. Mimo to, nadawanie uprawnień o charakterze bliskim wywiadowczemu, które policja otrzymała w ostatnich latach w celu umożliwienia skutecznego zwalczania terroryzmu, wznowiło debatę o iluzoryczności zasady rozdziału[23].

Istnieje pogląd, że policja nie może mieć uprawnień do pozyskiwania informacji, jeśli nie istnieje bezpośredni związek z odpieraniem konkretnego zamachu na porządek publiczny[24]. W przeciwieństwie do operacji służb specjalnych, które nie zawsze muszą być nakierowane na konkretne niebezpieczeństwo, obserwacje policyjne nie mogą mieć charakteru prewencji generalnej. Trudno jest jednak jednoznacznie odpowiedzieć na pytanie, gdzie leży granica między wywiadowczymi a policyjnymi działaniami operacyjnymi. Zarówno pierwsze, jak i drugie są prowadzone co do zasady niejawnie, dlatego kryterium tajności nie wydaje się być przesądzające. Dużo bardziej przekonuje kryterium celu – niemieckie służby policyjne podejmują czynności operacyjne, aby bezpośrednio zapobiegać przestępstwom, służby zbierają i analizują informacje, aby następnie przekazać je instytucjom mającym odpowiednie kompetencje wykonawcze. Policja prowadzi obserwację zachowań bezprawnych lub takich, których skutkiem bezpośrednim jest złamanie prawa. Służby specjalne zaś są zainteresowane również działalnością zgodną z prawem, która może być istotna z punktu widzenia bezpieczeństwa państwa. Działania informacyjne wywiadu mają więc charakter prewencji generalnej, policyjne zaś prewencji bezpośredniej. Wszczęcie postępowania karnego nie wyklucza dalszego prowadzenia obserwacji o charakterze wywiadowczym, nie przeszkadza ona bowiem toczącemu się postępowaniu. Mimo wszystko, w świetle zasady rozdziału, możliwość równoległego prowadzenia obydwu typów operacji i faktyczne wymieszanie działań policyjnych i wywiadowczych wymusza dalsze pytania związane z dopuszczalnością współpracy i wymianą informacji[25].

NJW 2007, s. 876.

[20] M. Ostheimer, *Verfassungsschutz*…, s. 77.

[21] Podobnie A. Demenko i P. Nalewajko, *Transfer dowodów między państwami Unii Europejskiej*, w: *Unijna polityka karna*, A.J. Szwarc (red.), Poznań 2011, s. 100.

[22] M. Ostheimer, *Verfassungsschutz*…, s. 79.

[23] N. Gazeas, *Übermittlung nachrichtendienstlicher Erkentnisse*…, s. 60.

[24] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*…, s. 27.

[25] K. Nehm, *Das nachrichtendienstliche Trennungsgebot und die neue Sicherheitsarchitektur*, NJW 2004, s. 3293.

3.2.2. Odpieranie zagrożeń (niem. Gefahrenabwehr) a ściganie karne (niem. Strafverfolgung)

Działania operacyjne mogą być podejmowane przez policję z własnej inicjatywy lub na polecenie prokuratury. W pierwszym przypadku są one oparte na prawie policyjnym, będącym częścią prawa administracyjnego, w drugim natomiast mają podstawę w prawie karnym procesowym. Przyporządkowanie operacyjnych działań policyjnych do jednego z tych obszarów jest niezbędne z kilku powodów. Po pierwsze, umożliwia to określenie rodzaju ochrony prawnej. Wobec działań prewencyjnych policji następuje ona w drodze administracyjnej, podjęcie działań represyjnych zaś powoduje otwarcie drogi odwoławczej w postępowaniu karnym. Po drugie, każdy z obszarów ma podstawy w odrębnej kompetencji ustawodawczej. Ustawodawstwo policyjne należy do kompetencji krajów związkowych, postępowanie karne natomiast jest uregulowane na poziomie federalnym. Po trzecie, policja jest związana poleceniami prokuratury tylko w przypadku podjęcia czynności procesowych w ramach ścigania karnego[26]. Po czwarte, policja, odpierając zagrożenia, kieruje się zasadą oportunizmu i samodzielnie decyduje, czy i w jaki sposób stosuje swoje uprawnienia. W niemieckim postępowaniu karnym jest stosowana zasada legalizmu, która zobowiązuje prokuraturę, a więc też działającą pod jej pieczą policję, do ścigania popełnionego przestępstwa[27].

Działania podejmowane przez policję z własnej inicjatywy mają charakter prewencyjny i służą zapobieganiu czynom przestępnym, natomiast te, nad którymi czuwa prokuratura, mają charakter represyjny i służą ściganiu już popełnionych przestępstw. Punktem wyjścia do rozważań o granicy pomiędzy nimi jest tzw. początkowe podejrzenie popełnienia przestępstwa (niem. *Anfangsverdacht*) w rozumieniu § 152 ust. 2 StPO. Występuje ono, jeśli zaistnieją wystarczające, rzeczywiste oznaki popełnienia przestępstwa. Dla wystąpienia tej przesłanki wystarczy niewysoki próg prawdopodobieństwa, jednak oznaki te nie mogą być wyłącznie teoretyczne[28]. W przypadku, gdy są one niewystarczające, szczególnie gdy okażą się bezpodstawne i nieprawidłowe, działania operacyjne muszą być oparte na ustawodawstwie policyjnym. Instrumenty operacyjne w ustawach policyjnych i kodeksie postępowania karnego są podobne, chociaż zgodnie z zasadą stosowania prawa karnego – także procesowego – jako *ultima ratio*, do czynności procesowych można sięgnąć dopiero wtedy, gdy doszło do czynu zabronionego, a więc niebezpieczeństwo przestało istnieć[29]. Problemy pojawiają się wówczas, gdy policja podejmuje czynności chroniące przed przyszłym niebezpieczeństwem i jednocześnie zabezpiecza dowody dla celów postępowania karnego. Takie przypadki należy jednak rozpatrywać indywidualnie, mając na uwadze to, że dane metody operacyjne występują zarówno jako czynności represyjne, jak i prewencyjne, i są obarczone tylko innymi rygorami w zależności od powodu ich podjęcia. Od operacyjnych czynności policyjnych i operacyjnych czynności procesowych należy odróżnić czynności wstępne (niem. *Vorermittlungen*), które podejmuje prokuratura w celu potwierdzenia informacji o prawdopodobieństwie popełnienia przestępstwa przed wszczęciem postępowania karnego, jednak po zaistnieniu niebezpieczeństwa[30]. (…)

[26] M. Walden, *Zweckbindung und änderung präventiv und repressiv erhobener Daten im Bereich der Polizei*, Berlin 1996, s. 151.

[27] Tamże, s. 220 i cytowana tam literatura.

[28] Tamże, s. 166.

[29] Tamże, s. 216.

[30] B. Wölfl, *Vorermittlungen der Staatsanwaltschaft*, „Juristische Schulung" 2001, s. 479.

Rozdział II. Instrumenty operacyjne służące przeciwdziałaniu terroryzmowi w ujęciu prawnoporównawczym

1. Uwagi wstępne

W niniejszym rozdziale zostaną omówione poszczególne instrumenty operacyjne stosowane w ramach prewencji antyterrorystycznej. Działania oparte jedynie na stosowaniu kar nie są w stanie skutecznie przeciwstawić się organizacjom terrorystycznym. O wiele ważniejsze jest aprioryczne zwalczanie terroryzmu oraz obserwowanie kierunków rozwoju środowisk terrorystycznych[31]. Analizie zostaną tu poddane przede wszystkim przepisy ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu[32], a także ustawy o Federalnym Urzędzie Kryminalnym. Jest to podyktowane kilkoma względami. Po pierwsze, ABW i BKA dysponują porównywalnymi uprawnieniami, zarówno w zakresie pozyskiwania informacji o zagrożeniach oraz przestępstwach terrorystycznych, jak i podejmowania działań zapobiegawczych pod kątem ich zwalczania. Po drugie, z ustaw kompetencyjnych wynika ich wiodąca rola w zwalczaniu terroryzmu. Po trzecie, pomimo tego, że BKA jest instytucją policyjną, a nie klasyczną służbą wywiadowczą, dysponuje kompetencjami o charakterze bliskim wywiadowczemu w zakresie pozyskiwania informacji, które pozostają w bezpośrednim związku z zagrożeniami terrorystycznymi. Jednocześnie, podobnie jak ABW, wykonuje obowiązki przynależące organom ścigania w przypadku tego rodzaju przestępstw. Uprawnienia dochodzeniowo-śledcze pozostają jednak poza zakresem tej pracy.

Czynności operacyjno-rozpoznawcze przeprowadzane przez służby polskie, w zależności od celu ich wykonywania, mogą być stosowane nie tylko w ramach niemieckich policyjnych środków prewencyjnych, lecz także środków wywiadowczych i instrumentów procesowych. Poniższa analiza będzie zawierać również uwagi i odesłania do wywiadowczego reżimu prawnego, ich odpowiedniki procesowe natomiast zostaną objaśnione w rozdziale III.

Omawiane przepisy ustawy o Federalnym Urzędzie Kryminalnym zawierają normy kompetencyjne znane z innych ustaw policyjnych. Uprawnienia, które BKA zyskało w 2008 r., są trzonem reformy związanej ze zwalczaniem terroryzmu[33]. Stanowią one podstawę prawną zwalczania zagrożeń i zapobiegania przestępstwom związanym z terroryzmem międzynarodowym, które są wyliczone w przepisie § 4a ust. 1 zd. 2 BKAG. Mimo wiodącej roli BKA w prewencji terrorystycznej, to instytucje policyjne krajów związkowych – co do zasady – są odpowiedzialne za odpieranie zagrożeń[34]. Ustawa przewiduje sytuacje wyjątkowe, w których instytucją właściwą do zwalczania terroryzmu jest Federalny Urząd Kryminalny[35]. Wiele przepisów ustawy o BKA zostało uznanych za niezgodne z konstytucją, jednak bez wywołania ich natychmiastowej nieważności. Nie były to jednak przepisy dotyczące właściwości Urzędu, która nie podle-

[31] S. Pikulski, *Prawne środki zwalczania terroryzmu*, Olsztyn 2000, s. 121.

[32] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (tekst jednolity: Dz.U. z 2016 r. poz. 1897).

[33] Te uprawnienia zostały włączone do ustawy o Federalnym Urzędzie Kryminalnym w drodze ustawy o odpieraniu zagrożeń międzynarodowego terroryzmu (*Gesetz zur Abwehr von Gefahren des internationalen Terrorismus durch das BKA*) z 25 XII 2008 r. (BGBl. I S. 3083).

[34] D. Kugelmann, BKA-Gesetz, § 20a BKAG (*Bundeskriminalamtgesetz*, BKA-Gesetz – przyp. red.), nb. 17 (numer boczny poszczególnych akapitów – przyp. red.).

[35] Paragraf 4a ust. 1 BKAG; szerzej omówione w rozdziale I, podpunkt 3.3.

ga konstytucyjnej wątpliwości i jest zgodna z ustawą zasadniczą, o ile jest subsydiarna względem właściwości policji krajów związkowych. Przepisy niekonstytucyjne zostaną w niniejszym opracowaniu wskazane. Będą one obowiązywały do uchwalenia nowych regulacji, jednak nie później niż do 30 czerwca 2018 r.[36] (…)

2.3.3. Funkcjonariusz działający pod przykryciem

Wykorzystanie funkcjonariusza wykonawczego Policji, działającego pod przykryciem (niem. *Verdeckter Ermittler*) i posługującego się tzw. legendą, jest przewidziane w przepisie § 20g ust. 5 BKAG. Służy ono wspomnianym już celom wszystkich szczególnych środków pozyskiwania informacji, wymienionych w podrozdziale 2.3. Funkcjonariusz operacyjny, działając pod legendą, jest uprawniony do dysponowania odpowiednio przygotowanymi dokumentami i może brać udział w obrocie prawnym. Może on wejść do mieszkania osoby obserwowanej za jej zgodą, ale nie może przy tym podawać fałszywych informacji wykraczających poza legendę, aby ten dostęp uzyskać. W wyniku wyroku Federalnego Trybunału Konstytucyjnego podejmowanie czynności pod przykryciem w każdym przypadku wymaga sądowego zarządzenia, mimo rozróżnienia w ustawie sytuacji, w których zadaniem funkcjonariusza jest obserwowanie konkretnej osoby, od tych, w których celem jest wkroczenie do mieszkania[37]. W przypadkach nieuchronnego zagrożenia wobec chronionego dobra prawnego, następcza decyzja sądu może zostać uzupełniona w ciągu trzech dni. Ten instrument zarządza się na maksymalnie dwa miesiące, a jego przedłużenie o ten sam okres wymaga ponownego sądowego zarządzenia.

Nieco ogólniej przedstawia się regulacja dotycząca używania dokumentów i oznaczeń kamuflujących w ramach działalności wywiadowczej, zawarta w § 8 ust. 2 BVerfSchG. Ich wykorzystanie jest szczegółowo określone w regulacjach wewnętrznych służb wywiadowczych. Zasady korzystania z legendy określa natomiast przepis § 9a BVerfSchG. Wywiadowcza praca pod przykryciem nie służy bezpośredniemu zwalczaniu zagrożeń, lecz rozpoznawaniu ich możliwych źródeł.

W ustawie o ABW oraz AW środkiem ekwiwalentnym do przepisów niemieckich jest art. 35 ust. 2. Jest to uprawnienie polegające na posługiwaniu się dokumentami legalizacyjnymi, uniemożliwiającymi ustalenie danych identyfikujących pracowników danej służby oraz środków, którymi się posługują przy realizacji swoich zadań[38]. Funkcjonariusze ABW działają jako zakamuflowani agenci organów operacyjnych i posługują się zmienioną tożsamością[39]. Agencja Bezpieczeństwa Wewnętrznego jest odpowiedzialna za sporządzenie dokumentów legalizacyjnych. Przepisy dotyczące działalności pod przykryciem milczą na temat szczegółowości celów; służba pod przykryciem jest wykonywana w związku z ustawowymi zadaniami Agencji. Uznaje się, że nie jest również możliwe określenie liczby dokumentów legalizacyjnych, którymi można się posłużyć[40]. Przepis, o którym mowa wyżej, nie odnosi się do ograniczeń stosowania tej formy działań operacyjnych oraz nie wskazuje na materiały zbierane przy jej użyciu. Dla tych ograniczeń istotne są jednak same czynności (zachowania będące przedmiotem

[36] BVerfG, wyrok z 20 IV 2016 r. (1 BvR 966/09, 1 BvR 1140/09), NJW 2016, s. 1781, nb. 355 i nast.
[37] BVerfG, wyrok z 20 IV 2016 r. (1 BvR 966/09, 1 BvR 1140/09), NJW 2016, s. 1781, nb. 358.
[38] R. Lizak, *Dokumenty legalizacyjne w służbach specjalnych,* „Prokuratura i Prawo" 2013, nr 2, s. 142.
[39] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*..., s. 305.
[40] R. Lizak, *Dokumenty legalizacyjne*..., s. 149.

innych instrumentów operacyjnych), a nie forma (ramy) podejmowania tych czynności[41]. Mimo to, nie wszystkie działania funkcjonariuszy pod przykryciem są usystematyzowane w ustawie. Prowadzenie działalności wywiadowczej rozumiane jako uzyskiwanie informacji dzięki swobodnej rozmowie z inną osobą jest jednym z takich działań. Podobnie infiltracja środowiskowa, czyli przeniknięcie do środowiska kryminalnego lub zyskanie w nim sprzymierzeńców, jest jedną z niepisanych czynności operacyjno-rozpoznawczych podejmowanych przez funkcjonariuszy pod przykryciem[42].

Dla tajnej działalności funkcjonariuszy nie mniej istotny jest art. 56 ust. 2 ustawy o ABW oraz AW, który mimo systematycznego umieszczenia w rozdziale zawierającym przepisy kadrowe, a nie konkretne uprawnienia, umożliwia oddelegowanie funkcjonariusza do wykonywania zadań służbowych poza Agencję. Ten przepis może być podstawą prawną do podejmowania specyficznych form tajnego działania poza Agencją, jednak – podobnie jak w przypadku art. 35 ust. 2 tej ustawy – nie jest to w polskim prawie konkretny instrument operacyjny. Tak oddelegowany funkcjonariusz pozostaje do dyspozycji szefa ABW; możliwe jest również oddelegowanie go do pełnienia służby poza granicami kraju[43]. Działalność tzw. nielegałów jest najbardziej tajną formą podejmowania czynności operacyjnych, wykorzystywaną szczególnie w celu zakonspirowania działań wywiadowczych prowadzonych długofalowo i powiązanych z infiltracją danego środowiska[44].

W Niemczech przeniesienie federalnego wykonawczego urzędnika policyjnego (niem. *Versetzung eines Polizeivollzugsbeamten des Bundes*) na stanowisko w innej instytucji państwowej (§ 8 ust. 2 *Bundespolizeibeamtengesetz* – BPolBG[45]) jest możliwe w przypadku, gdy (…) *zaistnieje służbowa potrzeba*. Jeśli nie dysponuje on odpowiednimi umiejętnościami, to umożliwia mu się ich zdobycie w czasie pełnienia służby policyjnej. Zgodnie z oficjalnymi danymi w okresie między 1 stycznia 2013 r. a 5 czerwca 2014 r. 66 funkcjonariuszy BKA i Policji Federalnej zostało odesłanych do służby w BfV (niem. Bundesamt für Verfassungsschutz – Federalny Urząd Ochrony Konstytucji), jednak na podstawie przepisów o tymczasowym odesłaniu (niem. *Abordnung*) zgodnie z § 27 *Bundesbeamtengesetz* – BBG[46] (zachowali oni jednocześnie swoje stanowisko w strukturach policji[47]). (…)

4. Wnioski prawnoporównawcze

Kompetencje związane z rozpoznawaniem przestępstw terrorystycznych przez Federalny Urząd Kryminalny, zapobieganiem im oraz ich wykrywaniem stanowi wyjątek od reguły mówiącej o tym, że to policja krajów federalnych jest odpowiedzialna za

[41] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*…, s. 305.

[42] T. Hanausek, *Kryminalistyka. Zarys wykładu*, Warszawa 2009, s. 114, 116.

[43] Paragraf 9 ust. 1 oraz § 17 *Rozporządzenia Prezesa Rady Ministrów z dnia 16 lutego 2004 r. w sprawie warunków i trybu oddelegowania funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego do wykonywania zadań poza Agencją* (Dz.U. z 2004 r. Nr 34 poz. 296).

[44] Więcej na ten temat zob. A. Kowalski, *Rosyjski sztylet. Działalność wywiadu nielegalnego*, Łomianki 2013; C. Bielakowski, *Polski nielegał*, „Wprost" [online] z 10 listopada 2014 r., https://www.wprost.pl/479195/Polski-nielegal [dostęp: 16 VI 2016]; P. Briançon, *The Spanish Story Of A Russian 'Illegal'*, „Politico" [online] z 16 czerwca 2016 r., http://www.politico.eu/interactive/the-spanish-story-of-a-russian-illegal-russian-spy-moscow/ [dostęp: 22 VI 2016].

[45] Ustawa o federalnych urzędnikach policyjnych z 3 VI 1976 r. (BGBl. I S. 1357, ze zm.).

[46] Ustawa o urzędnikach federalnych z 5 II 2009 r. (BGBl. I S. 160, ze zm.).

[47] Deutscher Bundestag, 18. Wahlperiode, Schriftliche Fragen mit den in der Woche vom 10. Juni 2014 eingegangenen Antworten der Bundesregierung, z 13 VI 2014 r., BT-Drs (B*undestagsdrucksache* – przyp. red.) 18/1742, s. 28.

zwalczanie zagrożeń. Każdy z instrumentów operacyjnych z wykazu zawartego w § 20a i następnych BKAG, którymi dysponuje ten organ, nawiązuje w swojej treści do celów związanych ze zwalczaniem terroryzmu. Odmiennie sytuacja kształtuje się w przypadku ABW, dla której zarówno zwalczanie terroryzmu[48], jak i ściganie jego sprawców jest jednym z wielu zadań, co do których podejmuje działania zapobiegawcze.

Z punktu widzenia charakteru działalności Federalny Urząd Kryminalny jest określany jako rodzaj służby policyjnej. Chociaż w literaturze dostrzega się jego podobieństwo do służb specjalnych – ze względu na rodzaj podejmowanych czynności – to przynajmniej z prawnego punktu widzenia BKA służbą specjalną nie jest[49]. Zgoła inaczej wygląda to w przypadku Agencji Bezpieczeństwa Wewnętrznego. Jest to jednocześnie organ ścigania, instytucja o charakterze policyjnym i krajowa służba specjalna zajmująca się prowadzeniem kontrwywiadu. Ze względu na nieistniejący w Polsce rozdział między służbami specjalnymi a policją, przyznanie ABW kompetencji analityczno-informacyjnych, operacyjno-rozpoznawczych i dochodzeniowo-śledczych nie stanowi problemu prawnego. Wiele czynności operacyjno-rozpoznawczych jest wykorzystywanych jednocześnie jako metody wywiadowcze, powiązane z celami analityczno-informacyjnymi. W Niemczech zarówno poszczególne instrumenty, jak i kompetencje odpowiednich służb w zakresie działalności (kontr-)wywiadowczej, są wymienione w odrębnych aktach prawnych.

Federalny Urząd Kryminalny i Agencja Bezpieczeństwa Wewnętrznego mają podobne uprawnienia operacyjne w zakresie prewencji antyterrorystycznej. Dlatego w ramach współpracy międzynarodowej można je uznać za instytucje porównywalne. Istotna różnica między charakterem analizowanych czynności wykonywanych przez Urząd i Agencję wynika z ich celu. Ustawa o BKA zawiera instrumenty służące rozpoznawaniu i wykrywaniu przestępstw, a także zapobieganiu im, podczas gdy czynności podejmowane przez ABW mogą mieć również funkcję represyjną, a więc mogą służyć ściganiu karnemu. Podstawą do podejmowania czynności represyjnych przez BKA w warunkach wyjątkowych jest niemiecki kodeks postępowania karnego. Z kolei czynności prewencyjno-policyjne wymagają sądowego zarządzenia tylko w najpoważniejszych przypadkach, gdyż z natury rzeczy nie są umyślnie podejmowane podczas procesu karnego.

Regulacja niemiecka przewiduje klauzulę generalną, która pozwala Federalnemu Urzędowi Kryminalnemu na podejmowanie wszelkich niezbędnych czynności w celu odparcia zagrożenia terrorystycznego, jeżeli nie są one określane w ustawie jako jeden z instrumentów. Ustawa o ABW oraz AW co prawda nie jest opatrzona klauzulą generalną, jednak w związku z tym, że pojęcie czynności operacyjno-rozpoznawcze nie ogranicza się do „instrumentów operacyjnych zawartych w ustawie", oraz zważywszy na przepis art. 19 ust. 3 ustawy o ABW oraz AW, także Agencja Bezpieczeństwa Wewnętrznego ma uprawnienie do zapobiegania aktom terrorystycznym. Na podstawie ustawy o działaniach antyterrorystycznych można wręcz wywieść obowiązek spoczywający na szefie ABW, zgodnie z którym jest on zobowiązany do zwalczania przestępstwa terroryzmu.

Tajne metody uzyskiwania informacji o osobach mogących stanowić zagrożenie bezpieczeństwa państwa i przetwarzania danych osobowych wymagają podstawy prawnej. W przypadku regulacji niemieckich znajduje się ona w każdym przepisie normują-

[48] Por. definicję pojęć zwalczanie i ściganie we wstępie opracowania.

[49] G. Weber, *Das Bundeskriminalamt und seine geheimdienstliche Tätigkeit. Abschied vom Legalitätsprinzip*, „vorgänge" 1982, nr 55 (z. 1: *Geheimdienste der Bundesrepublik*), s. 69.

cym poszczególny instrument operacyjny. Przepis § 20b BKAG należy rozumieć jako klauzulę na wypadek, gdyby przetwarzanie danych na podstawie innych przepisów nie było wystarczające do zapobieżenia przestępstwu terrorystycznemu. Polska regulacja dotycząca zbierania danych jest natomiast bardzo szeroka i niedookreślona. Agencja Bezpieczeństwa Wewnętrznego ma uprawnienie do pozyskiwania danych w zakresie swojej właściwości. Regulacja polska i niemiecka charakteryzują się tzw. modelem podwójnych drzwi, zgodnie z którym z jednej strony uprawnienie do zbierania danych ma podstawę w prawie policyjnym, z drugiej natomiast obowiązek przekazywania danych odpowiednim służbom jest nakładany na usługodawców w ustawach dotyczących świadczenia określonych usług.

Należy również zwrócić uwagę na pokrewność przechowywania danych osobowych związanych z potencjalnymi sprawcami przestępstw terrorystycznych. Działająca w Niemczech antyterrorystyczna baza danych (niem. *Antiterrordatei*) znalazła swoje odwzorowanie w polskich przepisach wraz z wejściem w życie ustawy o działaniach antyterrorystycznych. Na podstawie tego aktu prawnego sporządzono wykaz zawierający informacje o osobach ważnych z uwagi na zwalczanie terroryzmu. Wykaz ten jest prowadzony przez szefa ABW (art. 6 ustawy o działaniach antyterrorystycznych).

Do tzw. szczególnych środków pozyskiwania danych, które są wymienione w ustawie o BKA, należą: długotrwała obserwacja (z możliwością zastosowania środków technicznych), stosowanie środków technicznych poza mieszkaniem oraz instytucja funkcjonariusza pod przykryciem i tajnego współpracownika. Możliwość prowadzenia obserwacji, także przy zastosowaniu środków technicznych (zarówno obserwacji, jak i podsłuchu poza mieszkaniem), jest uregulowana jako uprawnienie funkcjonariuszy ABW, z którego korzystają oni podczas realizowania zadań. Po raz kolejny polska regulacja charakteryzuje się wyjątkowym stopniem ogólności i nie precyzuje, tak jak jej niemiecki odpowiednik, zakresu i ograniczeń dotyczących jej wykorzystania. Ponadto tzw. policyjna obserwacja szczególna, będąca w Niemczech instrumentem operacyjnym, nie jest znana polskiemu systemowi jako metoda wykonywania czynności, lecz wynika z ogólnej współpracy służb między sobą, mając także na uwadze koordynację czynności analityczno-informacyjnych w ramach ustawy o działaniach antyterrorystycznych.

Służba pod przykryciem oraz nawiązywanie tajnej współpracy są w polskim prawie jedynie formą podejmowania czynności operacyjno-rozpoznawczych, a nie konkretnym instrumentem operacyjnym, tak jak ma to miejsce na gruncie ustawy o Federalnym Urzędzie Kryminalnym. Funkcjonariusze pod przykryciem w obydwu systemach prawnych mogą korzystać z dokumentów służących do ukrycia ich tożsamości. W obydwu systemach istnieje także możliwość oddelegowania funkcjonariuszy do innych służb lub instytucji. Obydwa organy mogą również korzystać ze współpracy osób trzecich, co ma istotne znaczenie dla infiltracji środowisk kryminalnych.

Najbardziej doniosłym instrumentem operacyjnym w polskim systemie prawnym jest kontrola operacyjna, uregulowana w art. 27 ustawy o ABW oraz AW. Jest ona przeprowadzana na pięć różnych sposobów, z których każdy ma swój odpowiednik w prawie niemieckim. Uzyskiwanie i utrwalanie treści rozmów prowadzonych przy użyciu środków technicznych, w tym za pomocą sieci telekomunikacyjnych, odpowiada niemieckiej kontroli telekomunikacji. Uzyskiwanie i utrwalanie obrazu lub dźwięku osób z pomieszczeń, środków transportu lub miejsc innych niż miejsca publiczne można porównać do znanej prawu niemieckiemu rejestracji dźwięku i obrazu w lokalach mieszkalnych. Kontrola operacyjna może również polegać na uzyskiwaniu i utrwalaniu treści koresponden-

cji, w tym korespondencji prowadzonej środkami komunikacji elektronicznej, a także uzyskiwaniu dostępu do przesyłek i kontroli ich zawartości. Ustawodawstwo niemieckie przewiduje kontrolę korespondencji pocztowej w ramach działalności wywiadowczej i w ramach procesu karnego, jednak nie lokuje tych uprawnień wśród przepisów policyjno-prawnych. Kontrola bieżącej korespondencji elektronicznej odbywa się w Niemczech na podstawie prawnej kontroli telekomunikacji. Poważnym wkroczeniem w prywatność – związanym z rozwoju techniki w XXI wieku – jest możliwość uzyskiwania i utrwalania danych zawartych w informatycznych nośnikach danych, telekomunikacyjnych urządzeniach końcowych, systemach informatycznych i teleinformatycznych. Tak zwane przeszukanie online jest znane także ustawie o BKA.

W przypadku prowadzenia quasi-kontroli operacyjnej na podstawie polskiej ustawy o działaniach terrorystycznych nie przewiduje się sądowej kontroli. Oczekuje się skonfrontowania tego rozwiązania legislacyjnego z zasadą państwa prawa przez Trybunał Konstytucyjny, gdyż jej brak może się wydawać co najmniej wątpliwy. Niemiecki ustawodawca we wszystkich przypadkach dotyczących kontroli operacyjnej przewiduje sądowe zarządzenie tych instrumentów, a także obwarowania co do zakazu pozyskiwania danych stanowiących trzon sfery życia prywatnego. Bez kontroli sądu odbywa się w Polsce także pozyskiwanie metadanych od dostawców usług telekomunikacyjnych. I w Niemczech, i w Polsce te dane można gromadzić na zapas, jednak polskie terminy (12 miesięcy) są znacznie dłuższe niż niemieckie (10 tygodni). Obowiązek zapisywania danych ciąży zarówno na polskich, jak i na niemieckich dostawcach usług.

Instrumenty przesyłki niejawnie nadzorowanej i transakcji pozornej nie są w ustawie niemieckiej wymienione expressis verbis. Ten pierwszy instrument ma w prawie niemieckim charakter wyłącznie transgraniczny, drugi natomiast jest znany jako jedna z czynności kryminalno-taktycznych. W polskiej literaturze przedmiotu podkreśla się ich bardziej procesowy, niż operacyjny charakter.

Na uwarunkowania polskich i niemieckich działań wypływają także różnice dotyczące koncepcji ochrony interesów osoby, wobec której stosuje się metody operacyjne. W prawie niemieckim ich punktem wyjścia jest obowiązek poinformowania osoby, której dotyczy działanie operacyjne, o jego przeprowadzeniu. Tyczy się to zarówno działań prewencyjnych i policyjnych, jak i (choć naturalnie w mniejszym stopniu) środków podejmowanych przez służby wywiadowcze[50]. Wyjątków od tej reguły jest wiele i prawdopodobnie w praktyce są one stosowane dużo częściej niż sama zasada. Jeśli chodzi o działania wywiadowcze, obowiązek ochrony interesów osób można spełnić, o ile nie występuje już zagrożenie, przeciwko któremu była skierowana ingerencja lub gdy można wykluczyć wystąpienie szkód dla dobra Federacji albo kraju związkowego. Istnieje również zasada nieudzielania informacji, jeżeli jest to sprzeczne z uzasadnioną ochroną interesów[51] osób trzecich lub samego poszkodowanego. Przepis § 20w BKAG wymienia natomiast poszczególne instrumenty operacyjne i określa, kto musi zostać powiadomiony o ich zastosowaniu, a wyjątki są podobne do tych wspomnianych powyżej. Gdy na podstawie uzyskanych wiadomości wszczęto postępowanie przygotowawcze, to prokuratura udziela informacji o zastosowanych metodach operacyjnych, opierając się na procesowokarnej podstawie prawnej (§ 20w ust. 2 zd. 2 BKAG). Jeżeli nie można udzielić informacji poszkodowanemu w ciągu 12 miesięcy, to o dalszym odroczeniu tej czynności decyduje sąd (§ 20w ust. 3 BKAG).

[50] Por. §§ 8d ust. 3, 9 ust. 3 nr 1, 15, 19 ust. 4 BVerfSchG, § 7 BNDG, § 20w BKAG.

[51] Niem. *schutzwürdiges Interesse*, czyli „interes godny ochrony".

W polskiej koncepcji czynności operacyjno-rozpoznawczych nie ma mowy o ich ujawnianiu osobom, których one dotyczą. Jest to konstytucyjnie wątpliwe, zgodnie bowiem z art. 51 ust. 4 Konstytucji RP, każdy ma prawo żądać sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą. Wyjątkiem jest instrument operacyjny z art. 34a ustawy o ABW oraz AW, jednak i tutaj znajduje się wyjątkowa możliwość odroczenia obowiązku poinformowania podmiotu, którego informacje dotyczą, ze względu na możliwość zaszkodzenia wynikom podjętych czynności operacyjno-rozpoznawczych (ust. 10). Brak informacji ze strony organów państwowych o zebranych danych powoduje praktyczną niemożliwość skorzystania przez konkretny podmiot z konstytucyjnego prawa. Charakter czynności operacyjno-rozpoznawczych z natury rzeczy uzasadnia ich tajność *ex ante*, a więc ich podejmowanie i prowadzenie bez wiedzy i zgody osoby im poddanej[52]. Do tej pory wystarczającym usprawiedliwieniem nieujawniania informacji o tego typu czynnościach było zapewnienie kontroli sprawowanej przez sądy, a także zachowanie granicy proporcjonalności i zasady subsydiarności. Gdy materiały operacyjne są wykorzystywane w postępowaniu karnym, to dołącza się je do akt sprawy. Można jednak objąć je klauzulą tajemnicy państwowej. Wątpliwe jest, na ile takie rozwiązania są zgodne ze współczesnymi zasadami ochrony praw jednostki.

Rozdział III. Metody operacyjne w procesie karnym

1. Określenie problemu

Wykorzystanie rezultatów pracy operacyjnej w procesie karnym jest związane z kilkoma problemami. Po pierwsze, większość niemieckich instrumentów prewencyjnych ma swoje odpowiedniki w kodeksie postępowania karnego. Relacje zachodzące między metodami operacyjnymi stosowanymi prewencyjnie i procesowo są zatem jaśniejsze, gdyż przepisów prawa administracyjnego (policyjnego) nie stosuje się do celów procesowych. Inny problem występuje w prawie polskim, w którym wykaz pokrewnych instrumentów nie zawsze ma odzwierciedlenie w kodeksie postępowania karnego. Po drugie, czynności operacyjno-rozpoznawcze są w Polsce podejmowane w czasie trwania procesu; należy się więc zastanowić nad dopuszczalnością i zasadami takiego postępowania. Po trzecie, należy przeanalizować sposób wykorzystywania wyników pracy operacyjnej do celów postępowania karnego. (…)

2. Czynności operacyjne a poszczególne czynności procesowe

2.1. Procesowe czynności operacyjne w prawie niemieckim

Niemiecki system bezpieczeństwa państwa charakteryzuje się swoistym trójpodziałem czynności o charakterze operacyjnym. W związku z zasadą rozdziału służb wywiadowczych i policji te pierwsze nie dysponują uprawnieniami wykonawczymi,

[52] Trybunał Konstytucyjny (TK), wyrok z 23 VI 2009 r., K 54/07, OTK 2009, z. 6A, poz. 86, s. 61; wyrok z 12 XII 2005 r., K 32/04, OTK 2005, z. 11A, poz. 132, s. 7; D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze*…, s. 132.

a podejmowane przez nie czynności są osobnym reżimem prawnym. Więcej podobieństw można natomiast zauważyć między policyjnymi czynnościami zapobiegawczymi a instrumentami zawartymi w kodeksie postępowania karnego. Właściwie wszystkie instrumenty operacyjne, którymi dysponuje policja w celu rozpoznawania przestępstw i zapobiegania im, znajdują swoje odpowiedniki w kodeksie postępowania karnego, dzięki czemu mogą zostać wykorzystane do celów wykrywczych i dowodowych służących ściganiu karnemu[53]. Zależności zachodzące między nimi zostały wymienione przy okazji opisu systemu bezpieczeństwa państwa w rozdziale I, 3.2.2. Toteż w tym miejscu należy się ograniczyć wyłącznie do wyszczególnienia przepisów będących odpowiednikami policyjnych metod operacyjnych, w kontekście wymienionych w rozdziale uprawnień dotyczących prewencji terrorystycznej prowadzonej przez BKA. Należą do nich: pozyskiwanie danych osobowych (§ 163d StPO), techniczne środki obserwacji (§ 100h StPO), obserwacja długotrwała (§ 163f StPO), specjalna obserwacja policyjna (§ 163e StPO), stosowanie środków technicznych poza mieszkaniem (§ 100f StPO), praca pod przykryciem (§§ 110a–110c StPO), rejestracja dźwięku w mieszkaniu (§§ 100c, 100d StPO), kontrola telekomunikacji (§§ 100a, 100b StPO), kontrola korespondencji (§§ 97, 99 i 100 StPO), pozyskiwanie metadanych (§ 100g StPO), identyfikacja urządzeń mobilnych (§ 100i StPO) oraz masowe porównywanie danych (§ 98a StPO). Działalność tajnych współpracowników w procesie wywodzi się z klauzuli generalnej, umożliwiającej podejmowanie czynności dochodzeniowych zgodnie z zasadą swobodnego kształtowania postępowania przygotowawczego (§ 161 ust. 1 zd. 1 w zw. z § 163 zd. 2 StPO)[54].

Wymienione instrumenty nie różnią się sposobem ich przeprowadzania od swoich policyjno-prawnych odpowiedników. Inny jest ich procesowy cel oraz inne obwarowania zasad postępowania przy ich stosowaniu. Wymagają one zawsze sądowego zarządzenia (z wyjątkiem przypadków niecierpiących zwłoki)[55]. Jak już wspomniano, metody zawarte w regulacjach policyjno-prawnych są ukierunkowane na zdarzenia przyszłe (odparcie niebezpieczeństw, zapobieżenie przestępstwom), ich odpowiedniki procesowe są natomiast ukierunkowane na zdarzenia przeszłe (wykrycie przestępstwa i ustalenie jego okoliczności).

Warto zauważyć, że dwa policyjne środki operacyjne zawarte w ustawie o Federalnym Urzędzie Kryminalnym – § 20h BKAG (w zakresie zastosowania środków wizualnych w mieszkaniu oraz § 20k BKAG (przeszukiwanie systemu informatycznego) nie mają analogicznych regulacji w ramach postępowania karnego[56]. Brak pierwszego środka jest podyktowany uwarunkowaniami konstytucyjnymi – zgodnie z art. 13 ust. 3 w zw. z ust. 4 GG, stosowanie optycznych środków technicznych w mieszkaniu jest dopuszczalne tylko w celach prewencyjnych, a nie procesowych[57]. Jeśli zaś chodzi o ingerencję w system IT, to w obecnym stanie prawnym nie przewiduje się procesowej możliwości dokonania tego rodzaju czynności bez wiedzy osoby, której ona dotyczy[58]. Pokrewną

[53] T. Bode, *Verdeckte Ermittlungsmaßnahmen in Deutschland und in Polen im Vergleich*, w: *Neue Tendenzen im Strafprozessrecht – Deutschland, Polen und die Ukraine*, F.-C. Schroeder, T. de Vries (red.), Frankfurt am Main 2015, s. 164.

[54] T. Bode, *Verdeckte strafprozessuale Ermittlungsmaßnahmen*, Heidelberg 2012, s. 443 i cytowana tam literatura.

[55] T. Bode, *Verdeckte Ermittlungsmaßnahmen in Deutschland*…, s. 163.

[56] W. Griesbaum, *Strafverfolgung zur Verhinderung terroristischer Anschläge – Eine Bestandsaufnahme*, „Neue Zeitschrift für Strafrecht" (NStZ) 2013, s. 376.

[57] H.-J. Papier, w: *GG*, T. Maunz, G. Dürig, art. 13, nb. 73.

[58] BGH, postanowienie z 31 I 2007 r., StB 18/06., BGHSt (BGHSt – *Entscheidungen des Bundesgerichts-*

instytucją procesową jest przepis zezwalający na przeszukanie elektronicznych danych umieszczonych na fizycznie oddzielnym medium mającym pamięć masową, np. na serwerze lub w tzw. chmurze, o ile brak podjęcia czynności grozi utratą danych lub środków dowodowych, zawarty w § 110 ust. 3 StPO. Jest to jednak czynność procesowa jawna. Jeśli dane znajdują się na serwerze w innym państwie, dla ich zabezpieczenia nie wyklucza się skorzystania z pomocy prawnej[59]. (…)

7. Możliwość wykorzystania rezultatów zagranicznej pracy operacyjnej w procesie

Uzyskiwanie dowodów za granicą oraz ich wykorzystywanie jest jednym z elementów współpracy w sprawach karnych[60]. Podczas gdy w Polsce pomoc prawna jest uregulowana w ramach kodyfikacji postępowania karnego (dział XIII kpk[61]), w Niemczech jest to przedmiot odrębnego aktu normatywnego. Zarówno Polska, jak i Niemcy są stronami Konwencji z 29 maja 2000 r. o pomocy prawnej w sprawach karnych pomiędzy państwami członkowskimi Unii Europejskiej[62].

Co do zasady materiał dowodowy pochodzący od organów państw obcych może zostać wykorzystany w polskim procesie karnym[63]. W przypadku dowodów zebranych operacyjnie, lecz służących celom procesowym (tj. na podstawie przepisów operacyjnych niemieckiego kodeksu postępowania karnego – por. podrozdział 2.1.), przeprowadzonych na wniosek polskiego organu ścigania, podstawą prawną będzie art. 587 kpk. Zgodnie z jego treścią protokoły czynności dowodowych przeprowadzonych przez sądy lub prokuratorów państw obcych albo przez organy działające pod ich nadzorem, sporządzone na wniosek polskiego sądu lub prokuratora, mogą być odczytywane na rozprawie na zasadach określonych w art. 389, 391 i 393 kpk, o ile sposób przeprowadzenia czynności nie jest sprzeczny z zasadami rodzimego porządku prawnego. Nadesłanie protokołów, zanim zostanie zawnioskowane przeprowadzenie czynności dowodowej, niekoniecznie pozbawia ich charakteru dowodu[64]. Muszą być natomiast spełnione gwarancje ochronne zawarte w art. 587 kpk[65]. W świetle tego przepisu sprzeczność sposobu przeprowadzenia czynności z porządkiem prawnym należy rozumieć nie tyle ściśle – formalnie i materialnie – ile jako ogólną zgodność czynności z tymi zasadami polskiego porządku, które w sposób fundamentalny kształtują model procesu[66]. Do takich zasad zalicza się m.in. zasady dotyczące bezwzględnych zakazów dowodowych lub metod zakazanych przez polskie prawo.

Według ocen prezentowanych w literaturze przedmiotu w podobny sposób należy traktować każdy inny dowód, a zatem również taki, który powstał przy realizacji innego celu (a więc też w przypadku instrumentów prewencyjno-policyjnych – chociażby na podstawie przepisów § 20a i nast. BKAG), o ile został przekazany na podstawie wnio-

hofs in Strafsachen – Zbiór orzecznictwa Federalnego Sądu Najwyższego w sprawach karnych), 51, 211.

[59] S. Hegmann, w: *Beck'scher Online-Kommentar StPO*, J.-P. Graf (red.), § 110, nb. 13 i nast.

[60] B. Nita-Światłowska, *Ograniczenia w wykorzystywaniu w postępowaniu karnym dowodów przeprowadzonych przez obce organy*, w: *Pozaprocesowe pozyskiwanie dowodów i ich wykorzystanie w procesie karnym*, P. Hofmański, D. Szumiło-Kulczycka, P. Czarnecki (red.), Warszawa 2015, s. 297.

[61] *Ustawa z dnia 6 czerwca 1997 r. – Kodeks postępowania karnego* (tekst jednolity: Dz.U. z 2016 r. poz. 1749).

[62] Dz.U. z 2007 r. Nr 135 poz. 950.

[63] A. Sakowicz i in., *Wykorzystywanie w procesie karnym dowodów pochodzących z czynności pozaprocesowych – raport polski*, w: *Pozaprocesowe pozyskiwanie dowodów i ich wykorzystanie*…, s. 570.

[64] Sąd Najwyższy, uchwała z 30 IX 1977 r., VII KZP 32/77, OSNKW 1977, Nr 10–11, poz. 113.

[65] B. Nita-Światłowska, *Ograniczenia w wykorzystywaniu w postępowaniu karnym*…, s. 298.

[66] A. Sakowicz i in., *Wykorzystywanie w procesie karnym dowodów*…, s. 574.

sku, o którym mowa w art. 587 kpk[67]. Trzeba również zwrócić uwagę na to, że dowody operacyjne uzyskane w Niemczech, a przekazane polskim organom ścigania, powinny być oceniane przez pryzmat przepisów niemieckich, gdyż są one zaliczane w polskim postępowaniu w poczet materiałów dowodowych na zasadach ogólnych, pod warunkiem niesprzeczności z zasadami polskiego porządku prawnego. Obrót informacjami uzyskanymi przez policję, które są przekazane bezpośrednio organom drugiego kraju, może się odbywać w sposób ułatwiony na podstawie art. 5 ust. 7 polsko-niemieckiej umowy o współpracy służb policyjnych[68] (szerzej o niej w rozdziale IV, podrozdz. 3). Jeśli organ przekazujący[69] udzielił zgody na przekazanie informacji, w tym danych osobowych, to mogą być one wykorzystane jako dowody w postępowaniu karnym, w ramach którego zostały przekazane[70].

Również w Niemczech co do zasady można wykorzystywać dowody uzyskane w innym państwie w ramach postępowania karnego[71]. Ustawa o pomocy prawnej w sprawach karnych[72] jest aktem normatywnym przenoszącym różnego rodzaju przepisy z innych konwencji do celów prawa niemieckiego. Podobnie jak w regulacji polskiej na dopuszczalność dowodów zdobytych operacyjnie patrzy się przez pryzmat kraju, w którym dowód został uzyskany, a nie przez pryzmat niemieckiego prawa karnego procesowego. Jeśli dowód został uzyskany zgodnie z procedurami kraju, do którego się zwrócono z wnioskiem, to sąd z reguły zezwala na jego wykorzystanie[73]. Konieczne jest zwrócenie się do państwa trzeciego z wnioskiem o uzyskanie dowodu, przy czym jest on dopuszczalny, jeśli jego uzyskanie w taki sposób byłoby dopuszczalne w prawie krajowym[74]. W niemieckim postępowaniu karnym zdobywanie dowodów niezgodne z prawem (niem. *Beweiserhebung*) niekoniecznie musi prowadzić do zakazu ich wykorzystania (niem. *Beweisverwertungsverbot*). Sąd stwierdza, czy podczas uzyskiwania dowodu zostały naruszone podstawowe zasady niemieckiego porządku prawnego, a jeśli tak, to w jakim stopniu, a następnie podejmuje decyzję co do wykorzystania takiego dowodu. Na podstawie § 72 IRG (*Gesetz über internationale Rechtshilfe in Strafsachen* – niemiecka ustawa o międzynarodowej pomocy w sprawach karnych) jest możliwa zmiana celu wykorzystania dowodu, jeżeli nie pozostaje to w sprzeczności z przepisami prawa kraju, w którym został on zdobyty.

Niezależnie od przepisów dotyczących pomocy prawnej w relacjach pomiędzy państwami członkowskimi Unii Europejskiej, a więc także polsko-niemieckich, będzie możliwe skorzystanie z instrumentu europejskiego nakazu dochodzeniowego, który umożliwia wezwanie do przeprowadzenia w państwie wykonującym jednej lub więcej czynności dochodzeniowych, które służą gromadzeniu materiału dowodowego (motyw

[67] Tamże, s. 572.

[68] *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Federalnej Niemiec o współpracy służb policyjnych, granicznych i celnych, sporządzona w Zgorzelcu dnia 15 maja 2014 r.* (Dz.U. z 2015 r. poz. 939).

[69] Na przykład *Bundeskriminalamt* na podstawie § 14a BKAG.

[70] Deutscher Bundestag, 18. Wahlperiode, *Entwurf eines Gesetzes zu dem Abkommen vom 15. Mai 2014 zwischen der Regierung der Bundesrepublik Deutschland und der Regierung der Republik Polen über die Zusammenarbeit der Polizei-, Grenz- und Zollbehörden*, 7 I 2015 r., BT-Drs 18/3696, s. 32.

[71] L. Wörner, A. Sinn, M. Wörner, *Landesbericht Deutschland (Fragenkatalog)*, w: *Pozaprocesowe pozyskiwanie dowodów i ich wykorzystanie*…, s. 455.

[72] Ustawa o międzynarodowej pomocy prawnej w sprawach karnych (*Gesetz über die internationale Rechtshilfe in Strafsachen*) z 23 XII 1982 r. (BGBl. I S. 1537, ze zm.).

[73] L. Wörner, A. Sinn, M. Wörner, *Landesbericht Deutschland*…, s. 172.

[74] Tamże, s. 456.

7 dyrektywy 2014/41/UE[75]). To wezwanie może obejmować również pozyskanie istniejącego i przyszłego materiału dowodowego[76]. Natomiast nie stosuje się tego instrumentu wobec czynności podejmowanych w ramach obserwacji transgranicznej oraz podejmowanych przez zespoły dochodzeniowo-śledcze[77]. Europejski nakaz dochodzeniowy powinien zastąpić istniejący do tej pory europejski nakaz dowodowy w przepisach krajowych najpóźniej do 22 maja 2017 r. (art. 36 dyrektywy 2014/41/UE)[78]. Ma on mieć wymiar horyzontalny i powinien dotyczyć (…) *wszystkich czynności dochodzeniowych mających na celu gromadzenie materiału dowodowego*[79].

Wykładnia terminu c z y n n o ś ć d o c h o d z e n i o w a jest problematyczna w świetle różnic w procedurach karnych poszczególnych państw. Gdyby rozumeć ten termin przez pryzmat uzyskania dowodu, niektóre polskie czynności operacyjno-rozpoznawcze mogłyby mieć charakter dochodzeniowy, zważywszy na to, że ich ustawowym celem jest również ściganie sprawców i uzyskiwanie dowodów. Na takie rozumowanie wskazuje treść dyrektywy. W motywie 10 preambuły wskazano, iż (…) *organ wydający najlepiej potrafi ocenić, na bazie swojej wiedzy o szczegółach danego dochodzenia, jaką czynność dochodzeniową należy wykonać. Jednak gdy tylko jest to możliwe, organ wykonujący powinien wykonać inny rodzaj czynności dochodzeniowej, jeżeli wskazana czynność nie istnieje w jego prawie krajowym lub nie byłaby dopuszczalna w podobnej sprawie krajowej*. W kontekście niektórych metod operacyjnych, takich jak uzyskiwanie informacji bankowych, przesyłka niejawnie nadzorowana bądź dochodzenie prowadzone przez funkcjonariuszy pod fałszywą tożsamością, ustawodawca unijny zauważa, że mogą one być objęte europejskim nakazem dochodzeniowym, co nie wyklucza potrzeby powstania szczególnych ustaleń między współpracującymi państwami[80]. Motywy 30 i nast. dyrektywy 2014/41/UE odnoszą się do przechwytywania przekazów telekomunikacyjnych oraz metadanych. Zgodnie z art. 2 ust. 3 dyrektywy organem wydającym europejski nakaz dochodzeniowy może być nie tylko sąd czy prokurator, lecz także (…) *każdy inny właściwy organ określony przez państwo wydające i w danym przypadku wypełniający swoją funkcję organu dochodzeniowego*[81]. Wyobrażalne jest więc wystawienie nakazu przez instytucję policyjną[82]. (…)

---

[75] *Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego w sprawach karnych* (Dz.Urz. UE L 130 z 1 V 2014 r. poz. 1).

[76] Tylko do istniejącego materiału był ograniczony instrument europejskiego nakazu dowodowego na podstawie decyzji ramowej Rady UE Nr 2008/978/WSiSW z 18 XII 2008 r., uchylony rozporządzeniem Parlamentu Europejskiego i Rady 2016/95/UE z 20 I 2016 r.; zgodnie z art. 2 rozporządzenia 2016/95 wszelkie europejskie nakazy dowodowe wykonywane na mocy decyzji ramowej 2008/978/WSiSW w dalszym ciągu podlegają przepisom tej decyzji do czasu, aż stosowne postępowanie karne zakończy się wydaniem prawomocnego rozstrzygnięcia.

[77] M. Andrzejewska, *Wykorzystywanie dowodów pozyskanych za granicą – sprawozdanie z dyskusji*, w: *Pozaprocesowe pozyskiwanie dowodów i ich wykorzystanie*…, s. 167.

[78] Na brak możliwości bezpośredniego stosowania przepisów dyrektywy w postępowaniu karnym przed upływem tego terminu wskazuje T. Bode, *Verdeckte Ermittlungsmaßnahmen in Deutschland und in Polen im Vergleich*, w: *Neue Tendenzen im Strafprozessrecht – Deutschland, Polen und die Ukraine*, F.-C. Schroeder, T. de Vries (red.), Frankfurt am Main 2015, s. 179.

[79] *Dyrektywa Parlamentu Europejskiego i Rady nr 2014/41/UE z dnia 3 kwietnia 2014 r. w sprawie europejskiego nakazu dochodzeniowego*…, motyw 8.

[80] Tamże, motyw 24.

[81] B. Nita-Światłowska, *Wykorzystywanie dowodów pozyskanych za granicą*, w: *Pozaprocesowe pozyskiwanie dowodów i ich wykorzystanie*…, s. 287.

[82] H. Ahlbrecht*, Die Europäische Ermittlungsanordnung – oder: EU-Durchsuchung leicht gemacht*, StV 2013, s. 116.

Rozdział IV. Metody operacyjne w kontekście polsko-niemieckiej współpracy i członkostwa w Unii Europejskiej

3. Umowa o współpracy służb policyjnych, granicznych i celnych – nowa podstawa współpracy

Umowa o współpracy służb policyjnych, granicznych i celnych[83] podpisana 15 maja 2014 r., która weszła w życie 9 lipca 2015 r., zastąpiła m.in. wcześniejsze regulacje z roku 2002[84]. Ten nowy dokument jest ważnym elementem polsko-niemieckiej współpracy policyjnej, która od dawna jest intensywna i ma szczególne znaczenie zwłaszcza dla terenów przygranicznych – w związku ze zwalczaniem lokalnej przestępczości. Strategiczną wartość ma powstałe w 2007 r. Polsko-Niemieckie Centrum Współpracy Służb Granicznych, Policyjnych i Celnych w Świecku, w którym przedstawiciele wielu lokalnych instytucji policyjnych obydwu państw koordynują działania w zakresie obserwacji przygranicznych zagrożeń. Umowa wprowadza także podstawy prawne i konkretne instrumenty współpracy instytucji centralnych, co jest istotne w odniesieniu do zagrożeń ponadlokalnych, do których należy terroryzm międzynarodowy. Dzięki nowym przepisom funkcjonariusze poruszają się w jednoznacznym reżimie prawnym, korzystając z kompetencji na podstawie ustaw państwa sąsiedzkiego.

W art. 1 omawianej umowy jej strony zobowiązują się do współpracy w zapobieganiu, wykrywaniu, zwalczaniu i ściganiu przestępstw oraz do współdziałania w zapobieganiu i przeciwdziałaniu zagrożeniom bezpieczeństwa i porządku publicznego. Wśród organów centralnych można znaleźć zarówno Federalny Urząd Kryminalny, jak i Szefa ABW (art. 2 ust. 2 umowy). Mogą one współpracować ze sobą bezpośrednio (art. 4 ust. 1 umowy), a współpraca ta odbywa się na podstawie wniosków przekazywanych zgodnie z właściwością. Szczególną formą wspólnego działania jest klauzula dotycząca zapobiegania i zwalczania terroryzmu zawarta w art. 19. Umieszczenie jej w wykazie form szczególnych jest niefortunne, gdyż przepis ten nie precyzuje konkretnych metod, a jedynie wskazuje na to, iż właściwe organy realizują, zgodnie z prawem wewnętrznym, uzgodnione czynności, jeżeli wymaga tego zapobieganie i zwalczanie terroryzmu. Właściwe organy mogą powołać stałe lub na czas określony punkty współpracy funkcjonariuszy lub pracowników (art. 28), wymieniać oficerów łącznikowych (art. 11) i podporządkowywać swoich funkcjonariuszy lub pracowników, co wiąże się z realizowaniem uprawnień władczych pod kierownictwem (art. 13). Umowa przewiduje również pogłębianie współpracy m.in. przez sporządzanie wspólnych raportów sytuacyjnych, tworzenie wspólnych stanowisk dowodzenia, zespołów zadaniowych oraz planowanie i realizowanie wspólnych programów zapobiegania przestępczości (art. 14). W ramach współpracy naukowo-technicznej w umowie przewidziano m.in. udostępnianie specjalistycznego sprzętu i pomieszczeń służbowych.

---

[83] *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Federalnej Niemiec o współpracy służb policyjnych…*

[84] *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Federalnej Niemiec o współpracy policji i straży granicznych na terenach przygranicznych, podpisana w Berlinie dnia 18 lutego 2002 r.* (Dz.U. z 2005 r. Nr 223 poz. 1915) oraz *Umowa między Rządem Rzeczypospolitej Polskiej a Rządem Republiki Federalnej Niemiec o współpracy w zakresie zwalczania przestępczości zorganizowanej oraz szczególnie niebezpiecznych przestępstw, podpisana we Wrocławiu dnia 18 czerwca 2002* r. (Dz.U. z 2004 r. Nr 248 poz. 2486).

3.1. Wymiana informacji o zagrożeniach terroryzmem

Jak wspomniano wcześniej, właściwe organy Polski i Niemiec realizują uzgodnione czynności w celu zapobiegania i zwalczania terroryzmu. Na podstawie art. 6 ust. 1 pkt 10 umowy z 15 maja 2014 r. te organy mogą wymieniać informacje o planowanych i popełnionych zamachach terrorystycznych, metodach i technikach działania sprawców tych zamachów lub osób podejrzanych o ich popełnienie oraz o ugrupowaniach terrorystycznych planujących popełnienie przestępstwa o charakterze terrorystycznym. Przekazywanie informacji przez właściwe organy może odbywać się z własnej inicjatywy, zgodnie z prawem wewnętrznym. Wykaz informacji zawarty w art. 6 stanowi, iż mogą one dotyczyć m.in.:

- sprawców przestępstw lub osób podejrzanych uczestniczących w popełnieniu przestępstwa;
- istotnych okoliczności, podjętych czynności, powiązań między sprawcami, struktur, organizacji oraz metod działania zorganizowanych grup, typowych wzorców zachowań;
- właścicieli środków transportu, posiadaczy tych środków i osób nimi kierujących, a także danych i dokumentów identyfikujących środki transportu i uprawnienia do ich prowadzenia;
- ustalenia adresu zamieszkania, miejsca pobytu i statusu pobytu oraz wyników kontroli legalności pobytu;
- abonentów i użytkowników sieci telekomunikacyjnych i teleinformatycznych, danych z systemów informacyjnych, rejestrów i innych zbiorów danych;
- rozpytywania osób, sprawdzenia i ustalenia tożsamości osób, planowania, przygotowywania i przeprowadzania czynności poszukiwawczych, oględzin, zabezpieczania i dokumentacji śladów;
- szlaków i skali nielegalnej migracji oraz zjawisk migracyjnych; identyfikacji rzeczy, szczególnie broni, amunicji i materiałów wybuchowych, ich właścicieli lub posiadaczy oraz próbek materiałów wybuchowych i innych materiałów niebezpiecznych.

Ta regulacja nie wyczerpuje wszystkich możliwości i dotyczy współpracy policyjnej, a porozumienia odnoszące się do wspólnego działania w zakresie ścigania karnego pozostają nienaruszone[85].

3.2. Grupy operacyjno-śledcze

W polsko-niemieckiej umowie o współpracy przewidziano interesującą możliwość utworzenia grup operacyjno-śledczych (niem. *operative Ermittlungsgruppen*). Już samo nazewnictwo zwraca uwagę na nietypowy charakter grupy, którą należy odróżnić od ugruntowanego na podstawie prawa europejskiego wspólnego zespołu śledczego (niem. *gemeinsame Ermittlungsgruppe*)[86], uregulowanego w art. 589b i nast. KPK oraz § 93 IRG, który może podejmować działania dopiero na etapie postępowania przygotowawczego[87]. Grupa operacyjno-śledcza, którą utworzono na podstawie art. 12 umowy

[85] Deutscher Bundestag, 18. Wahlperiode, *Entwurf*..., BT-Drs 18/3696, s. 32.

[86] Ustanowione na podstawie *Decyzji ramowej Rady z dnia 13 czerwca 2002 r. w sprawie wspólnych zespołów dochodzeniowo-śledczych (2002/465/WSiSW)* (Dz.Urz. UE L 162 z 20 VI 2002 r. poz. 1).

[87] A. Górski, *Europejskie ściganie karne. Zagadnienia ustrojowe*, Warszawa 2010, s. 62, wskazuje na po-

o współpracy, umożliwia (…) *ścisłe współdziałanie w celu zapobiegania, wykrywania lub zwalczania przestępstw, w szczególności przestępstw popełnianych przez zorganizowane grupy*. Dopuszczalne wydaje się utworzenie grupy, która ma podejmować czynności prewencyjno-zapobiegawcze, a więc również operacyjno-rozpoznawcze. Takie rozumowanie wynika jednak bardziej z treści umowy sporządzonej w języku polskim, w której wskazano na (…) *równoległe prowadzenie czynności* (art. 12 ust. 1) oraz (…) *przeprowadzanie odpowiednich czynności* (art. 12 ust. 3 pkt 1). W niemieckojęzycznej wersji umowy posłużono się sformułowaniem „*Ermittlungen*" lub „*Ermittlungshandlungen*", co mogłoby wskazywać na ich charakter dochodzeniowo-śledczy, a nie operacyjno-rozpoznawczy. Jednak w świetle tytułu przepisu oraz wyraźnie wymienionych celów prewencyjnych (zapobieganie, zwalczanie; *Verhütung, Bekämpfung*), należy uznać, iż grupa operacyjno-śledcza może, w przeciwieństwie do wyżej wspomnianego instrumentu prawa wspólnotowego, podejmować czynności o charakterze operacyjno-rozpoznawczym. Taką wykładnię potwierdza uzasadnienie projektu ustawy transponującej umowę do niemieckiego ustawodawstwa, które wyraźnie wskazuje na to, że grupy operacyjne nie obejmują wspólnych zespołów śledczych kierowanych przez prokuraturę[88]. Termin „*Ermittlungen*" bywa używany przez niemieckiego ustawodawcę również w kontekście działań prewencyjnych (np. § 161 ust. 3 StPO – (…) *nicht offene Ermittlungen auf polizeirechtlicher Grundlage*). (…)

Uwagi końcowe

Podejmowanie tajnych czynności w stosunku do jednostek zagrażających bezpieczeństwu państwa zawsze będzie tematem kontrowersyjnym. Z jednej strony, aby zapewnić ochronę państwu, a jego obywatelom – bezpieczeństwo, policja oraz służby specjalne muszą dysponować skutecznymi mechanizmami pozwalającymi odgrywać im swoją rolę. Z drugiej jednak strony między uprawnieniami służb a wolnościami obywatelskimi zawsze będzie zachodziła rozbieżność. Bezpieczeństwo ma swoją cenę – jest nią ograniczenie swobód obywatelskich. Zadaniem ustawodawcy jest skonstruowanie takiego prawa, które w jak największym stopniu umożliwia zapobieganie różnego rodzaju zagrożeniom oraz ściganie sprawców przestępstw i jednocześnie w jak najmniejszym stopniu zezwala na wkraczanie w sferę prywatności obywateli.

Wykorzystanie owoców operacyjnej pracy służb w ramach postępowania karnego powoduje powstanie kolejnych problemów. Dokonuje się bowiem przemieszanie dwóch obszarów, w których państwo jest zobligowane do podejmowania działań – zapobiegania zagrożeniom oraz działalności karno-represyjnej. Nie są to oczywiście obszary całkowicie odległe. W tym kontekście warto choćby wspomnieć o definicji operacji wywiadowczej w świetle jednej z unijnych decyzji ramowych, która jest określana jako (…) *stadium postępowania, które nie jest jeszcze na etapie dochodzenia karnego, w którym właściwy organ ścigania jest upoważniony na mocy prawa krajowego do gromadzenia, przetwarzania i analizowania informacji o przestępstwach lub działalności przestępczej w celu ustalenia, czy konkretne przestępstwa zostały popełnione lub mogą zostać popełnione*[89]. Znamienne jest zestawienie

---

cząstkowo sporny charakter czynności tych zespołów.

[88] Deutscher Bundestag, 18. Wahlperiode, *Entwurf...*, BT-Drs 18/3696, s. 34.

[89] Art. 2 lit. c *Decyzji ramowej Rady 2006/960/WSiSW z dnia 18 grudnia 2006 r. w sprawie uproszczenia*

w niej kompetencji organów ścigania zbierających dane o przyszłych, negatywnych wydarzeniach, zarówno aby im zapobiec, jak i aby ścigać ich sprawców, z uprawnieniami informacyjnymi.

Polskie i niemieckie prawo dostrzega te dwie odrębne role, jednak tylko system niemiecki dokonuje odpowiedniego rozróżnienia w ustawodawstwie na podstawie celu danej czynności. Jest to związane z zasadą federalizmu, której jednym z elementów jest odpowiedzialność federacji za ściganie karne. Natomiast w gestii krajów związkowych leży policyjna działalność prewencyjna. Walka z terroryzmem wymaga maksymalnego wykorzystania dostępnych uprawnień państwa w świetle konstytucji. Metody operacyjne można umieścić w prawie niemieckim w dwóch reżimach. Prawo administracyjne zawiera normy kompetencyjne, które ustanawiają uprawnienia informacyjne służb wywiadowczych, oraz zapobiegawcze instrumenty operacyjne stosowane przez policję. Te instrumenty mają charakter zarówno informacyjny, jak i wykonawczy. Prawo karne procesowe obejmuje instrumenty pokrewne do policyjnych, które są stosowane zgodnie z represyjnymi aspektami procesu i są obarczone bardziej rygorystycznymi kryteriami. Z kolei system polski charakteryzuje się obecnością czynności operacyjno-rozpoznawczych, które mają charakter wywiadowczy, policyjno-prewencyjny, a często również procesowy. Charakter danej czynności zależy od momentu, w którym jest ona podejmowana, a często także od instytucji, która ją podejmuje. Z punktu widzenia systematyki prawa jest to rozwiązanie bardzo chaotyczne.

Mimo to, przewidziane rozwiązania prawne muszą być konsekwentne i możliwe do zrealizowania w praktyce. Zasadny jest argument, iż w ramach działalności prewencyjnej służby powinny mieć szersze uprawnienia, pod warunkiem, że wykorzystanie w procesie rezultatów tych czynności będzie podlegać ostrzejszym rygorom. Faktyczne uprawnienia służb polskich i niemieckich są jednak porównywalne, a w wielu aspektach praktycznie identyczne. Jeśli chodzi o rozwiązania prawne, wydaje się, że służby obydwu państw dysponują rozwiązaniami umożliwiającymi im skuteczne zwalczanie zagrożeń terrorystycznych. Rzeczywista zdolność przeciwdziałania terroryzmowi jest oparta nie tylko na rozwiązaniach legislacyjnych, lecz także przede wszystkim na jakości zaplecza operacyjnego, metodach szkoleniowych, wprowadzaniu innowacji technologicznych, zdolnościach analitycznych i umiejętnościach personelu. Strategiczne znaczenie ma współpraca międzyinstytucjonalna i międzynarodowa, a także polityka informacyjna[90].

Ustawodawstwo w obydwu państwach stoi jeszcze przed wieloma wyzwaniami. Ustawodawstwo niemieckie jest bardzo dojrzałe, a kultura ochrony danych osobowych i prywatności jest wysoka. To zjawisko prowadzi do wyśrubowanych standardów ustawodawczych odnoszących się do przepisów, które dotyczą kompetencji państwa do wkraczania w prawa jednostki. Przepisy odnośnie do służb wywiadowczych, ustawa o Federalnym Urzędzie Kryminalnym oraz kodeks postępowania karnego w części dotyczącej podejmowania tajnych czynności procesowych są zredagowane z niespotykaną w Polsce dokładnością i skrupulatnością. Ale jest to zjawisko zarówno pozytywne, jak i negatywne. Należy pochwalić regulacje niemieckie

wymiany informacji i danych wywiadowczych między organami ścigania państw członkowskich Unii Europejskiej (Dz.Urz. UE L 386 z 29 XII 2006 r. poz. 89).

[90] W. Griesbaum, *Strafverfolgung zur Verhinderung terroristischer Anschläge – Eine Bestandsaufnahme*, NStZ 2013, s. 378.

za ich precyzję i szeroki zakres, co jest gwarancją przestrzegania prawa. Przepisy niemieckie charakteryzują się rozbudowanymi, wielokrotnie złożonymi zdaniami, a poszczególne normy składają się z wielu jednostek redakcyjnych usiłujących uregulować wiele możliwych scenariuszy. Jeśli chodzi o metody operacyjne, które w czasach rozwoju informatycznego są oparte na coraz nowszych rozwiązaniach technicznych, istnieje ryzyko, że prawo nie będzie nadążać za zmianami technologicznymi. Warto więc postulować stanowienie zwięzłego, ponadczasowego prawa, które będzie obowiązywało przez wiele pokoleń.

Mimo że przepisy niemieckie są w porównaniu do polskich nadzwyczaj szczegółowe i wydają się w sposób bardzo rygorystyczny chronić prawa jednostki, to jednak wiele wyroków Federalnego Trybunału Konstytucyjnego doprowadziło do uznania ich za niezgodne z konstytucyjnymi standardami. Kolejna poważna reforma powinna zostać przeprowadzona do połowy 2018 r., gdy wiele uprawnień Federalnego Urzędu Kryminalnego utraci moc. Wyroki BVerfG są w niemieckiej kulturze prawnej szanowane. Federalny minister spraw wewnętrznych Thomas de Maizière stwierdził, że nie podziela zdania trybunału dotyczącego uprawnień BKA, gdyż wyrok ten utrudnia walkę z międzynarodowym terroryzmem, natomiast mimo wszystko (…) *należy z nim żyć, uszanować go oraz zaimplementować jego postanowienia*[91]. Niewykluczone, iż wkrótce zostaną podjęte reformy dotyczące uprawnień służb wywiadowczych – przede wszystkim BND i BfV.

Zarówno w polskim, jak i niemieckim systemie prawnym pojawiły się tzw. ustawy antyterrorystyczne. Występujące w nich problemy są jednak różnej natury. Nie można było spodziewać się, że ustawa o działaniach antyterrorystycznych spowoduje gruntowną przebudowę systemu bezpieczeństwa państwa. Ułatwia ona co prawda koordynowanie zadań w przypadku zdarzeń terrorystycznych i nieznacznie rozszerza istniejące kompetencje służb, ale nie wprowadza rewolucji w systemie bezpieczeństwa państwa. Postulat wprowadzenia ustawy o czynnościach operacyjno-rozpoznawczych pojawiający się w polskiej literaturze jest dalej aktualny i wstępnie można go uznać za zasadny[92]. Nie powinien się on jednak ograniczać wyłącznie do utworzenia wykazu czynności i regulacji dotyczących ich podejmowania, a kompleksowo zmodyfikować pojmowanie czynności procesowych i przedprocesowych ze względu na ich cel oraz jasno ustanowić zasady dotyczące wykorzystania ich rezultatów w toku postępowania karnego – z uwzględnieniem standardów konstytucyjnych.

Problem faktycznego zagrożenia terrorystycznego jest zagadnieniem bardzo dynamicznym. Do tej pory zwracano uwagę na to, że Polska pozostaje poza zainteresowaniem islamskich ekstremistów. W kontekście kryzysu migracyjnego w Europie, udziału Polski w misjach na Bliskim Wschodzie oraz zaangażowania militarnego w ramach NATO czy np. udostępniania infrastruktury dla tajnych więzień CIA[93] zmiana zainteresowania terrorystów może nastąpić z dnia na dzień. Niemcy dostrzegają nie tylko potrzebę utrzymania stanu obecnego, lecz także dalszego rozbudowywania międzynarodowej współpracy antyterrorystycznej[94]. Mimo że sposób uregulowania in-

[91] Redaktion beck-aktuell, *Reaktionen auf BKA-Urteil des BVerfG*, z 20 IV 2016 r., becklink 2003049, https://beck-online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2003049.htm [dostęp: 4 VII 2016].

[92] P. Czarnecki, *Czynności operacyjne u wrót procesu. Garść refleksji*, w: *Pozaprocesowe pozyskiwanie dowodów i ich wykorzystanie*…, s. 187.

[93] D. Szlachter, *Walka z terroryzmem w Unii Europejskiej – nowy impuls*, Toruń 2007, s. 221.

[94] Redaktion beck-aktuell, *Reaktionen*... [online], z 20 kwietnia 2016 r., becklink 2003049, https://beck-

strumentów operacyjnych jest w wielu wypadkach daleki od idealnego, trzeba mieć świadomość kompromisu między skutecznością a transparentnością działań służb specjalnych. Należy też mieć przy tym nadzieję, że dalsze kroki legislacyjne związane z regulowaniem przeprowadzania przez służby tajnych czynności doprowadzą do wzmożonego poczucia bezpieczeństwa wszystkich obywateli i do osłabienia obaw co do utraty prywatności. Ujęcie tego tematu w ramy prawne, a także kontrola organów wykonawczych, spoczywają w rękach sądownictwa oraz demokratycznie wybranych przedstawicieli władzy. Zwalczanie terroryzmu w sposób odpowiadający wysokim standardom państwa prawa jest trudne do pogodzenia ze współczesnymi, często niedającymi się okiełznać zagrożeniami, w których nasi przeciwnicy nie postępują fair. Jest to z pewnością wyzwanie dla cywilizacji łacińskiej i jej prawnej tradycji. Mówi się jednak, że nic tak nie jednoczy, jak wspólny wróg. Być może zjawisko terroryzmu spowoduje, że państwa narodowe, zjednoczone bardziej niż kiedykolwiek, wypracują wspólne mechanizmy w celu zapewnienia globalnego bezpieczeństwa, a przede wszystkim będą przedkładać współpracę w zakresie bezpieczeństwa międzynarodowego ponad interesy własne.

online.beck.de/Dokument?vpath=bibdata%2Freddok%2Fbecklink%2F2003049.htm [dostęp: 4 VII 2016].

Jakub Sałek

Nielegalność czynności operacyjno-rozpoznawczych a możliwość ich procesowego wykorzystania w postępowaniu dowodowym[1]

Ocena aktualnego stanu prawnego dotyczącego służb specjalnych musi być rygorystyczna ze względu na głęboką ingerencję w prawa oraz wolności człowieka i obywatela. Do tej ingerencji dochodzi podczas stosowania czynności operacyjno-rozpoznawczych. Na szczególną uwagę zasługuje tu weryfikacja tych aspektów działań operacyjnych, które z różnych powodów mogą tracić walor legalności. To jest, zdaniem autora, krytyczny punkt w czasie stosowania czynności operacyjnych, mający duże znaczenie w kontekście późniejszego wprowadzania dokumentów pochodzących z tych działań w poczet materiału dowodowego. Proces karny, wyposażony w wiele mechanizmów umożliwiających weryfikację legalności dowodu, zawiera również mechanizmy warunkujące dopuszczalność wykorzystania materiałów w czasie postępowania. Dlatego też obszar, na którym działania operacyjne stykają się z procesem karnym, będzie głównym tematem poniższej analizy.

Czynności operacyjno-rozpoznawcze na gruncie ustawodawstwa polskiego

Żadna z ustaw normujących działalność służb specjalnych nie zawiera definicji czynności operacyjno-rozpoznawczych. Aby je scharakteryzować, należy odnieść się do dorobku doktryny. Jedną z pierwszych definicji przedstawił Leon Schaff, według którego (…) *czynności operacyjne są to pozaprocesowe techniczne i taktyczne czynności wykształcone przez praktykę organów ścigania karnego, służące profilaktycznej walce z przestępczością*[2]. Na gruncie kryminalistyki czynności operacyjno-rozpoznawcze określa się jako ogół tajnych (bądź poufnych) pozaprocesowych działań organów ścigania zmierzających bądź do zdobycia informacji na potrzeby procesu (toczącego się lub przyszłego), bądź też do uniemożliwienia popełnienia przygotowanego przestępstwa[3]. Są również autorzy, którzy wzbraniają się od jednoznacznej definicji czynności operacyjnych. Stanisław Waltoś uważa, że w pojęciu czynności operacyjne kryje się zbyt wiele niewiadomych, które nie pozwalają na jednoznaczne zdefiniowanie owych działań[4]. Dobrosława Szumiło-Kulczycka natomiast, dokonując szerokiego oglądu działań służb na podstawie poszczególnych ustaw policyjnych, konkluduje, że skonstruowanie jednoznacznej definicji jest bezcelowe. Skłania się ku analizie celów, jakim służą owe czynności, szczególnie w zakresie możliwości pozyskiwania informacji przez służby[5]. Warto również przytoczyć szeroką definicję zaproponowaną przez Pawła Czarneckiego, który za czynności operacyjno-rozpoznawcze uznaje:

[1] Fragmenty pracy magisterskiej pt. *Nielegalność czynności operacyjno-rozpoznawczych a możliwość ich procesowego wykorzystania w postępowaniu dowodowym*, która zajęła II miejsce w konkursie Szefa ABW na najlepszą pracę magisterską/licencjacką z dziedziny bezpieczeństwa wewnętrznego (edycja 2015/2016). Redakcja dokonała niezbędnych poprawek oraz zmian numeracji przypisów (przyp. red.).

[2] L. Schaff, *Zakres i formy postępowania przygotowawczego*, Warszawa 1961, s. 77.

[3] Pisze o tym J. Widacki w: *Kryminalistyka*, *cz. I*, J. Widacki (red.), Katowice 1984, s. 127 i nast.

[4] S. Waltoś, *Model postępowania przygotowawczego na tle porównawczym*, Warszawa 1968, s. 146.

[5] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje do procesu karnego*, Warszawa 2012, s. 108–111.

> (…) ogół niejawnych działań upoważnionych ustawowo, wyspecjalizowanych służb i organów państwowych, których celem jest: jak najbardziej sprawne wykrywanie negatywnych zjawisk godzących w porządek publiczny i bezpieczeństwo powszechne, rozpoznawanie grup i środowisk przestępczych, ustalanie źródeł dowodowych, zabezpieczanie środków dowodowych i przeprowadzanie dowodów, które mogą zostać wykorzystane w procesie karnym, pozyskiwanie podmiotów współpracujących z organami ścigania oraz ujawnienie okoliczności sprzyjających popełnieniu zachowań nieakceptowanych społecznie[6].

Zgodnie z obowiązującym prawem czynności operacyjno-rozpoznawcze mogą przeprowadzać następujące służby: Policja – na podstawie *Ustawy z dnia 6 kwietnia 1990 r. o Policji*[7], Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu – na podstawie *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*[8], Centralne Biuro Antykorupcyjne – na podstawie *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym*[9], Wywiad Skarbowy – na podstawie *Ustawy z dnia 28 września 1991 r. o kontroli skarbowej*[10], Służba Kontrwywiadu Wojskowego i Służba Wywiadu Wojskowego – na podstawie *Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*[11], Straż Graniczna – na podstawie *Ustawy z dnia 12 października 1990 r. o Straży Granicznej*[12], Żandarmeria Wojskowa – na podstawie *Ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*[13] oraz Służba Celna – na podstawie *Ustawy z dnia 27 sierpnia 2009 r. o Służbie Celnej*[14].

Powyższym organom ustawodawca nadał wiele uprawnień służących do realizacji ich ustawowych celów, a zwłaszcza do wykrywania przestępstw i im zapobiegania. Do czynności operacyjno-rozpoznawczych zalicza się kontrolę operacyjną, transakcję pozorną, przesyłkę niejawnie nadzorowaną, uprawnienie do pozyskiwania danych telekomunikacyjnych przez niejawne pozyskiwanie danych od operatorów usług, od lutego 2016 r. – także pozyskiwanie danych elektronicznych, uprawnienie do pozyskiwania danych pocztowych, instytucję tajnego współpracownika, instytucję pracy pod przykryciem oraz – mniej sformalizowane pod względem konkretnej metody – czynności zmierzające do niejawnego pozyskania danych osobowych.

W doktrynie niektórzy powstrzymują się od jednoznacznego definiowania czynności operacyjno-rozpoznawczych, skłaniając się ku dokładniejszemu określeniu ich celów. Do tych czynności mają jednak zastosowanie reguły celowościowe, wyznaczane przez współczesną taktykę i technikę kryminalistyczną[15]. To właśnie rozpoznanie śro-

---

[6] P. Czarnecki, *Czynności operacyjno-rozpoznawcze a postępowanie karne*, „Palestra" 2014, nr 7–8, s. 122.

[7] *Ustawa z dnia 6 kwietnia 1990 r. o Policji* (Dz.U. z 1990 r. Nr 30 poz. 179, ze zm.).

[8] *Ustawa z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. z 2002 r. Nr 74 poz. 676, ze zm.).

[9] *Ustawa z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U. z 2006 r. Nr 104 poz. 708, ze zm.).

[10] *Ustawa z dnia 28 września 1991 r. o kontroli skarbowej* (Dz.U. z 1991 r. Nr 100 poz. 442, ze zm.).

[11] *Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego* (Dz.U. z 2006 r. Nr 104 poz. 709, ze zm.).

[12] *Ustawa z dnia 12 października 1990 r. o Straży Granicznej* (Dz.U. z 1990 r. Nr 78 poz. 462, ze zm.).

[13] *Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych* (Dz.U. z 2001 r. Nr 123 poz. 1353, ze zm.).

[14] *Ustawa z dnia 27 sierpnia 2009 r. o Służbie Celnej* (Dz.U. z 2009 r. Nr 168 poz. 1323, ze zm.).

[15] A. Taracha, *Czynności operacyjno-rozpoznawcze: aspekty kryminalistyczne i prawnodowodowe*,

dowisk kryminalnych, ich ewentualna dezintegracja oraz wykrycie przestępstw i potencjalnych sprawców jest głównym celem owych czynności, który dopiero później będzie mógł ukierunkować postępowanie karne[16]. Rozwój ustawodawstwa policyjnego przyczynił się do rozwinięcia funkcji dowodowych zadań operacyjnych. Wielu autorów wskazuje na związki tych czynności również z celami postępowania karnego, głównie ze względu na służenie przyszłym lub aktualnym celom procesu[17]. Funkcja dowodowa, nadal będąca przedmiotem sporu w doktrynie, jest najczęściej określana jako wtórna do całego zakresu działań operacyjnych. Nie bez znaczenia pozostają tu również funkcje informacyjne, rozpoznawcze, profilaktyczne oraz wykrywcze czynności operacyjnych[18].

Jak słusznie zauważył Trybunał Konstytucyjny, choć (…) *inne są cele czynności operacyjno-rozpoznawczych prowadzonych przez służby odpowiedzialne za utrzymanie porządku (np. Policję), inne zaś przez służby informacyjno-wywiadowcze (np. ABW, SKW), to z punktu widzenia naruszenia wolności i praw jednostki nie ma znaczenia, jaki organ władzy publicznej oraz na jakiej podstawie pozyskuje niejawnie informacje na jej temat. Stopień naruszenia prywatności i tajemnicy komunikowania się jest bowiem taki sam*[19].

Warunki ograniczania wolności i praw konstytucyjnych

Niebagatelną rolę w ukształtowaniu ustawodawstwa policyjnego należy przypisać orzecznictwu Trybunału Konstytucyjnego (TK). Szczególnie należy wyróżnić tutaj wyrok z 30 lipca 2014 r.[20], w którym TK odniósł się do wielu aspektów działania służb specjalnych i który przyczynił się do istotnej nowelizacji ustaw policyjnych[21]. Jak wskazano w uzasadnieniu projektu nowelizacji, jego podstawowym skutkiem miało być (…) *urzeczywistnienie zasad i gwarancji konstytucyjnych w sposób wskazany przez Trybunał Konstytucyjny*, a dodatkowo taka regulacja miała (…) *sprzyjać budowaniu zaufania jednostek do działań o charakterze niejawnym podejmowanych przez służby policyjne oraz służby ochrony państwa, w szczególności poprzez zwiększenie przejrzystości przepisów oraz określenie precyzyjnych procedur obowiązujących w omawianym obszarze funkcjonowania Państwa*[22]. Nowelizacja dokonana w lutym 2016 r. wzbudziła kontrowersje, ponieważ miała umożliwiać, kojarzoną jednoznacznie pejoratywnie, inwigilację obywateli[23]. Ta nowelizacja została zaskarżona do TK przez Rzecznika Praw Obywatelskich (dalej: RPO) 18 lutego 2016 r. W ocenie RPO (…) *zakwestionowane przepisy nie tylko nie realizują wyroku Trybunału Konstytucyjnego* (…)*, ale w poważnym zakresie naruszają konstytucyjne prawa i wolności człowieka oraz standardy międzynarodowe*[24].

Lublin 2006, s. 15.

[16] M. Kulicki, V. Kwiatkowska-Wójcikiewicz, L. Stępka, *Kryminalistyka. Wybrane zagadnienia teorii i praktyki śledczo-sądowej*, Toruń 2009, s. 77.

[17] T. Hanausek, *Kryminalistyka. Zarys wykładu*, Kraków 1998, s. 130; J. Kudła, P. Kosmaty, *Ryzyko w czynnościach operacyjno-rozpoznawczych policji: aspekty kryminalistyczne i prawnodowodowe*, Warszawa 2013, s. 239.

[18] A. Taracha, *Czynności operacyjno-rozpoznawczych: aspekty...*, s. 15.

[19] Wyrok TK z 30 VII 2014 r., sygn. akt K 23/11, LEX nr 1491305.

[20] Tamże.

[21] *Ustawa z dnia 15 stycznia 2016 r. o zmianie ustawy o Policji oraz niektórych innych ustaw* (Dz.U. z 2016 r. poz. 147).

[22] *Poselski projekt ustawy o zmianie ustawy o Policji oraz niektórych innych ustaw – uzasadnienie* [online], druk sejmowy nr 154, http://www.sejm.gov.pl/Sejm8.nsf/druk.xsp?nr=154 [dostęp: 17 I 2017].

[23] W takim tonie o nowelizacji pisała Fundacja Panoptykon: W. Klicki, K. Szymielewicz, *Inwigilacja po 6 lutego 2016* [online], https://panoptykon.org/wiadomosc/inwigilacja-po-6-lutego-2016 [dostęp: 17 I 2017].

[24] *Wniosek do TK ws. nowelizacji ustawy o Policji* [online], https://www.rpo.gov.pl/pl/content/wniosek-do-

TK podkreśla, że ingerencja organów państwowych w prywatność czy autonomię informacyjną jest możliwa wyłącznie na zasadach określonych przez ustawę zasadniczą. To państwo powinno zagwarantować prawidłową realizację praw i wolności obywatelskich, które podczas działań organów państwowych mogą zostać naruszone. Zwraca jednak uwagę, że (…) *wykorzystanie niejawnych metod pracy operacyjnej umożliwia ograniczenie skali przestępczości, a to przekłada się na podniesienie stopnia poczucia bezpieczeństwa obywateli i większą swobodę korzystania z zagwarantowanych im wolności i praw*[25].

Większość metod operacyjnych stosowanych przez organy państwowe służy gromadzeniu materiału operacyjnego, który w przeważającej części składa się z informacji o danej jednostce i jej zachowaniu. Podczas postępowania karnego ten materiał zostaje przekształcony w dowód procesowy. Nie bez znaczenia więc pozostaje art. 51 Konstytucji RP, ze szczególnym uwzględnieniem ust. 2 statuującego, że *Władze publiczne nie mogą pozyskiwać, gromadzić i udostępniać innych informacji o obywatelach niż niezbędne w demokratycznym państwie prawnym* oraz ust. 4 stanowiący, że (…) *każdy ma prawo do żądania sprostowania oraz usunięcia informacji nieprawdziwych, niepełnych lub zebranych w sposób sprzeczny z ustawą*.

TK w wyroku z 17 czerwca 2008 r. dotyczącym działalności wywiadu skarbowego wskazał, że art. 51 ust. 2 ustawy zasadniczej konstytuuje (…) *tzw. zasadę autonomii informacyjnej, stanowiącą szczególną eksplikację prawa do prywatności (art. 47 Konstytucji) i funkcjonalnie powiązaną z wolnością komunikowania się (art. 49 Konstytucji)*. Autonomia informacyjna (…) *oznacza prawo do samodzielnego decydowania o ujawnianiu innym informacji dotyczących swojej osoby, a także prawo do sprawowania kontroli nad takimi informacjami, jeśli znajdują się w posiadaniu innych podmiotów*[26]. Art. 51 ust. 4 Konstytucji kształtuje za to (…) *prawa jednostki do przedstawiania/kształtowania swego publicznego obrazu*[27], unormowane w uprawnieniach dotyczących żądania sprostowania informacji i prawie do żądania usunięcia informacji.

Przy uwzględnieniu specyfiki działania służb podczas stosowania czynności operacyjnych (szczególnie że są to czynności tajne) TK zwracał już uwagę, że uprawnienia z art. 51 ust. 4 Konstytucji są ograniczone. Działania operacyjne regulowane przez ustawodawstwo zwykłe (w zgodzie z art. 51 ust. 5 Konstytucji) muszą mieścić się w ramach wskazanych przez art. 49 i art. 51 ustawy zasadniczej. Ponieważ ustrojodawca w przypadku art. 51 ust. 4 Konstytucji nie zdecydował się na pozostawienie ustawodawcy dookreślenia tych uprawnień w drodze ustawy, to ocena proporcjonalności przekraczania granic praw i wolności obywatelskich musi się odbywać wedle surowszych kryteriów niż w wypadku, gdy sama Konstytucja przyznaje ustawodawcy możliwość ograniczenia konstytucyjnie unormowanej wolności lub prawa[28]. Ocena nielegalności pozyskiwania i wykorzystywania informacji o jednostce wymaga więc analizy już na etapie standardu wyznaczonego przez ustawę zasadniczą.

Asumptem do podziału na nielegalność pozyskania i wykorzystania informacji stało się orzeczenie TK z 12 grudnia 2005 r. Trybunał, orzekając o niekonstytucyjności uchylonego już art. 19 ust. 4 ustawy o Policji odnoszącego się do następczej zgody

tk-ws-nowelizacji-ustawy-o-policji [dostęp: 17 I 2017].

[25] Wyrok TK z 30 VII 2014 r., sygn. akt K 23/11, LEX nr 1491305.

[26] Wyrok TK z 17 VI 2008 r., sygn. akt K 8/04, OTK-A 2008 nr 5 poz. 81.

[27] Wyrok TK z 12 XII 2005 r., sygn. akt K 32/04, LEX nr 181611.

[28] Wyrok TK z 17 VI 2008 r., sygn. akt K 8/04, OTK-A 2008 nr 5 poz. 81.

sądu w przypadku nielegalnej (tu – niezalegalizowanej) kontroli operacyjnej, stwierdził, że nie może mieć miejsca sytuacja, w której decyzja sądu o zachowaniu nielegalnie zebranych materiałów z czynności operacyjnych miałaby doprowadzić do jednoczesnego zalegalizowania danej czynności. Taka możliwość wtórnej legalizacji czynności operacyjnej, w kontekście danych uzyskanych przez służby, byłaby bowiem niezgodna z art. 51 ust. 4 Konstytucji[29]. Stanowisko TK zostało zaaprobowane przez doktrynę, która jednoznacznie opowiada się za brakiem możliwości wykorzystania materiału operacyjnego podczas postępowania karnego, w przypadku uzyskania go w toku czynności operacyjnych przeprowadzonych z niezachowaniem ustawowych warunków ich przeprowadzania[30].

Dyspozycja art. 51 ust. 4 w części dotyczącej zbierania informacji o jednostkach jest dość szeroka. Definicyjnie to pojęcie jest na tyle obszerne, że w odniesieniu do procesu karnego i tematu gromadzenia dowodów uznaje się, że (…) *dowód zebrany sprzecznie z ustawą* jest pojęciem szerszym niż tzw. dowód nielegalny. Dowody zebrane sprzecznie z ustawą będą uzyskane w sposób sprzeczny z warunkami ich uzyskania określonymi w ustawie, choć niekoniecznie będą dowodami nielegalnymi[31].

Dowód nielegalny w procesie karnym

Pojęcie d o w ó d n i e l e g a l n y nie jest kategorią ustawową, a w literaturze przedmiotu brak jednolitości co do jego oznaczenia. Niniejsze rozważania warto rozpocząć od próby określenia pojęcia n i e l e g a l n o ś ć w kontekście dowodów oraz dokonać analizy legalności samych czynności operacyjno-rozpoznawczych i możliwości wpływania przez nie na „legalność" materiału operacyjnego, a później samych dowodów.

N i e l e g a l n y w rozumieniu językowym to niezgodny z prawem, niemający mocy prawnej, nieuznany przez prawo czy wręcz bezprawny lub nieformalny[32]. I choć ustawodawca nie definiuje pojęcia n i e l e g a l n o ś ć, to doktryna przeciwstawia to określenie – zdaniem autora jak najbardziej słusznie – pojęciu l e g a l n o ś ć. Oczywiście w takim ujęciu istnieje ryzyko wąskiego i jednoznacznego wyznaczenia semantycznej granicy przebiegającej jedynie na linii pojęć legalność – nielegalność. Ustawa karnoprocesowa nie definiuje legalności lub dopuszczalności dowodów. Nauka procesu karnego i doktryna o wiele częściej odnoszą się do nielegalnego źródła dowodowego, nielegalnego sposobu uzyskania dowodu[33] czy dowodu bezwartościowego lub skażonego[34]. Doktryna częściej odwołuje się do zakresu dopuszczalności dowodu lub ustawowych przesłanek samej legalności czynności dowodowych. Podkreśla się również, że „legalność dowodu" to określenie z szerszego zakresu dotyczącego czynności dowodzenia, mieszczących się w czynnościach procesowych. Dlatego postulaty dookreślenia w ustawodawstwie karnoprocesowym kryteriów

[29] Wyrok TK z 12 XII 2005 r., sygn. akt K 32/04, LEX nr 181611.

[30] D. Szumiło-Kulczycka, *Czynności operacyjno-rozpoznawcze i ich relacje…*, s. 143 i wskazane tam orzecznictwo.

[31] J. Skorupka, *Eliminowanie z procesu karnego dowodu zebranego w sposób sprzeczny z ustawą*, „Państwo i Prawo" 2011, nr 3, s. 81.

[32] *Słownik języka polskiego pod red. W. Doroszewskiego* [online], http://sjp.pwn.pl/doroszewski/nielegalny;5458146.html [dostęp: 17 I 2016].

[33] K. Marszał, *Proces karny*, Katowice 1998, s. 494.

[34] B. Kurzępa, *Zakazy wykorzystywania dowodów w procesie karnym*, „Wojskowy Przegląd Prawniczy" 2002, nr 2, s. 46 i 50.

dopuszczalności i legalności czynności procesowych – w kontekście tak niejednoznacznego pojęcia – należy uznać za słuszne[35].

Kodeks postępowania karnego w art. 246 § 1 posługuje się pojęciem legalność jedynie w kontekście zażalenia na zatrzymanie i możliwości zbadania przez sąd (…) *zasadności, legalności oraz prawidłowości* tej czynności. Art. 246 § 3 i 4 kpk posługują się też pojęciem nielegalność. W rozumieniu tego przepisu legalność to zgodność z prawem[36]. Nielegalność będzie więc niezgodnością z prawem, która będzie mogła przysłużyć się do wykazania wadliwej podstawy zatrzymania.

Doktryna dopuszcza stosowanie pojęcia dowód nielegalny na potrzeby analizy przepisów karnoprocesowych, chociaż najczęściej w kontekście dowodów uzyskanych wbrew zakazom dowodowym. J. Skorupka posługuje się tym określeniem w przypadku wprowadzania do procesu karnego i późniejszego wykorzystania informacji uzyskanych z pogwałceniem konkretnego przepisu ustawy procesowej[37]. Wskazuje tu również na obowiązek nałożony na organy państwa wynikający z art. 51 ust. 4 Konstytucji, który nakazuje im zbierać informacje (dowody) w sposób zgodny z ustawą. Autor uznaje pojęcie dowód nielegalny za szersze od pojęcia (…) *dowodu zebranego w sposób sprzeczny z ustawą*. To implikuje rozumienie takiego dowodu jako uzyskanego w sposób sprzeczny z warunkami wynikającymi z ustawy, co niekoniecznie będzie oznaczało, że taki dowód jest nielegalny[38].

Na szersze spojrzenie na problematykę związaną z dowodem nielegalnym zwracał również uwagę Z. Sobolewski. Uznawał on, że dowód może zostać uzyskany w dwojaki sposób: nielegalny lub niewiarygodny. Dowód nielegalny w rozumieniu tego autora to dowód uzyskany z pogwałceniem kodeksowych reguł określających sposób przeprowadzenia środka dowodowego. Dowód niewiarygodny zaś to dowód uzyskany w sposób wadliwy, który nie wpływa na jego legalność (choć może dojść do naruszenia przepisu ustawy), a jedynie na wiarygodność, która wykluczy jego dopuszczenie w procesie[39]. Wadliwość czynności nie będzie więc od razu prowadziła do jej wyeliminowania z postępowania, ale może mieć wpływ na ocenę jej wyników[40].

Warto również na koniec tych rozważań odnieść się do rozumienia nielegalności jako bezprawności. Bezprawność jest pojęciem języka prawnego, szczególnie na gruncie prawa karnego materialnego. Jest rozumiana jako element struktury przestępstwa oraz (…) *sąd wartościujący, odnoszący się do czynu realizującego znamiona typu czynu zabronionego pod groźbą kary i wyrażający sprzeczność tego czynu z normą nakazującą lub zakazującą określone zachowanie*[41]. Czyn „pierwotnie" legalny to zachowanie, które nie jest skierowane przeciw określonemu dobru prawnemu lub naruszeniu reguł postępowania z tym dobrem[42].

---

[35] M. Klejnowska, *Kilka uwag w wybranych kwestiach dotyczących pozaprocesowego pozyskiwania dowodów i ich wykorzystania w procesie karnym (głos w dyskusji)*, w: *Pozaprocesowe pozyskiwanie dowodów i ich wykorzystanie w procesie karnym,* P. Hofmański, D. Szumiło-Kulczycka, P. Czarnecki (red.), Warszawa 2015, s. 234–235.

[36] Piszą o tym K.T. Boratyńska i M. Królikowski, w: *Kodeks postępowania karnego. Komentarz*, A. Sakowicz i in. (red.), Warszawa 2016, s. 604.

[37] J. Skorupka, *Eliminowanie z procesu karnego…*, s. 81.

[38] Tamże.

[39] Z. Sobolewski, *Wartość nielegalnie uzyskanego dowodu w postępowaniu karnym*, „Annales Universitatis Mariae Curie-Skłodowska" 1976, t. XXIII, Sectio G, s. 45.

[40] A. Gaberle, *Dowody w sądowym procesie karnym*, Kraków 2007, s. 271.

[41] W. Wróbel, A. Zoll, *Polskie prawo karne. Część ogólna*, Kraków 2010, s. 154.

[42] Tamże, s. 167–168.

Tak szerokie rozumienie pojęcia n i e l e g a l n o ś ć, w tym d o w o d y n i e l e g a l n e, rodzi poważne trudności w jednoznacznym zakreśleniu problematyki dotyczącej tych terminów. Kłopotliwy jest również brak ogólnego zakazu dowodowego, obejmującego swym zakresem dowody uzyskane nielegalnie, które mogłyby zostać uznane za nieważne i definitywnie wyeliminowane z procesu karnego[43].

Na podstawie wyżej zarysowanego problemu nielegalność będzie rozumiana w dalszych rozważaniach nie tylko jako niezgodność z daną normą prawną, lecz także jako przekraczanie ustawowych ram dopuszczających daną czynność. Wpływa to na jej legalność, jak również na jej wiarygodność czy wadliwość skutkującą niemożnością wykorzystania ewentualnych wyników z owej czynności.

Legalność czynności operacyjno-rozpoznawczych i wpływ tych czynności na legalność dowodu

Czynności operacyjno-rozpoznawcze nie są czynnościami procesowymi, dlatego nie można odnosić do nich gwarancji procesowych zapewnionych w toku postępowania karnego[44]. Jest to sytuacja niebezpieczna, gdyż działania podczas czynności operacyjnych mogą w istotny sposób naruszać prawa jednostek, a brak stosowanych gwarancji procesowych może wzbudzać obawy, szczególnie w przypadku zbyt dużej samowoli działania organów państwa. Nie oznacza to jednak, że działania te są nieograniczone. Po pierwsze, służby specjalne działające w systemie organów państwowych muszą stosować czynności zgodnie z obowiązującym prawem i w zakresie swoich kompetencji[45]. Po drugie, działania operacyjne służą przeważnie wykrywaniu i ściganiu przestępstw. W ograniczonym zakresie natomiast mają funkcje prewencyjne i informacyjne. Dlatego funkcjonariusze powinni mieć świadomość, że uchybienia w czasie wykonywania tych czynności będą skutkowały trudnościami we wprowadzaniu ich wyników do procesu karnego[46].

Oddzielenie działań operacyjnych od procesowych skutkuje osłabieniem praw (przyszłego) oskarżonego w czasie stosowania owych czynności, które to prawa będą wobec niego stosowane dopiero w postępowaniu karnym. W doktrynie zwraca się jednak uwagę na koncepcję „wydłużonego działania" prawa procesowego na sferę przedprocesową, w tym i operacyjną. Skutkuje to uznaniem, że ze względu na gwarancje proceduralne ograniczające obowiązek dostarczania organom procesowym pewnych informacji dzięki czynnościom operacyjnym, zwłaszcza tych, którym następnie przypisuje się walory dowodowe, nie można czynić tego, na co te gwarancje nie pozwalają[47].

Przeciwdziałaniu jakimkolwiek naruszeniom prawa w toku działań operacyjnych służy głównie standard konstytucyjny, doprecyzowany przez orzecznictwo TK i Europejskiego Trybunału Praw Człowieka (ETPC). Zakres tej legalności dookreśla ustawodawca. Aby wyniki czynności operacyjnych uznać za legalne i móc je wykorzystać w procesie (bez znaczenia, czy są stosowane przed wszczęciem postępowania, czy w jego toku) należy spełnić kilka warunków. Po pierwsze, czynność musi być dokonana przez podmiot ustawowo do tego uprawniony bądź w ramach decyzji uprawnionego

[43] J. Skoczeń, *Istota dowodów nielegalnych*, „Forum prawnicze" 2015, nr 2, s. 41.

[44] A. Taracha, *Czynności operacyjno-rozpoznawcze: aspekty*…, s. 158.

[45] T. Hanausek, *Kryminalistyka*…, s. 40.

[46] A. Taracha, *Czynności operacyjno-rozpoznawcze: aspekty*…, s. 15.

[47] M. Klejnowska, *Prawnodowodowe skutki przekroczenia ram kontroli operacyjnej*, „Annales Universitatis Mariae Curie-Skłodowska" 2009/2010, t. LV l/L VII, Sectio G, s. 64.

organu. Po drugie zakres czynności musi być wyznaczony zgodnie z ustawą, tak w zakresie przedmiotowym, jak i podmiotowym. Prawidłowo zakreślony zakres czynności będzie wyznaczał nakaz wykonania decyzji w sposób w niej określony i tylko w ramach przez nią wskazanych. Po trzecie, decyzja musi być również aktualna lub zostać zatwierdzona, jeśli ma charakter czasowy. Odnośnie do tego A. Gaberle wskazywał na dwa przypadki, które mogą przyczynić się do nielegalności materiału operacyjnego wprowadzonego do procesu. Przede wszystkim, w razie wadliwości decyzji i nieprawidłowego wyznaczenia jej zakresu przedmiotowego bądź podmiotowego, nie doprowadzi ona do zalegalizowania materiału uzyskanego na jej podstawie. Poza tym, jeśli decyzja zostanie wykonana w sposób wadliwy, to również doprowadzi to do wadliwości materiału uzyskanego na jej podstawie[48].

Do przekroczenia zakresu podmiotowego bądź przedmiotowego – na przykładzie kontroli operacyjnej – może dojść w kilku sytuacjach:

- kontrola może dotyczyć osoby objętej postanowieniem o jej przeprowadzeniu, lecz uzyskano informacje na temat przestępstwa nieobjętego takim postanowieniem,
- kontrola może dotyczyć osoby nieobjętej postanowieniem, ale pozyskano informacje o przestępstwie objętym postanowieniem,
- uzyskano informacje o przestępstwie i osobie nieobjętych postanowieniem[49].

Wszystkie te sytuacje wpływają na wadliwość uzyskanego materiału. Według A. Lacha i B. Sitkiewicza, nawet jeśli można by było wskazać korzyści praktyczne, które uzasadniałyby możliwość wykorzystania materiału z kontroli operacyjnej z przekroczeniem jej zakresu (choć legalnych), to nie mogłyby one przeważyć nad względami gwarancyjnymi i koniecznością zapewnienia realizacji konstytucyjnej zasady proporcjonalności w przypadku stosowania tej czynności[50].

Ostatnią, czwartą z przesłanek dotyczącą ewentualnej oceny legalności działań operacyjnych jest spełnienie warunku subsydiarności danej czynności, jak w przypadku kontroli operacyjnej, zakupu kontrolowanego lub przesyłki niejawnie nadzorowanej. Te czynności są stosowane wtedy, gdy inne środki okazały się bezskuteczne lub zachodzi wysokie prawdopodobieństwo, że nie będą skuteczne. Niestety, w praktyce to jest przesłanka niezwykle trudna do zweryfikowania, gdyż wymaga udowodnienia, że inne czynności nie zostały w pełni wykorzystane, a czynność zarządzono wręcz pochopnie. Wszelkie problemy wynikające z niejednoznacznej oceny tej przesłanki mogą przekładać się na wątpliwości co do legalności zarządzenia danego działania[51].

Dowód nielegalny wyczerpujący znamiona przepisu ustawy karnej

Analizę dowodu nielegalnego należy rozpocząć w kontekście dowodu (głównie rozumianego jako środek dowodowy[52]) wyczerpującego znamiona przepisu ustawy karnej. Najczęściej wskazywane możliwości popełnienia przestępstwa w kontekście pozyskania dowodów obejmują:

- ujawnianie lub wykorzystanie informacji z art. 265 kk i 266 kk,

[48] A. Gaberle, *Dowody w sądowym procesie karnym. Teoria i praktyka*, Warszawa 2010, s. 394.

[49] M. Klejnowska, *Prawnodowodowe …*, s. 84.

[50] A. Lach, B. Sitkiewicz, *Glosa do postanowienia SN z 26.04. 2007 r., 1KZP 6/07,* „Prokuratura i Prawo" 2007, nr 10, s. 148.

[51] A. Taracha, *Czynności operacyjno-rozpoznawcze: aspekty…,* s. 284.

[52] S. Waltoś, P. Hofmański, *Proces karny. Zarys systemu*, Warszawa 2013, s. 342.

- uzyskanie informacji (stanowiącej jednocześnie dowód zdobyty na potrzeby postępowania) bez uprawnienia za pomocą przełamania elektronicznego, magnetycznego, informatycznego lub innego o charakterze szczególnym (art. 267 § 1 kk) lub posłużenie się urządzeniem podsłuchowym umożliwiającym uzyskanie takiej informacji (art. 267 § 3 kk),
- tworzenie fałszywych dowodów (art. 235 kk) lub zatajanie dowodów niewinności (236 kk),
- przekroczenie uprawnień przez funkcjonariusza, stypizowane w art. 231 kk,
- łapownictwo bierne i czynne (kolejno art. 228 kk i 229 kk).

Trzy ostatnie przestępstwa znajdą się w kręgu głównej analizy, szczególnie w kontekście czynności operacyjnych.

Podczas stosowania czynności operacyjno-rozpoznawczych może dojść do realizacji typu czynu zabronionego w przypadku m.in. zakupu kontrolowanego, kontrolowanej łapówki, posługiwania się dokumentami legalizacyjnymi przez funkcjonariusza ukrywającego prawdziwą tożsamość lub prowadzącego działalność pod przykryciem.

Możliwość popełnienia przestępstwa przekroczenia uprawnień przez funkcjonariusza publicznego z art. 231 kk ze względu na swój szeroki zakres jest obarczona najwyższym ryzykiem wystąpienia w czasie działań operacyjnych. P r z e k r o c z e n i e u p r a w n i e ń to podjęcie przez sprawcę czynności nieleżącej w granicach jego kompetencji. To przekroczenie zakresu czynności służbowych, do których wykonania sprawca jest uprawniony. Dlatego przypisanie odpowiedzialności może nastąpić dopiero po ustaleniu podstawy oraz zakresu jego uprawnień i obowiązków[53].

Przekroczenie uprawnień następuje nie tylko w momencie działania poza zakresem określonym w prawie procesowym (np. przy przekraczaniu kompetencji przy zatrzymywaniu osoby lub rzeczy albo przeszukaniu pomieszczeń lub osób z rozdziału 25 kpk), lecz także przy wychodzeniu poza działania za pomocą konkretnych metod operacyjnych zakreślone w ustawach policyjnych. Dodatkowo możliwe są również zbiegi przestępstwa przekroczenia uprawnień z np. prowokacją lub podsłuchem operacyjnym z przekroczeniem reguł ustawowych.

Działania operacyjne, podczas których dochodzi do kolizji różnych dóbr z zakresu bezpieczeństwa państwa i praw jednostki, zrodziły w doktrynie dyskusję na temat istnienia kontratypu stanu wyższej konieczności w działaniach funkcjonariuszy publicznych. Uznawanie istnienia takiego kontratypu jest kontrowersyjne, szczególnie ze względu na możliwą sprzeczność z podstawowymi zasadami porządku prawnego, szczególnie zaś z art. 7 i art. 31 ust. 3 Konstytucji RP[54]. Drugim z argumentów jest istnienie w systemie prawnym reguły, według której organy publiczne mogą w swoich działaniach poczynić tyle, na ile pozwala im przewidziane dla nich unormowanie prawne lub kompetencja. Jedynie pozycja prawna jednostki (działającej poza system przewidzianym dla organów państwa) jest ukształtowana według zasady pozwalającej na czynienie wszystkiego, co nie jest prawem zabronione[55].

Dlatego też lepiej będzie oddawał istotę problemu będzie tzw. kontratyp działania w ramach uprawnień i obowiązków (którego granice będą wyznaczać właśnie

[53] M. Szwarczyk, *Komentarz do art. 231 Kodeksu karnego*, w: *Kodeks karny. Komentarz*, T. Bojarski i in. (red.), LEX nr 10269.

[54] P. Daniluk, *Stan wyższej konieczności a legalność działania funkcjonariuszy*, „Wojskowy Przegląd Prawniczy" 2007, nr 1, s. 45.

[55] Tamże, s. 45; por. L. Garlicki, *Polskie prawo konstytucyjne. Zarys wykładu*, Warszawa 2001, s. 60–61.

art. 7 i 31 ust. 3 Konstytucji RP)[56]. Doktryna zaczęła się odnosić do takiego kontratypu głównie w momencie uregulowania w ustawodawstwie policyjnym prerogatyw prawa do prowokacji, w tym zakupu kontrolowanego i kontrolowanego wręczenia korzyści majątkowej. Zostały one ustanowione w stosunku do czynności operacyjno-rozpoznawczych (wskazanych powyżej), które wypełniają znamiona czynu zabronionego. Istotą kontratypu, o którym mowa, jest legalizacja tego rodzaju działań funkcjonariuszy. Takie unormowanie jest niezwykle istotne i potrzebne w demokratycznym państwie prawnym. Jego brak skutkowałby tym, że realizacja danej czynności (nawet całkowicie zgodna z unormowaniem ustawowym) stanowiłaby przestępstwo, stojące na przeszkodzie realizacji celów, jakim służą czynności operacyjne[57]. Ustawodawca posługuje się w przypadku legalizacji tych działań sformułowaniem *nie popełnia przestępstwa* (art. 144a ustawy o Policji, art. 21 ustawy o CBA, art. 32 ustawy o ABW i AW). Jest to konstrukcja, która nie określa okoliczności wyłączającej bezprawność, lecz normuje kontratyp operacyjny jako okoliczność przyzwalającą na bezprawność[58]. Problem tzw. paradoksu przestępstwa nieprzestępnego[59] wskazywany w literaturze nie jest jedyny. Główną konstatacją w tym kontekście jest to, że mimo iż czynności operacyjne mogą być dokonywane przez różne służby, to tylko niektóre z nich zostały objęte istnieniem ich odpowiedniego kontratypu. Są to Policja, CBA, ABW i AW oraz SWW i SKW. Poza tym kręgiem pozostają funkcjonariusze Służby Celnej i Wywiadu Skarbowego, Straży Granicznej oraz Żandarmerii Wojskowej. W połączeniu z tym, że jednak większość ustawowych działań operacyjnych pozostaje poza kręgiem ochrony kontratypem, wskazuje się na próby objęcia ich osłoną prawną. Może to być odwołanie się do konstrukcji rozkazu (zdefiniowanego w art. 115 § 18 kk) zgodnie z art. 318 kk, przy analogicznym stosowaniu konstrukcji rozkazu do działania funkcjonariuszy w poszczególnych służbach[60].

Dowód nielegalny sprzeczny z ustawą określającą sposób jego przeprowadzenia

Kodeks postępowania karnego reguluje wiele czynności wykonywanych przy przeprowadzaniu dowodów. Dotyczą one głównie swego rodzaju „ujawniania" środków dowodowych. Wskazuje się tutaj na przesłuchanie, oględziny, eksperyment procesowy oraz odczytanie dokumentu[61].

Ustawa karnoprocesowa sama wprowadza zakazy dowodowe, które eliminują dowody z powodu ich sprzeczności z ustawą określającą sposób ich przeprowadzania, m.in.:

- zakaz stosowania niedopuszczalnych metod w czasie zbierania dowodów z osobowych źródeł dowodowych (art. 171 § 4 i 5 kpk),
- zakaz substytuowania dowodu z wyjaśnień oskarżonego lub zeznań świadka treścią pism, zapisków lub notatek urzędowych (art. 174 kpk),
- zakaz wykorzystania na rozprawie protokołu zeznań złożonych przez świadka, który skorzystał z prawa odmowy zeznań (albo został zwolniony z obowiązku zeznawania w zgodzie z art. 186 kpk),

[56] F. Prusak, *Kontratyp czynności operacyjno-rozpoznawczych*, „Zeszyty Prawnicze" 2013, nr 1, s. 26.
[57] Tamże…, s. 26.
[58] K. Buchała, *Prawo karne materialne*, Warszawa 1980, s. 270.
[59] F. Prusak, *Kontratyp czynności*…, s. 27; J. Skoczeń, *Istota dowodów*…, s. 50.
[60] F. Prusak, *Kontratyp czynności*..., s. 30–31.
[61] Por. *Prawo dowodowe. Zarys wykładu*, R. Kmiecik (red.), Kraków 2005.

- zakaz skorzystania z treści oświadczenia oskarżonego, które dotyczy zarzucanego mu czynu, jeśli zostało złożone wobec biegłego albo lekarza udzielającego pomocy medycznej (art. 199 kpk),
- zakaz wykorzystania protokołu przesłuchania świadka, który jest przesłuchiwany w charakterze oskarżonego (391 § 2 kpk w zw. z 389 § 1 kpk)[62].

Doktryna wskazuje sytuacje, które również mogą doprowadzić do usunięcia z procesu karnego dowodu zdobytego niezgodnie z procesowymi regułami jego przeprowadzania. Te sytuacje są pośrednio związane z wyżej wymienionymi zakazami. Z. Kwiatkowski wyróżnił tutaj trzy rodzaje zakazów: zakaz wykorzystywania dowodów pozyskanych ze źródła nielegalnego, zakaz wykorzystania dowodów pozyskanych z niezachowaniem ustawowych warunków w zakresie przymusowego odebrania rzeczy, zatrzymania przesyłek i kontroli korespondencji oraz zakaz wykorzystania dowodów zebranych z niezachowaniem ustawowych warunków stosowania podsłuchu telefonicznego[63]. Autor w celu wskazania przykładu nielegalnego źródła dowodu odwołuje się do dwóch przykładów. Po pierwsze, za taką sytuację uznaje przeprowadzenie dowodu w zakresie tezy niepodlegającej dowodzeniu za pomocą jakichkolwiek dowodów (np. art. 108 § 1 kpk). Po drugie, wskazuje na nielegalność źródła, która wynika z przeprowadzenia niedopuszczalnego dowodu ze względu na zakaz dowodzenia za jego pomocą (gdy np. przesłuchano duchownego co do faktów, których dowiedział się podczas spowiedzi – art. 178 pkt 1 i 2)[64].

Najważniejsze jednak pozostają skutki, jakie powoduje pozyskanie dowodów ze źródeł nielegalnych. Z. Kwiatkowski uznaje, że jeśli ustawodawca, kierując się różnymi względami – aksjologicznymi lub prakseologicznymi – wprowadził do ustawy konkretne zakazy dowodowe, to pragnął nie dopuścić do tego, aby za ich pomocą, nawet w imię dotarcia do prawdy, miało dojść do naruszenia określonego dobra, które chroni dany zakaz dowodowy. Uznaje więc, że nielegalne źródło dowodu dyskwalifikuje każdy dowód – tak obciążający, jak i odciążający[65].

Znacznie szerszym problemem jest wykorzystanie w procesie dowodów „pośrednio legalnych". Po pierwsze, doktryna uznaje koncepcję autonomicznej legalności czynności dowodowych. Zgodnie z nią dowody uzyskane w czasie procesu powinny być traktowane niezależnie od legalności czynności procesowych, jeżeli same były wynikiem czynności dowodowych zgodnych z prawem[66]. Co więcej, dzięki zasadzie swobodnej oceny dowodów (art. 7 kpk) jest możliwe dopuszczenie do przeprowadzania wszelkich czynności dowodowych, z wyjątkiem czynności objętych wyraźnym zakazem ich przeprowadzania. Wykonywanie czynności dowodowej nieobjętej zakazem nie przyczynia się więc do jej autonomicznej dyskwalifikacji[67]. Ponieważ celem postępowania karnego jest wykrycie i pociągnięcie do odpowiedzialności sprawcy przestępstwa, również argumentem przemawiającym za dopuszczeniem dowodów pośrednio legalnych jest także określenie wagi uchybienia, do jakiego dochodzi w momencie przekroczenia zakresu ustawowego unormowania jego przeprowadzenia. Warunkiem dopuszczenia takiego dowodu będzie wtedy stopień naruszenia przepisów przy prze-

[62] Por. Z. Kwiatkowski, *Zakazy dowodowe w procesie karnym*, Kraków 2005.
[63] Tamże.
[64] Tamże, s. 387–388.
[65] Tamże, s. 389.
[66] Tamże, s. 426.
[67] J. Skoczeń, *Istota dowodów*…, s. 48.

prowadzaniu dowodu bezpośrednio nielegalnego oraz rozmiar i waga przekroczenia obowiązujących zakazów dowodowych i wiarygodność dowodu pochodzącego z nielegalnego źródła[68].

Powyższa problematyka i doktryna została w toku zmian ustawodawczych zaktualizowana o normę art. 168a kpk, który po nowelizacji kodeksu postępowania karnego w 2013 r.[69] wprowadzał z dniem 1 lipca 2015 r. ważną normę dotyczącą dowodów nielegalnych.

Dowody z czynności operacyjno-rozpoznawczych na gruncie art. 168a kpk

Każda analiza normy za art. 168a kpk musi rozpocząć się od wskazania, że była to pewna próba reminiscencji elementów teorii owoców zatrutego drzewa na gruncie polskiej procedury karnej. Sama teoria nigdy nie została zdefiniowana w polskiej ustawie karnoprocesowej. Ponieważ jednak odnosi się do możliwości wykorzystania w procesie dowodów nielegalnych w sposób pośredni, leżała w kręgu zainteresowania doktryny[70]. Wskazywano, że nigdy nie będzie ona mogła zostać przetransponowana do polskiego procesu karnego w postaci oryginalnej. Sprzeciwiała się temu zasada prawdy materialnej, mająca w naszej procedurze karnej kardynalne (choć nie bezwzględne) znaczenie. Dodatkowo za odrzuceniem teorii owoców zatrutego drzewa może przemawiać wspominana już koncepcja autonomicznej legalności czynności dowodowych[71].

Art. 168a kpk z dniem 1 lipca otrzymał następującą treść: *Niedopuszczalne jest przeprowadzenie i wykorzystanie dowodu uzyskanego do celów postępowania karnego za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 Kodeksu karnego*. To oznacza kategoryczny zakaz wykorzystania dowodu pozyskanego nielegalnie w rozumieniu realizacji znamion typu czynu zabronionego z art. 1 § 1 kk i dotyczy jedynie realizacji znamion strony przedmiotowej danego czynu (bez względu na winę, stopień społecznej szkodliwości czy uznanie tego czynu za typ przepołowiony)[72]. Ten zakaz odnosi się do pozyskiwania dowodów zarówno przez służby państwowe, jak i przez podmioty prywatne. Dodatkowym wymogiem aktualizacji zakazu z art. 168a kpk było uzyskanie dowodu *dla celów postępowania karnego*. Wymieniony artykuł określi granice dopuszczalności wykorzystania dowodów zaprezentowanych przez oskarżyciela, zawężone jedynie do czynności przeprowadzania i wykorzystania dowodów. Nie objęły więc one wszelkich czynności procesowych.

W doktrynie pojawiły się jednak opinie nieprzypisujące art. 168a kpk atrybutów zakazu dowodowego, lecz określające tę normę jako przepis statuujący, że czynności przeprowadzone w taki sposób są z mocy prawa procesowego bezskuteczne. Dlatego nie można takiego dowodu przeprowadzić lub wykorzystać w postępowaniu[73]. Nietrudno również zgodzić się z tym, że norma z art. 168a kpk nie była ostatecznym przychyleniem się przez ustawodawcę do teorii owoców zatrutego drzewa lub zakreśleniem problematyki dotyczącej dowodów pośrednio legalnych[74].

---

[68] Tamże, s. 47. Por. wyrok SO w Białymstoku z 26 XI 2009 r., sygn. akt III K 224/08, LEX nr 1294013.

[69] *Ustawa z dnia 27 września 2013 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw* (Dz.U. z 2013 r. poz. 1247).

[70] Z. Kwiatkowski, *Zakazy dowodowe*…, s. 426.

[71] P.M. Lech, *Owoce zatrutego drzewa w procesie karnym. Dowody zdobyte nielegalnie*, „Palestra" 2012, nr 3–4, s. 40.

[72] Piszą o tym K.T. Boratyńska, M. Królikowski w: *Kodeks postępowania karnego*…, s. 433.

[73] P. Kardas, *Wpływ kontradyktoryjnego modelu rozprawy głównej na przebieg postępowania karnego*, „Prokuratura i Prawo" 2015, nr 1–2, s. 229.

[74] J. Skoczeń, *Istota dowodów*…, s. 49.

Powyższa problematyka musi zostać wzbogacona o analizę nowego brzmienia art. 168a kpk. Zgodnie bowiem z nowelizacją procedury karnej, dokonaną w marcu 2016 r.[75] (ustawa weszła w życie 15 kwietnia 2016 r.), przepis art. 168a kpk otrzymał następujące brzmienie:

> Dowodu nie można uznać za niedopuszczalny wyłącznie na tej podstawie, że został uzyskany z naruszeniem przepisów postępowania lub za pomocą czynu zabronionego, o którym mowa w art. 1 § 1 kodeksu karnego, chyba że dowód został uzyskany w związku z pełnieniem przez funkcjonariusza publicznego obowiązków służbowych, w wyniku: zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności.

Ustawodawca usunął z zakazu dowodowego podstawę wyłączenia dowodu ze względu na jego niezgodność z przepisami postępowania lub uzyskaniem go za pomocą czynu zabronionego w rozumieniu art. 1 § 1 kk. Dodatkowe stwierdzenie o niedopuszczalności dowodu uzyskanego przez funkcjonariusza oraz za pomocą konkretnie wskazanych czynów zabronionych wymaga chwilowego zatrzymania się nad tym problemem, gdyż w uzasadnieniu ustawy[76] czytamy, że tego typu uregulowanie odnosi się do orzecznictwa ETPC, w którym Trybunał nie wiązał nielegalnego pozyskiwania dowodów z zakazem jego przeprowadzania w postępowaniu karnym[77]. Taka argumentacja ustawodawcy nie została zaaprobowana przez doktrynę, odnoszącą się do orzecznictwa krajowego i międzynarodowego. TK podkreślał, że konieczna jest ochrona jednostki przed tendencją organów ścigania zmierzającą do pozyskiwania dowodów bez względu na prawa i wolności obywatelskie, szczególnie w kontekście ochrony godności, prywatności i wolności komunikowania się owej jednostki[78]. ETPC wskazywał, że prawo procesowe powinno być wyposażone w mechanizmy pozwalające na podważenie dowodu uzyskanego z przekroczeniem przez służby organów państwowych ustawowych przesłanek dopuszczalności dowodów, szczególnie w przypadku ich niezgodności z art. 3 *Konwencji o ochronie praw człowieka i podstawowych wolności*[79].

Problematyczne może być również określenie właściwego charakteru art. 168a kpk w kontekście zakazów dowodowych. O ile przed nowelizacją z kwietnia 2016 r. normę tego artykułu uznawano za zakaz bezwzględny niezupełny, o tyle teraz uznaje się, że może ona być swoistym „kontrzakazem dowodowym"[80].

Ustawodawca zdecydował się na usunięcie zwrotu dotyczącego uzyskania dowodu *dla celów postępowania karnego*. Brak podjęcia działań podmiotu w celu pozyskania dowodu rozszerza znaczenie aktualnego brzmienia art. 168a kpk. Ustawodawca

[75] *Ustawa z dnia 11 marca 2016 r. o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw* (Dz.U. z 2016 r. poz. 437, ze zm.).

[76] *Rządowy projekt ustawy o zmianie ustawy – Kodeks postępowania karnego oraz niektórych innych ustaw – uzasadnienie* [online], druk sejmowy nr 207, http://www.sejm.gov.pl/sejm8.nsf/druk.xsp?nr=207 [dostęp: 17 I 2017].

[77] Por. wyrok ETPC z 12 VII 1988 r. w sprawie Schenk przeciwko Szwajcarii, skarga nr 10862/84; wyrok ETPC z 12 V 2000 r. – Khan przeciwko Wielkiej Brytanii, sygn. 35394/97.

[78] Wyrok TK z 30 VII 2014 r., sygn. akt K 23/11, LEX nr 1491305, wyrok TK z 12 XII 2005 r., sygn. akt K 32/04, LEX nr 181611.

[79] Wyrok ETPC z 1 III 2011 r. w sprawie Welke i Białek przeciwko Polsce, nr skargi 15924/05, wyrok ETPC z 1 VI 2010 r. w sprawie Gäfgen przeciwko Niemcom, skarga nr 22978/05.

[80] Pisze o tym M. Kurowski w: *Kodeks postępowania karnego. Komentarz do zmian 2016*, D. Świecki i in. (red.), Warszawa 2016, s. 167.

posłużył się jednak stwierdzeniem odnoszącym się do uzyskania dowodów z naruszeniem przepisów postępowania. Należy przez to rozumieć każde naruszenie przepisów postępowania karnego i przepisów dotyczących pozyskiwania dowodów wymienianych w ustawach szczególnych[81].

Norma art. 168a kpk w części dotyczącej funkcjonariusza publicznego odwołuje się do uzyskania dowodu w związku z pełnieniem przez niego obowiązków służbowych. Ta norma wyklucza posłużenie się dowodem w czasie procesu przez osobę trzecią, jeśli weszła ona w jego posiadanie w związku z pełnieniem przez funkcjonariusza obowiązków służbowych[82]. Pojęcie funkcjonariusz publiczny jest zdefiniowane w art. 115 § 3 kk i powinno być rozumiane zgodnie z tym przepisem. Elementem aktualizacji normy wskazanej w art. 168a kpk będzie związek funkcjonalny między działaniem funkcjonariusza publicznego podczas służby a pozyskaniem dowodu. Dopiero wykazanie związku między tymi czynnościami przełoży się na ewentualną eliminację dowodu z procesu.

Ostatnim składnikiem zakazu jest udowodnienie, że osoba zdobyła dowód w wyniku metod działań przestępnych wskazanych w przepisie, tj. zabójstwa, umyślnego spowodowania uszczerbku na zdrowiu lub pozbawienia wolności.

Nowe brzmienie art. 168a kpk przekształciło myślenie na temat dopuszczalności dowodu uzyskanego za pomocą czynu zabronionego. Pojęcie naruszenie prawa nie jest nowe na gruncie kodeksowym – kodeks postępowania karnego posługuje się nim m.in. w przypadku podstaw kasacji w art. 523 § 1. Samo więc naruszenie powinno być rozumiane szeroko, jako uchybienie w zastosowaniu normy procesowej w przypadku uzyskiwania dowodów. Doktryna wskazuje jednak na inne problemy. Takie brzmienie przepisu ogranicza rolę sądu w przypadku pozyskiwania dowodów przez funkcjonariuszy publicznych, głównie ze względu na wyłączenie możliwości zastosowania art. 170 § 1 pkt 1 kpk jako podstawy oddalenia wniosku dowodowego[83]. Dodatkowo przyjęcie dowodu jako zgodnego z normą art. 168a kpk nie uzasadnia jego automatycznego uznania za dowód wiarygodny. Nadal będzie on podlegał ocenie pod kątem zgodności z zasadą swobodnej oceny dowodów. Sąd będzie mógł dokonać jego oceny w kontekście ewentualnego naruszenia określonych norm. Jednak ocena wiarygodności dowodu leży w jego sferze faktycznej, a nie normatywnej, która odnosi się do jego dopuszczenia w procesie[84]. Sąd nadal będzie mógł dokonać oceny konstytucyjności przepisu na etapie wyrokowania, co pozwoli mu na ewentualne pominięcie przepisu niezgodnego z Konstytucją[85] w podstawie orzeczenia.

Powyższa opinia wskazuje na to, że art. 168a kpk w aktualnym brzmieniu może być normą niekonstytucyjną. Wątpliwości te podzielił już RPO, który 6 maja 2016 r. skierował do TK wniosek o stwierdzenie niezgodności tego artykułu z Konstytucją RP i *Konwencją o ochronie praw człowieka i podstawowych wolności*[86]. RPO wskazał, że norma z art. 168a kpk dopuszcza sytuację, w której będzie mogło dojść do oparcia przez sąd aktu oskarżenia na czynności (lub dowodzie) popełnionej całkowicie niezgodnie

[81] Tamże, s. 171.

[82] Tamże.

[83] Tamże, s. 175.

[84] Por. wyrok SA we Wrocławiu z 15 X 2015 r., sygn. akt II AKa 224/15, LEX nr 1927493.

[85] Piszą o tym K.T. Boratyńska i M. Królikowski w: *Kodeks postępowania karnego*…, s. 437–438.

[86] Wniosek RPO do TK ws. owoców zatrutego drzewa (art. 168a kodeksu postępowania karnego) z 6 V 2016 r., sygn. II.510.360.2016.KŁS [online], https://www.rpo.gov.pl/sites/default/files/Wniosek%20do%20TK%20owoce%20zatrutego%20drzewa%20art%20art.%20168a%20%20KPK%206.05.2016.pdf [dostęp: 17 I 2017].

z prawem. Mimo wyjątków wprowadzonych przez ustawodawcę, w związku z którymi dowód nie będzie mógł być dopuszczony do procesu karnego, ten przepis nadal dopuszcza możliwość wykorzystania w procesie materiałów z czynności operacyjnych, nawet gdy te materiały zdobyto podczas przeprowadzania czynności operacyjnych niezgodnych z prawem. Wyjątki wprowadzone przez ustawodawcę nie są wystarczające ze względu na szeroki zakres działań operacyjnych[87]. Ponieważ w zgodzie z art. 168a kpk będzie dopuszczalne wykorzystanie dowodów nielegalnych, organ procesowy może ustalić strategię procesową na podstawie takich dowodów. Jest to szczególnie niebezpieczne podczas stosowania kontroli operacyjnej, ponieważ przepisy nie przewidują informowania zainteresowanych o tym, że były wobec nich prowadzone czynności z zakresu tej metody. Organy władzy publicznej mogą więc nawet same skłaniać się ku temu, że będą zdobywały materiał dowodowy z naruszeniem przepisów prawa[88].

Wątpliwości RPO należy uznać za słuszne i zasadne. Takie unormowanie art. 168a kpk znacznie utrudniło ewentualną eliminację z procesu tych dowodów, które mogły być zbierane w ramach nielegalnych działań operacyjnych. Wskazywany już wcześniej brak unormowania – w przypadku wszystkich służb specjalnych – tzw. kontratypu operacyjnego mógł zostać w pewnym stopniu wyeliminowany przez zachowanie poprzedniego brzmienia art. 168a kpk. Na gruncie współczesnej doktryny prawa karnego odrzucono koncepcję zaliczenia okoliczności wyłączających bezprawność czynu, co skutkuje wyróżnianiem tzw. legalności wtórnej, czyli braku bezprawności ze względu na zaistnienie kontratypu (w opozycji do tzw. legalności pierwotnej) do znamion negatywnych czynu zabronionego. Dlatego też w doktrynie pojawiły się opinie, że nieracjonalne byłoby wykluczanie dowodów z procesu ze względu na wspominane kontratypy określone przez ustawodawcę[89].

Oczywiście na gruncie poprzedniego stanu prawnego zakaz z art. 168a kpk był ujęty bardzo wąsko, ze względu na odwołanie się do czynu zabronionego w rozumieniu art. 1 § 1 kk nie obejmował naruszeń prawa nieskutkujących realizacją określonego czynu zabronionego stypizowanego w kodeksie karnym. Ostatnia nowelizacja procedury karnej pogłębiła więc tylko ten problem. Zakres możliwości naruszenia przepisów w czasie stosowania czynności operacyjno-rozpoznawczych jest tak szeroki, że nawet wówczas, gdy funkcjonariusz działałby w ramach kontratypu operacyjnego, inne uchybienia w stosowaniu konkretnej metody zawsze mogłyby skutkować pociągnięciem go do odpowiedzialności za przestępstwo przekroczenia uprawnień, unormowane w art. 231 kk. Jako przykład może tu posłużyć uzyskanie w czasie stosowania kontroli operacyjnej materiałów, które nie mogą być wykorzystane w procesie z uwagi na brak zgody sądu na zastosowanie tej metody. Uprawnienia do kontroli zostają zakreślone w decyzji sądu. Zamieszczenie w akcie oskarżenia zarzutów opartych wyłącznie na nieprawidłowej kontroli operacyjnej mogłoby skutkować pociągnięciem funkcjonariusza do odpowiedzialności karnej na podstawie przepisu art. 231 § 1 kk[90]. Na gruncie znowelizowanego art. 168a kpk nie musi już jednak dojść do eliminacji takich dowodów. Oczywiście przepis ten stanowi, że nie można uznać danego dowodu za niedopuszczalny, jeśli

[87] Tamże, s. 8.

[88] Tamże, s. 12–14.

[89] A. Lach, *Dopuszczalność dowodów uzyskanych z naruszeniem prawa w postępowaniu karnym*, „Państwo i Prawo" 2014, nr 10, s. 46–47.

[90] Ł. Twarowski, *Legalizacja i procesowe wykorzystanie podsłuchów zgromadzonych w ramach czynności operacyjno-rozpoznawczych Policji*, „Palestra" 2010, nr 9–10, s. 78.

naruszenie przepisów postępowania byłoby jedyną podstawą jego odrzucenia. A to, zdaniem autora, może stanowić swego rodzaju furtkę dla poszukiwania innych podstaw niedopuszczalności dowodu.

Ponieważ problematyka art. 168a kpk już w poprzednim brzmieniu tego przepisu budziła wątpliwości, nadal aktualne pozostają postulaty jak najszybszego unormowania w kodeksie postępowania karnego kompleksowej regulacji dotyczącej pozyskiwania i wykorzystania w procesie karnym materiałów z czynności operacyjnych[91].

Dopuszczalność wykorzystania dowodów uzyskanych z naruszeniem prawa

Temat dopuszczalności dowodów uzyskanych z naruszeniem prawa w ujęciu idealnym może prowadzić do konkluzji, że organy procesowe, przekraczając normy prawne, nie mogą czynić ustaleń faktycznych i biorą za podstawę czynności wadliwe. Model idealny może być jednak tylko punktem odniesienia w trakcie poniższych rozważań. A. Lach proponuje dokonać podziału dopuszczalności dowodów na trzech płaszczyznach normatywnych: na poziomie ustawy karnoprocesowej, Konstytucji oraz Europejskiej Konwencji Praw Człowieka (EKPC)[92]. Taki podział warto przeanalizować.

Jak wskazuje A. Lach, kodeks postępowania karnego nie określa ogólnej normy, która zakazywałaby wykorzystania dowodów uzyskanych z naruszeniem prawa. Autor wskazuje również, że ewentualnego dookreślenia takich zakazów można poszukiwać w regulacjach odnoszących się jedynie do określonej grupy dowodów. Wymienia w niej art. 171 § 7 kpk, zgodnie z którym wyjaśnienia, zeznania oraz oświadczenia złożone w warunkach wyłączających swobodę wypowiedzi lub uzyskane wbrew zakazom wymienionym w § 5 tego artykułu nie mogą stanowić dowodu. Zwraca również uwagę na przepisy dotyczące wykorzystania materiałów z kontroli i utrwalania rozmów z art. 237 § 2 kpk (oraz już uchylonego w aktualnym stanie prawnym art. 237 § 8 kpk)[93].

Możliwość bezpośredniego stosowania przepisów Konstytucji w procesie karnym nie budzi w doktrynie wątpliwości. Dlatego za kolejną płaszczyznę niedopuszczalności dowodu nielegalnego należy wskazać unormowania konstytucyjne. W wyroku SA w Białymstoku z 18 marca 2010 r.[94] w kontekście zakazu wykorzystania, nawet w sposób pośredni, informacji pozbawionych atrybutów legalności, sąd odwołał się do art. 5 i 7 Konstytucji RP. A. Lach uznaje to za nieprzekonującą podstawę uznania niedopuszczalności dowodów ze względu na ogólny charakter tych przepisów[95]. Nie sposób jednak pominąć w tym miejscu art. 51 ust. 4 Konstytucji, dotyczącego autonomii informacyjnej jednostki. Publiczne prawo podmiotowe, zagwarantowane w tym przepisie, nakazuje organom publicznym usuwać informacje o jednostce zebrane w sposób sprzeczny z ustawą. Organ publiczny, który będzie chciał wykorzystać materiał uzyskany niezgodnie z prawem lub taki, który powinien być ze względu na wadliwość zniszczony, zawsze będzie postępował sprzecznie ze standardem art. 51 ust. 4 Konstytucji. Przepis, o którym mowa, będzie miał zastosowanie również do czynności operacyjnych. Jednak ze względu na ich poufny charakter zakres stosowania tego przepisu może być znacznie ograniczony[96].

[91] P. Czarnecki, *Czynności operacyjne u wrót procesu. Garść refleksji*, w: *Pozaprocesowe pozyskiwanie*…, s. 187.
[92] Zob. A. Lach, *Dopuszczalność dowodów*…, s. 40–41
[93] Tamże, s. 39.
[94] Wyrok SA w Białymstoku z 18 III 2010 r., sygn. akt II AKa 18/10, LEX nr 577418.
[95] A. Lach, *Dopuszczalność dowodów*…, s. 41.
[96] P. Czarnecki, *Czynności operacyjne u wrót procesu*…, s. 186.

Trzecią płaszczyzną są unormowania międzynarodowe, zwłaszcza w zakresie EKPC. ETPC nieraz wskazywał w swoim orzecznictwie na to, że w gestii organów krajowych leży problem unormowania dopuszczalności dowodów w procesie karnym, co jednak pozwalało mu wnioskować, że dowód pozyskany z naruszeniem prawa może zostać dopuszczony w postępowaniu[97]. Trybunał podkreślał w wielu orzeczeniach, że problematyka gromadzenia i dopuszczania dowodów w procesie przekłada się na rzetelność całego postępowania. Unormowaniem odnoszącym się do tej rzetelności na gruncie polskiej ustawy ustrojowej jest art. 45 Konstytucji, a na gruncie EKPC – jej art. 6.

ETPC często odwoływał się do naruszenia tej zasady w przypadku stosowania czynności operacyjnych z przekroczeniem jej ustawowych ram lub z brakiem podstaw do stosowania tych czynności. O procesie nierzetelnym, niezgodnym z art. 6 EKPC mówi się w przypadku oparcia materiału dowodowego na bezpodstawnej prowokacji przeprowadzonej w ramach działań operacyjnych. Materiał z takich działań służb powinien być przez sąd pominięty[98]. Za naruszenie art. 6 EKPC należy uznać również pozyskanie dowodu niezgodnie z art. 3 EKPC określającym zakaz stosowania tortur, w którym Trybunał bezwzględnie odrzucił możliwość wykorzystania takiego dowodu[99].

Wyznaczenie zakresu podstaw do ograniczania dopuszczalności dowodów w procesie karnym jest konieczne, ale rodzi problemy, szczególnie podczas ostatecznego wykorzystania materiału pochodzącego z wadliwych czynności operacyjnych w trakcie postępowania przed sądem.

Pierwszą z możliwości jest określenie skutków, jakie wywołuje przekroczenie ustawowych ram danej czynności. Odpowiedź na pytanie, co powoduje uzyskanie dowodu w sposób sprzeczny z ustawą, wydaje się prosta, zwłaszcza w kontekście orzecznictwa SN, który stwierdził, że brak zachowania określonych ustawowych warunków dopuszczalności przeprowadzenia działań operacyjno-rozpoznawczych zawsze będzie uniemożliwiał wykorzystanie materiału dowodowego[100] zdobytego podczas takich działań. Doktryna jednak wskazuje na jedną z metod – kontrolę operacyjną – która nawet przy tak jednoznacznym orzecznictwie nadal stwarza trudności przy ewentualnym dopuszczaniu do postępowania materiału zgromadzonego podczas jej stosowania. W przypadku tej metody ustawodawca zdecydował się na sporządzenie wykazu przestępstw, przy których wykrywaniu służby mogą prowadzić swoje działania.

Na przestrzeni lat doktryna wypracowała model postępowania z materiałem operacyjnym w takiej sytuacji. Należy podkreślić, że jest to sytuacja, w której samo zarządzenie kontroli operacyjnej przez odpowiedni organ jest prawidłowe. Zakreślenie wykazu przestępstw, w których przypadku może być stosowana kontrola operacyjna, stanowi gwarancję możliwości ich przeprowadzenia i przekłada się na realizację postulatu pewności prawa, wymaganego w demokratycznym państwie prawnym.

W przypadku uzyskania podczas kontroli operacyjnej informacji, które mogą dotyczyć przestępstwa spoza katalogu ustawowego, w doktrynie przyjmowano, że nie mogą one być bezpośrednio wykorzystane w procesie[101]. Zgodnie z art. 19 ust. 17 ustawy o Policji powinny zostać zniszczone. Gdyby jednak były umieszczone na jednym nośni-

[97] Por. wyrok ETPC z 12 VII 1988 r. w sprawie Schenk przeciwko Szwajcarii, skarga nr 10862/84.

[98] Por. wyroki ETPC z 5 II 2008 r. w sprawie Ramanauskas przeciwko Litwie, skarga nr 74420/01 oraz z 9 VI 1998 r. w sprawie Teixeria de Castro przeciwko Portugalii, skarga nr 25829/94.

[99] Wyrok ETPC z 11 VII 2006 r. w sprawie Jalloh przeciwko Niemcom, skarga nr 548100/00.

[100] Postanowienie SN z 30 XI 2010 r., sygn. akt III KK 152/10, OSP 2011, nr 6, poz. 65; postanowienie SN z 22 IX 2009 r., sygn. akt III KK 58/09, OSNKW 2010, nr 3, poz. 28.

[101] P. Czarnecki, *Czynności operacyjno-rozpoznawcze a postępowanie*..., s. 125.

ku razem z informacjami objętymi katalogiem ustawowym i decyzją o kontroli – będą podlegać bezwzględnemu zakazowi dowodowemu[102]. Zniszczenie materiału nie pozbawia jednak możliwości dowodzenia danej okoliczności za pomocą innych środków dowodowych, które zostały ustalone na podstawie wadliwego materiału. Ponadto wskazuje się, że nie ma przeszkód, aby te materiały stały się źródłem informacji o dowodzie, umożliwiającym przeprowadzenie postępowania sprawdzającego albo wszczęcie postępowania lub innych czynności zgodnie z kpk[103].

Drugą z możliwości przekroczenia zakresu stosowania kontroli operacyjnej jest zebranie w jej trakcie materiału dotyczącego osoby, która nie została objęta przedmiotem kontroli. W tym przypadku będzie konieczne uzyskanie zgody następczej sądu na wykorzystanie danego materiału w czasie postępowania[104].

Powyższa problematyka musi jednak być wzbogacona o analizę art. 168b kpk, wprowadzonego nowelą kwietniową w 2016 r., w którym ustawodawca zdecydował się na uregulowanie problemu zgody następczej w ustawie karnoprocesowej, nadal pozostawiając w ustawach dotyczących poszczególnych służb kwestie dotyczące stosowania samej metody. Podmiotem uprawnionym do wykorzystania materiału procesowego na gruncie nowego przepisu jest więc prokurator. Ustawa nie określa jednak, w jakiej formie ma być wydana decyzja o dopuszczeniu materiału z kontroli. Problem pojawia się m.in. w wyroku SN z 16 października 2012 r., w którym czytamy:

> Dla oceny dopuszczalności dowodu z materiałów z kontroli operacyjnej, o której mowa w art. 19 ust. 1 ustawy z 1990 r. o Policji, istotny jest kierunek tego dowodu. Jeśli jego celem jest wykazanie niewinności oskarżonego lub uzyskanie dowodów świadczących na jego korzyść, to może być on przeprowadzony niezależnie od faktu, że wobec tego oskarżonego nie wydano postanowienia w trybie art. 19 ust. 3 tej ustawy, ani też określonego w art. 19 ust. 15c postanowienia o zgodzie następczej[105].

Gdy więc prokurator nie wystąpi o zgodę następczą, we wskazanych powyżej przypadkach sąd i tak będzie uprawniony do skorzystania z materiałów, a niepodjęcie przez prokuratora stosownych czynności będzie oceniane przez pryzmat art. 168a kpk. Dlatego taki dowód nie będzie mógł być uznany za niedopuszczalny (ze względu na bierność prokuratora w opozycji do art. 168b kpk), a sąd będzie mógł przeprowadzić dowód na korzyść oskarżonego[106].

Unormowanie odchodzące od zgody następczej wydawanej przez sąd, a cedujące ją na prokuratora, budzi w doktrynie duże wątpliwości. Po pierwsze, jest to przepis wprost odnoszący się do czynności operacyjnych, które w całości są uregulowane poza kpk i do których nie odnoszą się gwarancje procesowe. Po drugie, daleko idącą zmianą jest również to, że wcześniejsze unormowanie pozwalało na kontrolę sądu w zakresie zgody pierwotnej oraz następczej, co było zasadne ze względu na zagwarantowaną niezawisłość tego organu i obowiązek rzetelnego rozpatrzenia sprawy – również w kon-

[102] K. Boratyńska, *Wokół problematyki związanej z wykorzystaniem dowodowym materiałów operacyjnych*, w: *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu – nowoczesne technologie i praca operacyjna*, L. Paprzycki, Z. Rau (red.), Warszawa 2009, s. 152.

[103] P. Czarnecki, *Czynności operacyjno-rozpoznawcze a postępowanie*…, s. 125; M. Klejnowska, *Prawnodowodowe skutki*…, s. 86.

[104] Tamże.

[105] Wyrok SN z 16 X 2012 r., sygn. akt V KK 414/11, LEX nr 1226789.

[106] Pisze o tym M. Kurowski w: *Kodeks postępowania*…, s. 179–180.

tekście wydania zgody następczej. Nie sposób nie zgodzić się z poglądami doktryny, że aktualne unormowanie art. 168b kpk wraz z jego nowym brzemieniem może wręcz zachęcić służby do szerszego stosowania kontroli operacyjnej, gdyż norma tego artykułu ułatwia jej późniejszą legalizację[107].

Przez to, że ustawodawca nie zdecydował się na szczegółowe dookreślenie analogicznych regulacji wobec innych metod operacyjnych, podczas których może dojść do dopuszczenia materiału dowodowego zgromadzonego z naruszeniem przepisów ustawowych, należy przychylić się do stwierdzenia, że standard konstytucyjny dotyczący eliminacji materiału nielegalnego nie został zrealizowany[108].

Ostatnią z poruszonych kwestii dotyczących dopuszczalności dowodów uzyskanych z naruszeniem prawa będzie ewentualna konwalidacja i konwersja czynności w celu jej dalszego dopuszczenia w postępowaniu. Jest to możliwe w przypadkach, w których nie dochodzi do sytuacji niedopuszczalnych – w sensie zabronionych w prawie procesowym – ze względu na bezwzględną nieważność czynności (takie czynności nie mogą być konwalidowane)[109]. Konwalidacja jako zjawisko usuwania wadliwości czynności dowodowych lub skutków tej wadliwości służy wypełnieniu funkcji gwarancji praworządności. Ma to znaczenie szczególnie w aspekcie uprawnień i obowiązków organów procesowych, do których zadań należy usuwanie dostrzeżonych uchybień procesowych i naprawianie ewentualnych wadliwych czynności[110].

Ogólne reguły konwalidacji mogą więc zostać zastosowane do oceny legalności czynności operacyjnych. A. Taracha uznaje za konwalidację m.in. przejście do kolejnego etapu rozpatrzenia sprawy (gdy np. brak zgody prokuratora będzie konwalidowany przez postanowienie sądu). Podkreśla jednak, że najważniejsza jest ocena wagi problemu, gdyż dostrzeżenie braków lub uchybień może być utrudnione ze względu na wysoki stopień utajnienia akt sprawy. Odpowiedni dostęp do całości akt i materiałów będzie zawsze skutkował większą szansą na kontrolę i uniknięcie jej iluzoryczności[111]. Rozważania autora dotyczące problemów w przypadku metod zakreślonych tylko dla poszczególnego katalogu przestępstw pozostają nadal aktualne w obecnym stanie prawnym i pokrywają się z problematyką poruszaną powyżej[112].

A. Taracha porusza również problem konwersji czynności operacyjnych, gdy jedna czynność niespełniająca wymogów ustawowych może je spełniać w przypadku konwersji na inną czynność. Dla przykładu, może dojść do sytuacji, w której czynność o węższym zakresie przedmiotowym (np. przesyłka niejawnie nadzorowana) w przypadku przekroczenia swojego ustawowego zakresu „zmieści się" w przesłankach czynności szerszej, np. kontroli operacyjnej. Możliwość konwersji jednak w tym przypadku nigdy nie nastąpi, ze względu na ustawowy wymóg wydania postanowienia przez sąd w przypadku kontroli operacyjnej.

Drugim przykładem tego autora jest sytuacja, w której równolegle z czynnością wadliwą ze względu na zakres przedmiotowy, np. prowokacją policyjną, następuje prawidłowa kontrola operacyjna. Taka sytuacja jest do zaakceptowania, gdyż wadliwość

[107] Wspominają o tym K.T. Boratyńska i M. Królikowski w: *Kodeks postępowania karnego*..., s. 441–442.

[108] P. Czarnecki, *Czynności operacyjne u wrót procesu*..., s. 186.

[109] R. Kmiecik, *Konwalidacja i konwersja wadliwych dowodów w procesie karnym*, „Państwo i Prawo" 1989, nr 5, s. 94–95.

[110] Tamże, s. 93.

[111] A. Taracha, *Czynnościoperacyjno-rozpoznawcze: aspekty*..., s. 280–281.

[112] Tamże, s. 281.

jednej czynności nie może przemawiać za uznaniem wadliwości drugiej, ponieważ czynności te, choć stosowane jednocześnie, są zlecane w odrębnych postępowaniach[113].

Doktryna i orzecznictwo wykształciły na przestrzeni lat mechanizmy ewentualnej eliminacji materiału wadliwego i niedopuszczenie do usunięcia z podstawy ustaleń faktycznych dowodów o charakterze znaczącym dla sprawy. Ostatnie zmiany ustawodawcze trudno jednak uznać za wystarczające, szczególnie w przypadku transponowania zaleceń TK w zgodzie z orzeczeniem o sygn. K 23/11 i ostatnią nowelizacją procedury karnej. TK w najbliższym czasie będzie badał skargi wniesione przez RPO oraz NRA dotyczące ustaw policyjnych, a dodatkowo skargę RPO na art. 168a kpk. Najbliższe miesiące mogą więc doprowadzić do sytuacji całkowitej zmiany analizowanych powyżej zakresów czynności operacyjnych.

[113] A. Taracha, *Czynnościoperacyjno-rozpoznawcze: aspekty*..., s. 282–284.

Krystian Radziejewski

Cyberbezpieczeństwo w administracji rządowej w Rzeczypospolitej Polskiej[1]

Rozdział I. Teleinformatyczna i cybernetyczna infrastruktura krytyczna

Polska jest krajem, w którym sprawna infrastruktura krytyczna (dalej: IK) staje się elementem coraz bardziej istotnym dla bezpieczeństwa państwa. Niezakłócone działanie tej infrastruktury przekłada się na pracę ważnych podmiotów dla funkcjonowania państwa: przemysłowych, administracyjnych czy logistycznych oraz odbiorców ich usług. Ten stan uzależnienia musi być więc objęty szczególną ochroną, aby nie zahamować sprawności państwa i bezpieczeństwa jego obywateli.

1.1. Systematyzacja infrastruktury krytycznej

Podstawowym źródłem prawnym dotyczącym infrastruktury krytycznej jest *Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym*[2]. W zakresie cyberbezpieczeństwa najistotniejszymi jej elementami jest Rządowe Centrum Bezpieczeństwa (dalej: RCB) jako jednostka opiniodawczo-monitorująca stan bezpieczeństwa polskiej infrastruktury krytycznej, rzeczywistej i sieciowej, na podstawie zadań uwzględnionych w art. 11–11a ustawy o zarządzaniu kryzysowym. Bardzo ważnym dokumentem dotyczącym IK jest *Narodowy Program Ochrony Infrastruktury Krytycznej*[3]. Jest on adresowany zarówno do organów administracji rządowej, jak i operatorów IK jako podstawowych podmiotów wykorzystujących założenia tego programu. Może być także kierowany do środowisk naukowych, przemysłowych, a także do społeczeństwa, gdyż większość dokumentacji jest jawna i odpowiednio przygotowana, aby mogła być używana przez jak najszersze kręgi odbiorców[4].

Chcąc przyjrzeć się cyberbezpieczeństwu IK, powinno się przeanalizować wszystkie systemy włączone do tej infrastruktury. Celem niniejszej pracy jest omówienie przede wszystkim systemów łączności i sieci teleinformatycznych, które zapewniają komunikację między poszczególnymi obiektami i decyzyjność na możliwie wysokim poziomie.

Krytyczna infrastruktura teleinformatyczna (dalej: KITI) została poddana kwalifikacji przez specjalnie powołany zespół jako urządzenia i usługi powiązane funkcjonalnie, kluczowe dla bezpieczeństwa państwa i obywateli[5]. Nieprawidłowe działanie lub

---

[1] Fragmenty pracy magisterskiej pt. *Cyberbezpieczeństwo w administracji rządowej w Rzeczypospolitej Polskiej*, która zajęła III miejsce w konkursie Szefa ABW na najlepszą pracę magisterską/licencjacką z dziedziny bezpieczeństwa wewnętrznego (edycja 2015/2016). Autor jest absolwentem Uniwersytetu Warszawskiego, Wydziału Dziennikarstwa i Nauk Politycznych. Redakcja dokonała niezbędnych poprawek oraz zmian numeracji materiałów ilustracyjnych i przypisów (przyp. red.).

[2] Tekst jednolity: Dz.U. z 2017 r. poz. 209.

[3] *Narodowy Program Ochrony Infrastruktury Krytycznej 2015* [online], http://rcb.gov.pl/wp-content/uploads/Narodowy-Program-Ochrony-Infrastruktury-Krytycznej-20151.pdf [dostęp: 26 IV 2016].

[4] Tamże, s. 15–17.

[5] Zespół ds. Krytycznej Infrastruktury Teleinformatycznej został powołany 9 XI 2004 r. na podstawie decyzji Przewodniczącego Kolegium ds. Służb Specjalnych.

uszkodzenie systemów bądź urządzeń może spowodować istotne zagrożenie życia lub zdrowia ludzi, interesów obronności oraz bezpieczeństwa wewnętrznego albo może narazić te interesy na znaczną szkodę. Ministrowie odpowiedzialni za systemy zaliczane do IK są gwarantem zaangażowania władz państwowych w sprawny proces budowania bezpieczeństwa wewnętrznego państwa[6]. Odpowiedzialność za ochronę IK spoczywa na ministerstwach oraz służbach specjalnych, straży i siłach porządkowych państwa. Ideą tej ochrony jest zapewnienie ciągłości działania, funkcjonalności i integralności IK, aby zapobiec zagrożeniom, różnego rodzaju ryzyku lub powstawaniu słabych punktów IK, a także szybko zneutralizować zagrożenia spowodowane atakami lub awarią i odtworzyć uszkodzoną albo zniszczoną infrastrukturę[7].

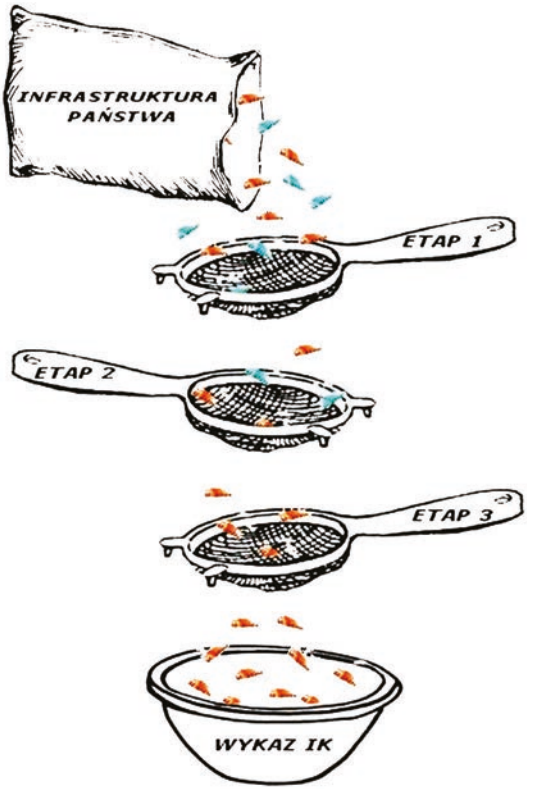
Konkretne obiekty zaliczone do infrastruktury krytycznej, wyłonione w procesie identyfikacji, są katalogowane w niejawnej dokumentacji na różnych szczeblach administracji publicznej. Sam proces identyfikacji obiektów włączonych do IK jest przeprowadzany i aktualizowany przez RCB we współpracy z ministerstwami i kierownictwem administracji centralnej według następujących kryteriów[8]:

1) kryterium systemowe – to systematyka, według której różne obiekty mogą zostać zaliczone do IK. Wykorzystuje się tu: analizę funkcji i instalację i usług oferowanych przez obiekty,
2) kryterium przekrojowe –
3) to spis parametrów, które odnoszą się do konsekwencji, jakie zniszczenie lub uszkodzenie danego obiektu może za sobą nieść. Przykładowo kryteria te obejmują: możliwość ewakuacji, ofiary w ludziach, skażenie środowiska, stratę unikatowej usługi czy skutki międzynarodowe.

Wymienione kryteria są następnie wykorzystywane do identyfikacji IK umożliwiającej skatalogowanie obiektów należących do niej, a także podjęcie procedur i regulacji ich ochrony. Identyfikacja odbywa się w trzech etapach (rys. 1):

1) wstępna selekcja obiektów, usług instalacji i urządzeń, które teoretycznie mogłyby kwalifikować się w określonych systemach jako IK. Wobec nich stosuje się kryteria systemowe, odpowiednio dla systemu IK,
2) dalsze sprawdzenie, czy analizowany podmiot jest ważny dla bezpieczeństwa państwa oraz czy jego istnienie i funkcjonowanie pozytywnie wpływa na pracę administracji, biznesu i instytucji. Wobec tego typu podmiotów należy także odnieść się do art. 3 pkt 2 ustawy o zarządzaniu kryzysowym, to znaczy sprawdzić, czy spełniają one wymóg postawiony przez ustawę,
3) analiza skutków potencjalnej blokady funkcjonowania podmiotu bądź jego zniszczenie oraz efekty, jakie mogą one przynieść dla bezpieczeństwa państwa i jego obywateli. Na tym etapie stosuje się kryteria przekrojowe[9].

[6] *Narodowy Program Ochrony Infrastruktury Krytycznej*…, s. 17.
[7] Infrastruktura krytyczna [online], http://rcb.gov.pl/infrastruktura-krytyczna/ [dostęp: 26 IV 2016].
[8] Szczegółowe definicje są opisane w niejawnych załącznikach do programu.
[9] *Narodowy Program Ochrony Infrastruktury Krytycznej*…, s. 13–14.



Rys. 1. Identyfikacja infrastruktury krytycznej.

Źródło: *Narodowy Program Ochrony Infrastruktury Krytycznej 2015* [online], http://rcb.gov.pl/wp-content/uploads/NPOIK-dokument-g%C5%82%C3%B3wny.pdf, s. 14 [dostęp: 26 IV 2016].

1.2. Systemy infrastruktury krytycznej a cyberbezpieczeństwo

Po przeprowadzeniu inwentaryzacji systemów i sieci teleinformatycznych oraz identyfikacji IK wskazuje się na elementy[10], które klasyfikują się do grupy infrastruktury teleinformatycznej o znaczeniu krytycznym, tj.:

- systemy i sieci istotne dla prowadzenia statutowej działalności organów administracji publicznej oraz wymiany danych i informacji w siłach zbrojnych i rejestrach państwowych, czyli wyróżnienie warstwy aplikacji (oprogramowania, usług itd.),
- sieci łączności telekomunikacyjnej, w tym operatorzy sieci telekomunikacyjnych, które są wykorzystywane przez administrację publiczną i armię, czyli wyróżnienie drugiej warstwy mediów transmisyjnych (np. linie telekomunikacyjne).

[10] *Infrastruktura Teleinformatyczna Państwa*, B. Chojnacki (red.) [online], https://www.itl.waw.pl/publikacje_pliki/statutowe/pliki/505.pdf, s. 86–88 (podrozdział: *System Informacyjny o infrastrukturze krytycznej państwa*) [dostęp: 26 IV 2016].

Analizując destrukcyjny wpływ zagrożeń na infrastrukturę teleinformatyczną w kraju, należy stwierdzić, że przewidywane obiekty i miejsca IK zagrożone bezpośrednio to przede wszystkim obiekty i miejsca lokalizacji kluczowych elementów – urządzeń i systemów telekomunikacyjnych, takich jak:

- centra utrzymywania i zarządzania infrastrukturą teleinformatyczną:
  - obejmujące administracyjnie miasta i aglomeracje miejskie;
  - przekładające się na prywatne przedsiębiorstwa dostarczające usługi telekomunikacyjne na terenie miast i aglomeracji;
- stacje bazowe i satelitarne;
- centrale przedsiębiorców telekomunikacyjnych wspierających organy administracji publicznej oraz straże i służby biorące udział w fazach zarządzania kryzysowego;
- sieci łączności i lokalizacje przebiegu linii telekomunikacyjnych, międzycentralowych i podstawowych;
- serwery zarządzające bazami danych i systemami, w tym bazy danych krytycznych[11];
- inne obiekty telekomunikacyjne, np. koncentratory, węzły dostępowe czy stacje czołowe.

Można więc się domyślać, że do powyższej listy systemów telekomunikacyjnych mogą należeć dostawcy usług telekomunikacyjnych, tacy jak Telekomunikacja Polska SA, Exatel SA, Telekomunikacja Kolejowa sp. z o.o., Netia Telekom czy niektórzy operatorzy sieci GSM; dostawcy sieci telekomunikacyjnych, jak Energo-Tel SA[12], lub dostawcy zróżnicowanych technologicznie systemów łączności i komunikacji radiowej dla służb bezpieczeństwa publicznego, ratownictwa i straży.

Systemy teleinformatyczne IK są charakterystycznym elementem infrastruktury krytycznej ze względu na możliwość prowadzenia komunikacji i procesów zarządzania wobec innych systemów. Utrudnieniem staje się prywatyzacja podmiotów IK, które często muszą wybierać między własnym bezpieczeństwem a ekonomią i zyskiem[13]. W związku z tym ochrona systemów łączności powinna zakładać szczególne środki i procedury do skutecznego zabezpieczenia ich prawidłowego funkcjonowania. W tej dziedzinie siły łączą między innymi zespoły naukowe NASK i zespoły CERT, które na bieżąco monitorują stan IK pod kątem cyberbezpieczeństwa, definiują nowe zagrożenia i reagują w przypadku wystąpienia ataków lub awarii[14]. Zespoły reagowania na zagrożenia i incydenty w cyberprzestrzeni wykorzystują różną gamę platform, oprogramowania i usług do realizacji wyznaczanych im zadań, a także współpracują z organizacjami międzynarodowymi, które je wspierają. Przykładem takiej organizacji jest Europejska Agencja ds. Bezpieczeństwa Sieci i Informacji (ENISA)[15].

---

[11] Wśród baz danych krytycznych dla administracji publicznej Zespół ds. KITI wyróżnia bazy PESEL, REGON, KEP, CEPIK, KATASTER, TERYT, rejestry sądowe.

[12] *Infrastruktura Teleinformatyczna Państwa*…, s. 11, 61.

[13] *O bezpieczeństwie infrastruktury krytycznej*, „Systemy alarmowe" [online], 2010 r., http://systemyalarmowe.com.pl/index.php/pl/relacje/1189-o-bezpieczestwie-infrastruktury-krytycznej [dostęp: 28 IV 2016].

[14] M. Pyznar, T. Włodarczyk, *Ochrona Teleinformatyczna Infrastruktury Krytycznej*, „CIIP focus" [online] 2012, nr 1, s. 11–12, http://rcb.gov.pl/wp-content/uploads/ciip-focus-1.pdf [dostęp: 27 IV 2016].

[15] Organizacja ENISA dostarcza rekomendacje i rozwiązania w cyberbezpieczeństwie, wspiera rozwój legislacji i jej implementacji w życie i współpracuje z zespołami reagowania w obrębie całej Unii Europejskiej, zob. https://www.enisa.europa.eu/ [dostęp: 28 IV 2016].

Ochrona IK zachodzi również na poziomie operacyjnym. Jednostką wspierającą tę ochronę jest RCB, którego zadaniem jest wyszukiwanie słabych punktów wśród podmiotów IK w systemach łączności i sieci teleinformatycznych oraz informowanie ich właścicieli o niedociągnięciach. Rządowe Centrum Bezpieczeństwa zajmuje się również opracowywaniem tzw. *Best practices* w Narodowym Programie Ochrony IK, które powinny pomóc przygotować lepsze warunki ochrony tej infrastruktury. Trzecim rodzajem wsparcia jest udział RCB we współtworzeniu Polityki Ochrony Cyberprzestrzeni Rzeczpospolitej Polskiej, a także definiowanie zagrożeń cyberprzestrzeni, wskazywanie jednostek odpowiedzialnych za monitorowanie cyberbezpieczeństwa administracji publicznej oraz koordynowanie operacji w przypadku cyberzagrożeń, zamieszczone w Krajowym Planie Zarządzania Kryzysowego. Czwartym – współpraca z tymi podmiotami, które chcą współtworzyć cyberbezpieczeństwo[16].

Rozdział II. Zarządzanie cyberbezpieczeństwem w ramach krytycznej infrastruktury teleinformatycznej

Obecnie sieci teleinformatyczne nabrały zupełnie nowego znaczenia, nie są jedynie środkiem komunikacyjnym pomiędzy współpracującymi organami. Całą sieć informatyczną wykorzystywaną w administracji publicznej można porównać do układu nerwowego organizmu[17], który spaja jego funkcje życiowe i podtrzymuje koordynację jego poszczególnych części. Centralny układ nerwowy zbiera dane docierające do niego przez narządy, zarówno z wewnątrz organizmu[18], jak i z otoczenia, analizuje je i dzięki temu gromadzi wiedzę, która pomaga podjąć decyzję o zachowaniu całego ciała[19]. Co istotne – organizm nie jest w stanie produktywnie istnieć bez układu nerwowego bądź z uszkodzonym systemem. Podobnie jak układ nerwowy, sieci teleinformatyczne łączą ośrodek centralny z ośrodkami terenowymi, które przekazują informacje o świecie ośrodkowi centralnemu. Dlatego przywiązuje się duże znaczenie do ich sprawnego działania. (…)

2.1. Klasyfikacja elementów krytycznie ważnych dla cyberbezpieczeństwa

Współcześnie administracja rządowa RP intensywnie wykorzystuje technologie informatyczne do rozszerzania swojego potencjału w sprawnym zarządzaniu państwem. Ułatwiają one komunikację na linii obywatel – administracja oraz usprawniają pracę przedstawicielom administracji publicznej. Są to środowiska, dzięki którym odbywa się zarządzanie zasobami i danymi na szczeblu rządowym. Podstawą działania jest zbieranie, gromadzenie, przetwarzanie, przesyłanie i analizowanie informacji zarówno przez jednostki rządowe, terytorialne, jak i przez inne organy władzy publicznej w ramach przepisów wewnętrznych. Dane, które są przetwarzane w ten sposób, określa się mianem

[16] *Ochrona Teleinformatyczna Infrastruktury Krytycznej*…, s. 9.

[17] Cyberprzestrzeń została porównana do układu nerwowego m.in. w dokumencie strategicznym USA, *National Strategy to Secure Cyberspace*, Department of Homeland Security, luty 2003. Dokument dostępny pod adresem https://www.dhs.gov/national-strategy-secure-cyberspace.

[18] E. Niewiadomska *Systemy informacyjne administracji rządowej*, „Zeszyty naukowe Uniwersytetu Szczecińskiego", „Studia Informatica" 2012, nr 29, s. 220.

[19] J. Kendall, D.O. Fulenwinder, *Six Sigma, e-commerce pose new challenges*, „Quality Progress" 2000, nr 33; fragment tekstu można odnaleźć na stronie http://docplayer.pl/3615408-Kompleksowa-organizacja-gromadzenia-i-analizy-danych.html [dostęp: 24 IV 2016].

„danych administracyjnych”[20]. Na podstawie modelu sieciowego OSI[21] do środowisk, których praca jest oparta na przetwarzaniu danych, działających w ramach resortów, administracji rządowej i terytorialnej, można zaliczyć wymienione poniżej elementy[22].

Repozytoria danych rejestrowych – działają jako specjalne bazy danych przeznaczone do przetwarzania i gromadzenia danych osobowych, obiektów materialnych, spisów, zdarzeń społecznych, ekonomicznych lub innych. Ich gromadzenie jest niezbędne jednostkom administracji publicznej do realizacji zadań publicznych, np. kontroli lub nadzoru ze strony państwa nad działalnością wybranej grupy podmiotów. Zbierane informacje są z reguły wrażliwe dla bezpieczeństwa wewnętrznego państwa lub bezpieczeństwa osobowego obywatela. Przykładem rejestru danych jest Krajowy Rejestr Sądowy, rejestr REGON czy PESEL[23].

e-Usługi – to zbiory usług informatycznych pośredniczących między potrzebą obywatela a ofertą podmiotu administracji publicznej, dostępne w sieci publicznej, tzn. w Internecie. Te usługi są udostępniane na platformie ePUAP. Dzięki tej platformie można skorzystać z dokumentów i pism urzędowych ułatwiających łączność obywatela z urzędem, nawet jeśli ten obywatel przebywa w dowolnym miejscu na świecie[24].

Serwisy i serwery bankowe – to środowiska otwartej i zamkniętej komunikacji banków między sobą, a także komunikacji z klientem. Wśród nich znajdują się platformy płatności cyfrowej, serwery rozliczeń międzybankowych, ochrony przed fraudami, serwisy obsługi klientów oraz rozwiązania dotyczące zarządzania ryzykiem braku zgodności. Wśród nich można znaleźć głównie systemy prywatnych przedsiębiorstw bezpieczeństwa bankowego[25].

Systemy ERP – służą do integracji zasobów, funkcji i działów w firmie dzięki korzystaniu ze wspólnych baz danych. Wszystkie procesy prowadzone podczas pracy systemów oraz informacje są gromadzone i nadzorowane w jednym źródle, dzięki czemu jest ułatwione zarządzanie przedsiębiorstwem. Te systemy łączą zasoby magazynowe, dział handlowy i dział produkcyjny, co pozwala na kontrolowanie aktualnie posiadanych środków, zwiększenie przepustowości produkcji, a także zwiększenie skuteczności przedstawicieli w kontakcie z klientem[26]. W administracji publicznej są one wykorzystywane między innymi w służbach mundurowych z zastosowaniem na przykład systemów Comarch[27].

---

[20] Definicja systemów informacyjnych administracji publicznej zob. http://www.encyklopedialesna.pl/hasla/index/1051 [dostęp: 12 V 2016].

[21] O modelu sieciowym OSI (opisującym strukturę komunikacji sieciowej – przyp. red.) zob. *Założenia Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej* [online], https://mc.gov.pl/files/zalozenia_strategii_cyberbezpieczenstwa_v_final_z_dnia_22-02-2016.pdf, s. 12–13 [dostęp: 12 V 2016] oraz http://searchnetworking.techtarget.com/definition/OSI [dostęp: 12 V 2016].

[22] Opracowano na podstawie:

– *Założenia Strategii Cyberbezpieczeństwa dla Rzeczypospolitej Polskiej*…, s. 12,

– *Bezpieczeństwo teleinformatyczne administracji państwowej, program ochrony cyberprzestrzeni RP*, prezentacja multimedialna, Departament Bezpieczeństwa Teleinformatycznego ABW, zastępca dyrektora Departamentu Marcin Ludwiszewski, 2008 r.

– *Infrastruktura Teleinformatyczna Państwa*…

[23] J. Oleński, *Rejestry administracyjne i systemy katastralne w infrastrukturze informacyjnej państwa*, Wisła-Malinka, 7–9 września 2005 r – prezentacja [online], http://www.wodgik.katowice.pl/www/pobierz/wydarzenia/2005/Olenski.pdf, s. 1–6 [dostęp: 14 V 2016].

[24] https://mac.gov.pl/uslugi-elektroniczne-udostepniane-na-epuap-moga-miec-charakter-uslug-centralnych-badz-lokalnych [dostęp: 14 V 2016].

[25] Opracowano przy wykorzystaniu http://www.bsb.pl/sektor-bankowy.html [dostęp: 14 V 2016].

[26] O systemach ERP zob. http://www.microsoftdynamicserp.pl/system-erp/co-to-jest-system-erp/ [dostęp: 14 V 2016].

[27] Comarch w administracji publicznej [online], http://www.comarch.pl/administracja-publiczna/ [dostęp: 14 V 2016].

Bazy danych – to środowiska gromadzenia danych w zbiory rekordów. Są one oparte na różnych strukturach, systemach i usługach (np. MySQL), dzięki którym mogą być wykorzystywane do zapisywania, aktualizacji, zmiany, powielania itd. różnych zasobów danych. W administracji publicznej służą do przechowywania np. informacji statystycznych, dotyczących demografii, gospodarki, stanu środowiska i innych. Wśród nich można wymienić Bilans Kapitału Ludzkiego lub DanePubliczne.gov.pl[28].

Serwisy i witryny internetowe resortów – to przede wszystkim środowiska kontaktu obywatela (lub klienta) z podmiotem administracji rządowej. Zawierają informacje dostępne publicznie, charakterystyczne dla przeglądanego resortu. Stanowią także źródło bieżących komunikatów ogłaszanych przez podmiot oraz umożliwiają kontakt obywatela (lub klienta) z podmiotem, np. za pośrednictwem e-maili. Można zaliczyć do nich wszystkie witryny w domenie gov.pl oraz strony internetowe władz terytorialnych i samorządowych.

Aplikacje rządowe i serwery aplikacji – to narzędzia służące komunikacji z obywatelem. Przetwarzają dane w taki sposób, aby ułatwiać wdrażanie między innymi projektów i aplikacji webowych. Różnią się od serwerów internetowych innym sposobem obsługi aplikacji, gdyż odbywają się na innym poziomie warstwy programowej. Obsługują transakcje sieciowe dostarczane przez producenta platformy, z której korzysta użytkownik, wspierają przetwarzanie zasobów i prowadzenie operacji na dużą skalę – dla dużych przedsiębiorstw[29]. Są wykorzystywane np. w systemie CEPIK[30].

Systemy SCADA – są stworzone do kontroli, sterowania i akwizycji danych oraz systemów technologicznych i pomiarowych typu PLC lub RTU, które są wykorzystywane do automatyzacji procesu technologiczno-produkcyjnego w przemyśle, transporcie, teletransmisji, medycynie i innych sektorach gospodarki państwowej. Te systemy przede wszystkim zbierają dane z urządzeń, wizualizują ich statusy, sterują operacjami urządzeń, alarmują i archiwizują dane.

Sieci resortowe, sieci wewnętrzne IK, sieci do komunikacji niejawnej – w tej grupie są zawarte wszystkie sieci wewnętrzne, tzn. wydzielone z sieci publicznej, chronione przed dostępem z zewnątrz lub VPN. Zawierają w sobie komplet systemów potrzebnych do autonomicznego funkcjonowania, możliwie bez łączenia ich z wyjściami do sieci publicznej. Są one traktowane jako systemy łączności specjalnej do przekazywania informacji niejawnych, których ujawnienie mogłoby naruszyć bezpieczeństwo lub renomę firmy lub resortu. Często są objęte specjalnymi systemami kryptograficznymi[31]. Przykładem tych systemów jest Polwan, Sieć Łączności Rządowej (SŁR) czy Pesel-Net.

Systemy bezpieczeństwa – to systemy zarządzania dostępem podmiotów osobowych i nieosobowych do odpowiednich zasobów sieci. Zawierają w sobie systemy wczesnego ostrzegania i monitorowania ruchu w sieci, systemy reagowania, firewalle, sondy analityczne, środowiska typu HoneyPot[32], systemy ochrony kryptograficznej i inne. Przykładem jest ARAKIS-Gov.

---

[28] Bazy danych i witryna internetowa DanePubliczne.gov.pl, https://danepubliczne.gov.pl/ [dostęp: 14 V 2016].

[29] Na temat serwerów aplikacyjnych zob. http://www.computerworld.pl/news/283589/Serwery.aplikacyjne.Java.html [dostęp: 14 V 2016].

[30] Assecco i opis systemu CEPIK zob. https://pl.asseco.com/sektory/instytucje-publiczne/administracja-centralna/ [dostęp: 14 V 2016].

[31] J. Matyszak, *Funkcjonowanie systemu telekomunikacyjnego administracji publicznej*, https://www.bbn.gov.pl/download/1/1003/funkcjonowaniesystemu.pdf, s. 81–83 [dostęp: 14 V 2016].

[32] Więcej o HoneyPot zob. http://www.computerworld.com/article/2573345/security0/honeypots--the-sweet-spot-in-network-security.html [dostęp: 14 V 2016].

Hurtownie danych administracyjnych – to rejestry gromadzące zintegrowane informacje, które pochodzą z rejestrów systemów oraz z innych źródeł, wykorzystywane do dalszej analizy. Łączą dane, integrując je z różnych źródeł i przechowując historię ich zmian. Cechują się dużą wydajnością przy przetwarzaniu informacji. Są one systemami wspierającymi rejestry danych, dostarczają proste raportowanie zaistniałych zmian bądź złożone i interaktywne analizy informacji, różne metody wyświetlenia wyników, aż do złożonych systemów wykorzystujących wzorce czy regularność klastrowania w dużych bazach danych. Te systemy są szybkie i pozwalają na interaktywną współpracę z innymi systemami lub innymi podmiotami [33]. Przykładem jest system PLOUG.

2.2. Kwalifikacja cybernetycznej infrastruktury krytycznej

Największe znaczenie dla wymienionych systemów informatycznych ma jakość projektu systemów oraz poziom ich zabezpieczeń cybernetycznych uniemożliwiający nieuprawione skorzystanie z nich lub włamanie się do nich. Część z tych systemów ma także szczególne znaczenie w budowaniu bezpiecznego, ciągłego i spójnego zarządzania cyberprzestrzenią. Stąd ich użytkowanie jest obwarowane szczególnymi przepisami.

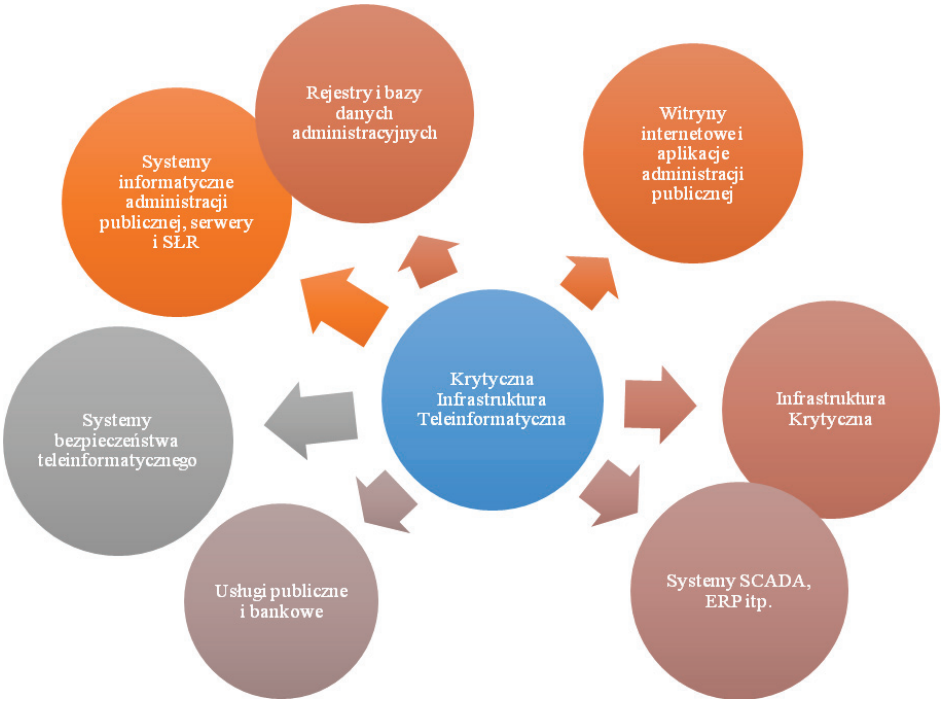
W myśl *Rządowego programu ochrony cyberprzestrzeni RP na lata 2011–2016* krytyczna infrastruktura teleinformatyczna jest częścią składową cyberprzestrzeni, która dotyczy systemów informatycznych infrastruktury krytycznej[34]. Zawiera ona w sobie systemy i sieci teleinformatyczne wrażliwe dla funkcjonowania gospodarki i bezpieczeństwa państwa, tzn. takie, które odnoszą się do ogólnej definicji infrastruktury krytycznej jako zbioru rzeczywistych i cybernetycznych systemów podlegających możliwości analizy przez pryzmat kryteriów identyfikacji IK. Krytyczna infrastruktura teleinformatyczna to systemy informacyjne w cyberprzestrzeni o uporządkowanych elementach, które charakteryzują się powiązaniami i relacjami o strategicznym znaczeniu, które są niezbędne do podstawowego funkcjonowania gospodarki i współczesnego państwa[35]. Warto więc rozważyć, czy wydzielić z KITI Cybernetyczną Infrastrukturę Krytyczną (dalej: CIK), która została wcześniej sprecyzowana i przedstawiona w tym rozdziale, ze względu na to, że w cyberprzestrzeni funkcjonuje ona jako odpowiednik cyfrowej IK oraz podmiotów administracji publicznej w Internecie. W rozumieniu ogólnym CIK można podzielić na infrastrukturę otwartą i zamkniętą. Infrastruktura otwarta dotyczy systemów i sieci, które umożliwiają dostęp z sieci publicznych, np. serwisy informacyjne, e-usługi, aplikacje, platformy płatnicze banków. Infrastruktura zamknięta natomiast to zbiór sieci i systemów wyodrębnionych z sieci publicznych, jak sieci resortowe oraz wewnętrzne sieci obiektów IK. Współczesny poziom informatyzacji przemysłu, administracji, usług publicznych oraz IK wymaga również zwrócenia uwagi na znaczenie CIK jako cybernetycznej warstwy KITI ze względu na skalę unowocześniania technologii i poziomu uzależnienia obiektów od informatyki.

[33] Materiały szkoleniowe o Data Warehouse zob. www.ploug.org.pl/konf_03/materialy/pdf/27_Pentacomp_IACS.pdf [dostęp: 15 V 2016].

[34] *Rządowy program ochrony cyberprzestrzeni Rzeczypospolitej Polskiej na lata 2011–2016* [online], Warszawa 2010, Ministerstwo Spraw Wewnętrznych i Administracji, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Poland_Cyber_Security_Strategy.pdf, s. 12 [dostęp: 14 V 2016].

[35] Infrastruktura krytyczna, witryna internetowa Rządowego Centrum Bezpieczeństwa, Krytyczna infrastruktura teleinformatyczna http://rcb.gov.pl/infrastruktura-krytyczna/ [dostęp: 14 V 2016].

Praca systemów teleinformatycznych może zostać zakłócona, podsłuchana lub zatrzymana (np. przez zniszczenie), może przekładać się na zagrożenie mienia, danych osobowych, zdrowia i życia obywateli, a także na bezpieczeństwo pozostałych systemów IK. Ochrona CIK jest wyzwaniem, przed którym stoi rząd RP. Musi on wykazać się sprawnym kierowaniem (np. przez system zarządzania cyberbezpieczeństwem) i umiejętnością przeciwdziałania dysfunkcjom wywołanym przez awarie, cyberprzestępczość, cyberterroryzm[36] oraz infiltrację. W ochronę systemów sieci teleinformatycznych IK są zaangażowane podmioty administracji rządowej, przede wszystkim MSWiA, MON, szefowie ABW i SKW oraz przedsiębiorstwa prywatne prowadzące obiekty IK, które również są uczestnikami w zarządzaniu kryzysowym cyberprzestrzeni.



Rys. 2. Model struktur składowych zakwalifikowanych jako elementy Cybernetycznej Infrastruktury Krytycznej (propozycja autora).

Źródło: Opracowanie własne.

Na rys. 2 przedstawiono kwalifikację różnych systemów informatycznych jako cybernetycznych składowych KITI oraz rozłożenie odpowiedzialności za funkcjonowanie gospodarki i bezpieczeństwa państwa, w tym za bezpieczeństwo teleinformatyczne. Posługując się identyfikacją IK i jej kryteriami, można stwierdzić, że wśród środowisk i usług przestrzeni cybernetycznej jest możliwe wskazanie, które środowiska, systemy,

[36] *Narodowy Program Ochrony Infrastruktury Krytycznej 2013*, załącznik 1: *Charakterystyka systemów infrastruktury krytycznej* [online], http://rcb.gov.pl/wp-content/uploads/NPOIK-załącznik-1.pdf, pkt 2.8, s. 67 [dostęp: 14 V 2016].

usługi, witryny i repozytoria podlegają szczególnemu ryzyku[37]. Wspomniana odpowiedzialność to wynik rozproszenia kompetencji i odpowiedzialności poszczególnych podmiotów w polskim systemie prawnym, a szczególnie w ustawach określających różne kategorie i poziomy tajemnicy chronionej przez prawo, np. tajemnicy bankowej, danych osobowych czy tajemnicy skarbowej. To oznacza, że żadna z wymienionych instytucji rządowych nadzorujących działanie systemów IK nie jest w stanie przejąć odpowiedzialności innego podmiotu, która jest sprawą indywidualną każdego z osobna[38].

Natomiast ryzyko związane z dysfunkcją określonych podmiotów pozwala na powiązanie roli baz danych administracyjnych z systemami informatycznymi administracji publicznej, a także IK z systemami SCADA. Włamanie do bazy lub serwera skutkuje brakiem dostępu do środowiska, przechwyceniem danych (szczególnie groźne jest przechwycenie danych z SŁR). Celowe wywołanie awarii lub błędy oprogramowania systemów IK mogą zagrażać zarówno społeczeństwu, jak i produkowanym towarom. Mogą spowodować wymierne straty finansowe, materialne albo niematerialne (utrata renomy czy zaufania klientów)[39].

Rozdział III. Analiza bezpieczeństwa cybernetycznego RP na podstawie szczytu NATO 2016 w Polsce

Celem analizy badawczo-porównawczej będzie potwierdzenie tezy, że polska cyberprzestrzeń jest dobrze chroniona pod względem dostosowania systemu prawnego do zarządzania bezpieczeństwem i ochroną technologiczną. Obecne regulacje prawne i strategie zarządzania cyberbezpieczeństwem, a także przygotowanie technologiczne, muszą być realizowane na najwyższym poziomie, aby Rzeczpospolita Polska – będąca organizatorem dwóch dużych międzynarodowych wydarzeń, jakimi są szczyt NATO i Światowe Dni Młodzieży, które mają się odbyć w ciągu jednego miesiąca – mogła je skutecznie zabezpieczyć. Podstawą analizy będzie szczyt NATO w Warszawie, który jest ważnym wydarzeniem międzynarodowym pod względem dyplomatycznym, organizowanym głównie przez Polskę.

Celem analizy nie jest proponowanie scenariusza ataku na szczyt NATO w Warszawie bądź pokazanie słabych stron albo luk zabezpieczenia. Zamierzeniem niniejszej analizy jest prognoza skutków incydentów teleinformatycznych naruszających bezpieczeństwo cybernetyczne organizacji szczytu NATO i Rzeczpospolitej Polskiej, które mogą się potencjalnie wydarzyć.

Rozdział został podzielony na podstawie koncepcji czterech faz cyklu życia projektu (zgodnie z metodyką zarządzania projektowego)[40].

1. W ramach etapu definiowania zostanie dokładniej przedstawiony szczyt NATO w Warszawie 2016 r. oraz jego poprzednie edycje – w Chicago w 2012 r. oraz w Newport w 2014 r.
2. Drugim etapem jest sprecyzowanie, jakie incydenty lub zagrożenia cybernetyczne dotknęły lub groziły poprzednim szczytom i jakie prawdopodobnie mogą za-

[37] Patrz: rozdz. II, pkt. 2.2.

[38] R. Kośla, *Ochrona infrastruktury krytycznej w Polsce – aktualny stan prac*, prezentacja multimedialna na IT.FORUM Secure 2002, materiał dostępny pod adresem http://www.cert.pl/PDF/Kosla_p.pdf [dostęp: 14 V 2016].

[39] Tamże.

[40] Więcej o cyklu życia projektu zob. http://zarzadzanieprojekt.pl/fazy-zarzadzania-projektem-cykl-zycia-projektu/ lub http://goprojekt.pl/baza_wiedzy/strona/etapy_zarzadzania_projektami/ [dostęp: 3 VI 2016].

istnieć w Warszawie. Zostanie przeprowadzone badanie wszystkich zgłoszonych ataków, do których doszło podczas trwania obu poprzednich szczytów, a następnie, na podstawie utworzonego katalogu, zostanie podjęta próba dedukcji, jakiego rodzaju ataki mogą prawdopodobnie pojawić się w trakcie szczytu w Warszawie.
3. Trzecim etapem jest prognoza, co mogłoby się stać, gdyby doszło do dwóch wybranych cyberataków.
4. Ostatni etap to podsumowanie analizy przewidywanych długo- i krótkofalowych skutków ataku oraz przedstawienie własnej propozycji przygotowania się do nich bądź zapobieżenia im.

1. Przedstawienie wydarzenia

Szczyt NATO to międzynarodowe, niecykliczne spotkanie przedstawicielstw władz państwowych, na którym są podejmowane najistotniejsze decyzje powiązane z przyszłością polityczno-wojskową wszystkich członków Sojuszu. Decyzje, które zapadają na tych spotkaniach, mają wpływ na jego kształt i funkcjonowanie, dotyczą spraw strategicznych, ścieżek rozwoju przygotowań do misji międzynarodowych, włączania nowych krajów do Sojuszu lub podejmowania partnerstwa pomiędzy państwami członkowskimi i niezrzeszonymi[41]. Do analizy porównawczej zostanie wykorzystany przebieg szczytów z 2012 r. w Chicago oraz z 2014 r. w Newport jako wydarzeń najnowszych w historii NATO, które musiały liczyć się z ryzykiem cybernetycznym na podobnym poziomie zaawansowania technologicznego, co szczyt w Warszawie.

1.1. Minione szczyty NATO w Chicago i w Newport

Szczyt w Chicago odbył się 20 i 21 maja 2012 r. Spotkanie było rutynowym podsumowaniem minionego okresu. Uważa się, że dokumenty, które ogłoszono na szczycie, nie miały przełomowego charakteru w sprawach bezpieczeństwa i współpracy państw członkowskich NATO, choć *Smart defence*, czyli inicjatywa współpracy państwowej w systemach ochrony rakietowej państw członkowskich, jest jednym z ważnych fundamentów działalności Paktu Północnoatlantyckiego, jakie wypracowano na spotkaniu. Podstawowymi sprawami, które miały być poruszone, była „arabska wiosna" oraz kryzys finansowy i związane z nim cięcia budżetowe w obronności państw członkowskich. Jednym z tematów była misja ISAF w Afganistanie oraz próba jej wygaszenia. Podjęto także decyzję na temat postanowień rezolucji z operacji *Unified Protector* z 1973 r. w Libii[42]. Wśród ważnych spraw do omówienia na szczycie znalazły się relacje z Rosją oraz ogólny przegląd przygotowania obronnego państw członkowskich. W ramach tego przeglądu zauważono, że w perspektywie kryzysu finansowego tylko trzy państwa członkowskie są w stanie realizować politykę przeznaczania 2 proc. budżetu na obronność państwa. Podczas gdy większość państw starała się zmniejszać wydatki na obronność po zakończeniu zimnej wojny na świecie, Polska przeznaczała na ten cel blisko 1,95 proc. budżetu. Porównując to z budżetem obronnym samego USA, ale także Rosji i Chin, zauważono, że takie podejście może spowodować w przyszłości większą marginalizację

[41] Czym jest szczyt NATO, witryna internetowa Ministerstwa Spraw Zagranicznych, https://www.msz.gov.pl/pl/polityka_zagraniczna/szczyt_nato_2016/aktualnosci/szczyt_nato_czyli_drogowskaz [dostęp: 2 VI 2016].

[42] Więcej o operacji zob. http://www.nato.int/cps/en/natolive/71679.htm [dostęp: 2 VI 2016].

NATO i obniżenie wiarygodności Sojuszu w obliczu innych mocarstw świata[43]. Szczyt zaowocował podjęciem decyzji o zmianie formy dowodzenia misją pokojową w Afganistanie na formę instruktorską i nadzorczą. Zaplanowano też, że do końca 2014 r. zostanie wycofanych z tego kraju około 130 tys. żołnierzy. Innym rezultatem rozmów było podjęcie współpracy wojskowej z 13 państwami niebędącymi w strukturach NATO[44].

Szczyt w Newport (Walia) odbył się 4 i 5 września 2014 r. Przyjmuje się, że był on do tej pory najważniejszym spotkaniem Sojuszu na szczeblu władz państwowych od czasów, gdy do NATO dołączyła Polska. To spotkanie było tym bardziej istotne, że początkowo (jeszcze w 2013 r.) traktowano je jako spotkanie rutynowe, które miałoby podsumować misję ISAF w Afganistanie. Jednak czas, w którym się odbywało, był znamienny ze względu na trwającą ofensywę sił rosyjskich na wschodnie tereny Ukrainy i aneksję Krymu. Te wydarzenia były argumentem do przedefiniowania pierwotnej idei Sojuszu, jaką było połączenie sił we wspólnej obronie państw członkowskich NATO. Decyzje, które podjęto, uznano za sprzyjające polskim interesom. Zdaniem członków było to sprawne i kompletne wdrożenie zakładanych ustaleń. Każde państwo było też zobowiązane do wzmacniania własnego potencjału obrony i systemów bezpieczeństwa[45].

Wśród spraw ważnych dla RP w dziedzinie bezpieczeństwa znajdował się między innymi postulat stałej obecności wojsk NATO w Polsce oraz większej ich integracji z polskimi siłami zbrojnymi (środkiem do osiągnięcia tego celu miało być spotkanie Grupy Wyszehradzkiej w lipcu 2014 r. w Warszawie). Szczyt przebiegł sprawnie – odbyło się pięć głównych spotkań na szczeblu rządowym oraz kilkanaście spotkań ministrów obrony i ministrów spraw zagranicznych. Warto zaznaczyć, że podczas szczytu odbyły się tzw. kolacje robocze przedstawicieli obrony narodowej państw członkowskich. Najistotniejszym ustaleniem było przyjęcie niejawnego *Planu działań na rzecz gotowości* (*Readiness Action Plan*[46]). Sukcesem Polski było wynegocjowanie stworzenia tzw. szpicy na terenie RP, którą utworzyłyby państwa sojusznicze. Podjęto też decyzję o wsparciu finansowym Ukrainy, a także zdecydowano się na podjęcie stanowczych kroków i wspólnego działania wobec agresji Państwa Islamskiego prowadzącego dżihad[47].

1.2. Szczyt w Warszawie

Szczyt w Warszawie został zaplanowany na 8 i 9 lipca 2016 r. Miejsce i termin spotkania zostały oficjalne ogłoszone przez Sekretarza Generalnego NATO w maju 2015 r.[48] Uczestnikami szczytu będzie około 2500 delegatów z ponad 60 państw członkowskich. Przebieg spotkania będzie relacjonowany przez około 500 reprezentantów ośrodków naukowo-badawczych oraz około 1500 dziennikarzy z całego

[43] P. Pietrzak, *Szczyt NATO w Chicago – determinanty, oczekiwania i rezultaty*, „Bezpieczeństwo Narodowe" 2012, nr 22, s. 47–64.

[44] Na temat efektów szczytu w Chicago zob. *NATO Chicago summit meets its golas* [online], http://www.nato.int/cps/en/natohq/news_87603.htm [dostęp: 3 VI 2016].

[45] S. Koziej, P. Pietrzak, *Szczyt NATO w Walii: uwarunkowania, rezultaty, wnioski dla Polski*, „Bezpieczeństwo Narodowe" 2014, nr 31, s. 11–29.

[46] Tamże, s. 21.

[47] P. Maciążek, *Szczyt NATO w Walii: kluczowe decyzje*, Defence24.pl [online] z 5 września 2014 r. [dostęp: 3 VI 2016].

[48] *NATO Secretary General announces dates for 2016 Warsaw Summit* [online], 22 V 2015 r., witryna internetowa North Atlantic Treaty Organization, http://www.nato.int/cps/en/natohq/news_120085.htm [dostęp: 3 VI 2016].

świata. Przyjmuje się, że warszawski szczyt będzie kamieniem milowym dla Sojuszu. Motywem przewodnim będzie wzmacnianie i modernizacja systemu obrony państw członkowskich oraz podkreślenie postawy odstraszania potencjalnych agresorów ma kraje NATO. Sojusznicy będą także oceniać długofalowe konsekwencje kryzysu w relacjach z Rosją i decydować o następnych krokach. Przewiduje się także dyskusję o poprawie jakości wywiadu i wczesnego ostrzegania przed zagrożeniami, integracji własnych sił zbrojnych, wzmocnieniu obrony cybernetycznej państw członkowskich, a także poprawie relacji z UE oraz między innymi z Finlandią i Szwecją. Ważnym dla Polski punktem spotkania będzie także debata o większej obecności wojsk Sojuszu we wschodniej części Europy. Z przekazów medialnych wiadomo[49], że podczas spotkania będzie omawiana sytuacja na wschodniej Ukrainie w kontekście trwającego tam konfliktu i aneksji Krymu przez rosyjskie wojska, będzie także podjęta dyskusja o próbie zażegnania wojny w tamtym rejonie. Zostanie również poruszony temat kryzysu polityczno-militarnego w północnej części Bliskiego Wschodu, czyli przede wszystkim problem ISIS. Tematem rozmów będą także zwiększenie obrony powietrznej nad Turcją oraz zapobieżenie rozprzestrzenianiu się konfliktu na terenie Syrii. Jako podsumowanie całego szczytu zaplanowano dyskusję o zwiększeniu poziomu zaufania społeczeństw wobec struktur NATO, które jest podważane w wyniku wypełniania zobowiązań umów członkowskich.

2. Analiza ryzyka

Wnioski po przeanalizowaniu ryzyka w przypadku tak poważnego wydarzenia międzynarodowego, jakim jest szczyt NATO organizowany w Warszawie, mogą stanowić podstawę do efektywnego zapobieżenia incydentowi lub zminimalizowania skutków jego wystąpienia. Oznacza to, że warto przyjrzeć się ryzyku zarówno w świecie rzeczywistym, jak i w cyberprzestrzeni. Dane analityczne odnoszące się do cyberbezpieczeństwa uzyskano z dostępnych powszechnie źródeł z lat ubiegłych.

2.1. Ryzyko rzeczywiste

Rządowe Centrum Bezpieczeństwa zdefiniowało główne ryzyko dla szczytu NATO w Warszawie w katalogu zagrożeń, które mają pewne prawdopodobieństwo wystąpienia oraz wywołania sytuacji kryzysowej. Zostały w nim opisane zadania i podział ról podmiotów działających na rzecz bezpieczeństwa w ramach zarządzania kryzysowego w fazie reagowania. Siatka ryzyka, którą opracowano, została przygotowana na podstawie danych historycznych, doświadczeń oraz wniosków wyciągniętych z wcześniejszych wizyt papieża oraz innych osobistości, ważnych z punktu widzenia dyplomacji. Sugerowano się także konkluzjami uzyskanymi z poprzednich szczytów NATO. Wyzwaniem, według RCB, było uwzględnienie wystąpienia ataku terrorystycznego, do którego nigdy wcześniej w Polsce nie doszło. Rządowe Centrum Bezpieczeństwa nie było więc w stanie określić prawdopodobieństwa wystąpienia tego zdarzenia na podstawie zebranych informacji i zdecydowało się skorzystać

[49] *Vershbow: Szczyt NATO w Warszawie będzie jednym z najbardziej brzemiennych w skutkach*, wPolityce.pl [online] z 3 czerwca 2016 r., http://wpolityce.pl/swiat/295347-vershbow-szczyt-nato-w-warszawie-bedzie-jednym-z-najbardziej-brzemiennych-w-skutkach [dostęp: 3 VI 2016].

z pomocy ekspertów oraz specjalnych technik analitycznych[50]. Przede wszystkim brano pod uwagę ryzyko zaistnienia incydentów, które przedstawiono według kolejności numeracji w siatce:

1) podłożenie bomby lub użycie broni,
2) katastrofa lotnicza,
3) zbiorowe zakłócanie porządku publicznego,
4) awaria systemów energetycznych,
5) awaria systemów teleinformatycznych lub łączności,
6) uprowadzenie osoby lub osób,
7) naruszenie granic powietrznych przez drony,
8) katastrofa w ruchu drogowym lub kolejowym,
9) sabotaż i dezinformacja,
10) inwigilacja spotkań szczytu, kolacji roboczych bądź administracji rządowej RP.

Tab. 1. Matryca ryzyka dla szczytu NATO 2016.

skutki						
	duże					
	średnie		3,5,9	4		
	małe		6,7,8	1,2	10	
		małe	średnie		duże	
	prawdopodobieństwo					

Źródło: Opracowanie na podstawie http://rcb.gov.pl/.

Ze względu na duże znaczenie tego szczytu dla stosunków państw członkowskich NATO z Rosją jako głównym rywalem gry politycznej, który nie jest członkiem Sojuszu – dodano do listy zagrożeń punkt dziesiąty. Wynika on z dotychczasowych obserwacji, że Rosja będzie wykazywać chęci strategicznego wyprzedzania struktur NATO. Od dawna podejrzewano Rosjan, ale także Amerykanów, o wykorzystywanie odpowiedniej aparatury do prowadzenia podsłuchów[51]. Problemem może być strategiczne położenie ro-

[50] *Przygotowania Rządowego Centrum Bezpieczeństwa do Szczytu NATO i Światowych Dni Młodzieży* [online] z 11 kwietnia 2016 r., witryna internetowa Rządowego Centrum Bezpieczeństwa, http://rcb.gov.pl/przygotowania-rcb-do-szczytu-nato-i-swiatowych-dni-mlodziezy/ [dostęp: 3 VI 2016].

[51] Na podstawie artykułów: *Rosyjska ambasada w sąsiedztwie Kancelarii Premiera i MSZ. To poważne ryzyko podsłuchu!* Niezależna.pl [online] z 21 listopada 2013 r., http://niezalezna.pl/48553-rosyjska-ambasada-w-sasiedztwie-kancelarii-premiera-i-msz-powazne-ryzyko-podsluchu [dostęp: 3 VI 2016] oraz *Ambasada, czyli o najważniejszym budynku w Warszawie*, Salon24.pl [online] z 25 października 2013 r., http://rybitzky.salon24.pl/543474,ambasada-czyli-o-najwazniejszym-budynku-w-warszawie [dostęp: 3 VI 2016].

syjskiej ambasady w Warszawie[52] względem placówek administracji rządowej, siedziby ABW, CBA i BOR oraz luksusowych hoteli, w których mogą mieszkać lub przebywać goście zaproszeni na szczyt.

Według informacji podanych przez RCB nad zapewnieniem maksymalnego poziomu bezpieczeństwa szczytu będą działać zespoły zadaniowe. Ich obowiązkiem będzie monitorowanie przebiegu wydarzeń i przewidywanie potencjalnych zagrożeń, ich przeanalizowanie pod kątem wystąpienia sytuacji kryzysowych, a także planowanie z wyprzedzeniem kroków, które należy podjąć w fazie reagowania. Nacisk zostanie także położony na upraszczanie procedur wzbudzania sił i środków reagowania, które na co dzień są w dyspozycji komendantów, wojewodów oraz ministrów. Ważne będzie także przeorganizowanie systemu komunikowania się w celu usprawnienia wymiany łączności[53].

2.2. Ryzyko cybernetyczne

Określenia cyberzagrożeń, do których może dojść podczas szczytu NATO w Warszawie, dokonano na podstawie statystyk i raportów prywatnych firm zajmujących się bezpieczeństwem Internetu. Dane do statystyk i raportów są zbierane za pośrednictwem odpowiednich algorytmów informatycznych, sond, skanerów i innych specjalistycznych narzędzi w cyberprzestrzeni, którymi posługują się korporacje. Dane analityczne[54] zawierają między innymi informacje o wykrytych lukach w kodzie źródłowym, infekcjach malware, różnego typu atakach i próbach włamań, kradzieży danych i pieniędzy, sabotowaniu ofiary i podszywaniu się (np. *phishing*). Dostępne są również informacje o najczęściej występujących cyberprzestępstwach, statystyki i zestawienia danych oraz prognozy wraz z zaleceniami dla odbiorców raportów. Poniżej zaprezentowano najistotniejsze wnioski dotyczące zagrożeń cybernetycznych występujących w 2012 i 2014 r.

W ostatnich dwóch – trzech latach zaobserwowano gwałtowny wzrost ataków technicznie zaawansowanych. Jedną w ważnych cech tych ataków była głęboka infiltracja kodu źródłowego z wykorzystaniem bomb czasowych oczekujących właściwego momentu słabości systemu. Były one specjalnie przygotowywane, aby omijać standardowe pułapki do wykrywania malware[55].

Przeanalizowanie ataków w skali państwa pozwala stwierdzić, że ich głównymi motywami było szpiegostwo i wpływanie na dane. Informacje interesujące hakerów obejmowały kod źródłowy, e-maile, dokumenty wewnętrzne, aktywność sił zbrojnych, dane osobowe funkcjonariuszy państwowych. Zasób danych, jakie były przechwytywane, był bardzo zróżnicowany, a wyrafinowanie technologiczne ataków stało na wysokim poziomie. Często źródła ataków były maskowane za pomocą pośredników lub w ogóle pozostawały nieznane[56].

---

[52] R. Zieliński, K. Majszak, *Tak podsłuchują Rosjanie. Kluczowe polskie urzędy zagrożone*, dziennik.pl [online] z 21 listopada 2013 r. [dostęp: 3 VI 2016].

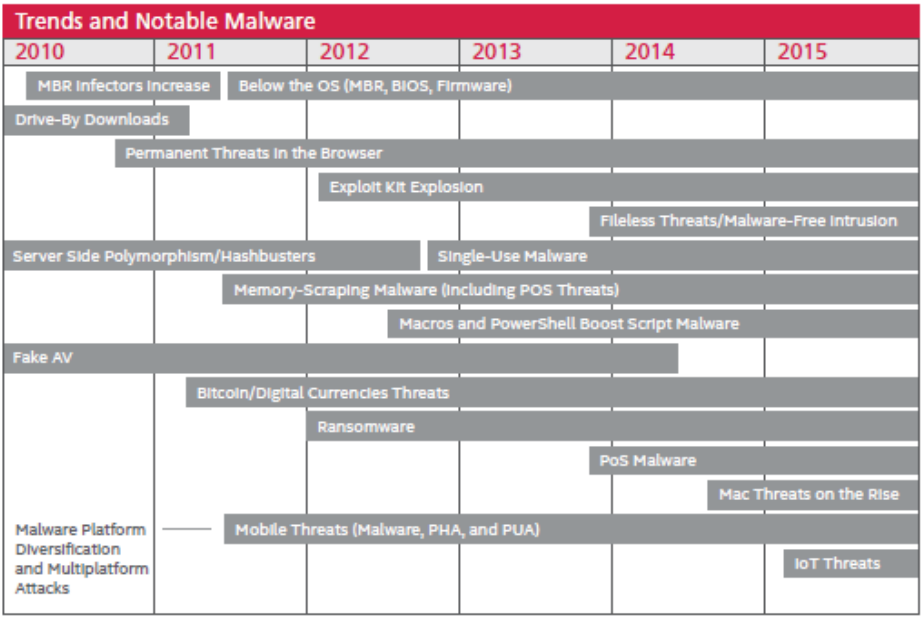
[53] *Przygotowania Rządowego Centrum Bezpieczeństwa do Szczytu NATO i Światowych Dni Młodzieży* [online] z 11 kwietnia 2016 r., witryna RCB [dostęp: 3 VI 2016].

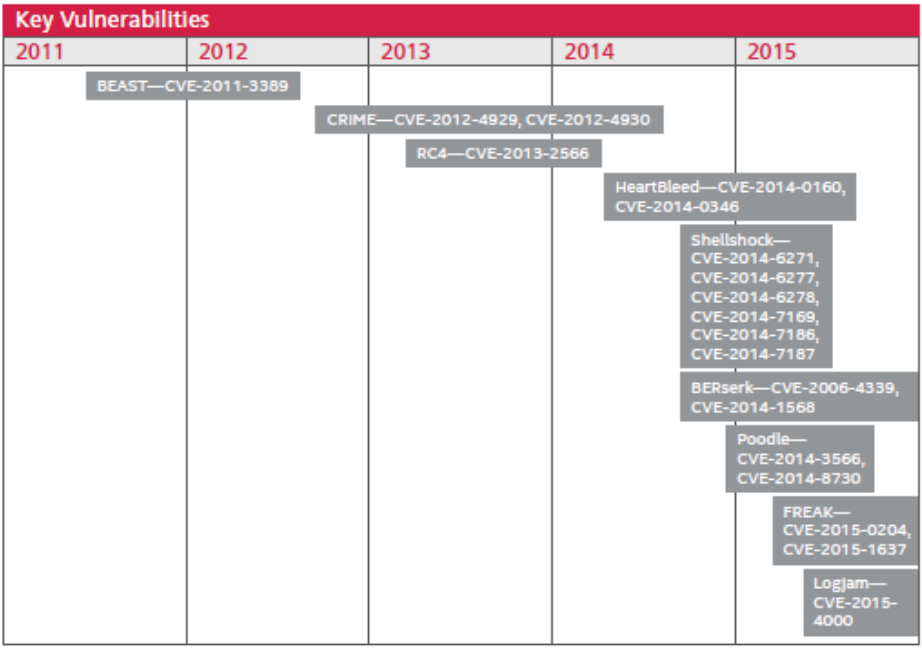
[54] Źródłem danych są: http://www.hackmageddon.com/, http://www.mcafee.com/us/, https://www.symantec.com/, https://securelist.com/analysis/kaspersky-security-bulletin/ [dostęp: 3 VI 2016].

[55] *McAfee Labs Threats Report, August 2015* [online], https://www.mcafee.com/au/resources/reports/rp-quarterly-threats-aug-2015.pdf, s. 10 [dostęp: 3 VI 2016].

[56] Tamże, s. 17.

Tab. 2. Góra: retrospekcja trendów zagrożeń w cyklu sześciu lat. Dół: główne ataki typu Exploit – wyniki w skali globalnej.





Źródło: McAfee Labs Threats Report, August 2015 [online], https://www.mcafee.com/au/resources/reports/rp-quarterly-threats-aug-2015.pdf [dostęp: 3 VI 2016].

Trzeci kwartał 2014 r. wyjątkowo obfitował w podejrzane adresy URL oraz ataki typu *phishing* (czterokrotnie większe niż w medianie za pozostałe kwartały tego roku)[57], jednak w tej sytuacji winą obarczano modę na krótkie adresy, tzw. TinyURL[58]. Podejrzewano również, że za *phishing* odpowiada rosyjska kampania *pill-spam*, która tworzyła subdomeny dla każdego odwiedzającego. W tym kwartale znacznie częściej rozsyłano też spamy.

W 2014 r. hakerzy zwiększyli liczbę skutecznych ataków z użyciem podstawionych mediów o mniej więcej 8 proc. w porównaniu z rokiem poprzednim. To kosztowało ich mniej wysiłku, gdyż wygenerowali 14 proc. mniej e-maili zawierających malware, które wysłali do 20 proc. mniej odbiorców. Innymi słowy, przygotowali lepiej dostosowane pod ofiarę fałszywe strony i mniejszym nakładem pracy osiągnęli lepsze efekty, tzn. wzrosła skuteczność takich ataków. Niemalże każda korporacja jest wrażliwa na *phishing*. Według danych statystycznych pięć na sześć dużych firm było celem tego typu ataków w 2014 r., co oznacza wzrost o 40 proc. w porównaniu do roku wcześniejszego[59].

Udział procentowy włamań do instytucji rządowych i terytorialnych oraz kradzieży ich danych wynosił w 2014 r. 2 proc. Dla porównania – w sektorze finansowym to 23 proc. udziału wśród wykradzionych danych, a w handlu – 59 proc. Z drugiej jednak strony dane osobowe, prywatne i służbowe, funkcjonariuszy państwowych były drugimi najczęściej publikowanymi danymi, które zostały wykradzione. Pierwszymi były dane osobowe innych obywateli[60].

W 2014 r. w kategorii malware przygotowanego na system operacyjny Mac OS X dominowało adware (uporczywe reklamy), trojany generujące złośliwy kod lub backdoory („tylne wejścia" omijające zapory) szpiegowskie, które przejmują kontrolę nad systemem, kradną dane kontaktowe bądź dane ze wszystkich urządzeń Apple z zainfekowanym urządzeniem. Wielka Brytania znalazła się na czwartym miejscu na świecie w rankingu krajów najbardziej zagrożonych tego typu atakami oraz siódme miejsce w kategorii ataków online na sektor bankowy, które polegały na kradzieży pieniędzy z kont bankowych, np. za pośrednictwem trojana Zeus[61].

We wrześniu 2014 r. zaobserwowano dużą liczbę ataków o charakterze cyberprzestępczym (około 70 proc. globalnych ataków, czyli około 15 proc. więcej w porównaniu do sierpnia tego samego roku), jednak w okresie trwania szczytu NATO nie stwierdzono większej liczby incydentów. Blisko 16 proc. incydentów w cyberprzestrzeni było skierowanych przeciwko podmiotom rządowym – było to drugie miejsce zaraz po atakach w przemyśle (około 40 proc.)[62]. W dniu 5 września doszło do ataku na jedną ze stron rządowych Indii (ajk.gov.pk) za pomocą iniekcji SQL, czego rezultatem była kradzież danych logowania[63].

---

[57] Tamże, s. 37.

[58] *McAfee Labs Threats Report, November 2014* [online], https://www.mcafee.com/hk/resources/reports/rp-quarterly-treath-q3-2014.pdf, s. 32 [dostęp: 3 VI 2016].

[59] Raport incydentów autorstwa firmy Symantec zob. *Internet Security Threat Report* „Istro20" [online], nr 20, kwiecień 2015, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Symantec_annual_internet_threat_report_ITU2015.pdf, s. 6, 7.

[60] Tamże, s. 16.

[61] Statystyki cyberataków w 2014 r. [online], *Overall statistics for 2014*, „Kaspersky Security Bulletin 2014" [online], https://securelist.com/analysis/kaspersky-security-bulletin/68010/kaspersky-security-bulletin-2014-overall-statistics-for-2014/ [dostęp: 3 VI 2016].

[62] Statystyki ataków cybernetycznych we wrześniu 2014 r. [online], http://www.hackmageddon.com/2014/10/13/september-2014-cyber-attacks-statistics/ [dostęp: 4 VI 2016].

[63] Linia czasu incydentów we wrześniu 2014 r. [online], http://www.hackmageddon.com/2014/09/29/1-

Między 20 a 21 maja 2012 r. doszło do serii ataków cybernetycznych na systemy teleinformatyczne i struktury służb policji Chicago oraz witryny NATO. W obu przypadkach autorem ataków była grupa Anonymous, która zablokowała witryny i serwery obu ofiar (atak DDoS)[64]. Ataki były umotywowane rzekomym sprzeciwem wobec postulatów NATO[65]. Odnotowano także, że współczynnik ataków na strony rządowe był największym w tamtym miesiącu (około 22 proc.), z iniekcją SQL oraz atakiem DDoS jako najczęściej wykorzystywanymi technikami[66].

W najnowszych raportach na kwiecień 2016 r. wskazano na większą aktywność ataków cybernetycznych wobec sieci przemysłowych (około 31 proc.) i rządowych (około 14,5 proc.). Siedemdziesiąt jeden procent wszystkich ataków stanowiła cyberprzestępczość. Po przeanalizowaniu trendów z podziałem na poszczególne dni, można stwierdzić, że wraz z upływem czasu liczba ataków się zwiększa[67], co może mieć wpływ na bezpieczeństwo cybernetyczne podczas szczytu NATO w Warszawie, tym bardziej, że oczekuje się, iż to wydarzenie przyniesie pozytywne skutki dla Europy Wschodniej.

Biorąc więc pod uwagę całe wcześniej wspomniane ryzyko cybernetyczne, można na tej podstawie wypracować jego matrycę. Ulokowanie danego ryzyka na matrycy jest wynikiem dedukcji z przeprowadzonych obserwacji i stwierdzonych tendencji z ostatniego okresu. Wśród nich można wyliczyć:

1) ataki DDoS paraliżujące serwery lub witryny internetowe szczytu,
2) włamanie do wewnętrznych repozytoriów danych, kradzież wrażliwych danych,
3) *phishing* domen NATO, usług bankowych i serwisów służb porządkowych,
4) paraliż systemów SCADA IK,
5) dezinformację mediów i bojkot medialny,
6) zastosowanie exploitów,
7) *sniffing*.

Tab. 2. Matryca ryzyka cybernetycznego.

skutki						
	duże					
	średnie		2			
	małe		4,6	3	1	
				5	7	
		małe		średnie		duże
	prawdopodobieństwo					

Źródło: Opracowanie własne.

15-september-2014-cyber-attacks-timeline/ [dostęp: 2 VI 2016].

[64] Linia czasu incydentów w maju 2012 r. [online], http://www.hackmageddon.com/2012/06/04/may-2012-cyber-attacks-timeline-part-ii/ [dostęp: 2 VI 2016].

[65] Motywacja Anonymous [online], http://infinitynewsnetwork.com/2012/05/20/anonymous-puts-antis3curityops-into-action/ [dostęp: 2 VI 2016].

[66] Statystyki ataków cybernetycznych V 2012 [online], http://www.hackmageddon.com/2012/06/10/may-2012-cyber-attacks-statistics/ [dostęp: 2 VI 2016].

[67] Statystyki ataków cybernetycznych IC 2016 [online], http://www.hackmageddon.com/2016/06/01/april-2016-cyber-attacks-statistics/ [dostęp: 3 VI 2016].

3. Prawdopodobne scenariusze przebiegu cyberataków

Z matrycy ryzyka cybernetycznego wynika, że najbardziej brzemiennymi w skutkach incydentami byłyby włamanie się do wewnętrznych repozytoriów NATO lub rządu RP i kradzież poufnych danych. Najbardziej prawdopodobnym zdarzeniem mogą być ataki paraliżujące przepustowość serwerów obsługujących szczyt, czyli DDoS. Pierwsze wydarzenie zostanie opisane jako sytuacja A, drugie jako sytuacja B. Można domniemywać, że wspólnym celem obu sytuacji nie byłoby wywołanie konfliktu zbrojnego bądź zaostrzenie trwającego konfliktu na Ukrainie, ale inwigilacja, pozyskanie wrażliwych danych, zakłócenie przebiegu lub też niedopuszczenie do odbycia się szczytu (np. z powodu wywołania stanu nadzwyczajnego). W gronie potencjalnych podmiotów dokonujących ataku należy uwzględnić państwa niebędące członkami NATO i uznające szczyt za niekorzystny dla nich, jak na przykład Rosję czy toczące walkę z Sojuszem Państwo Islamskie.

Sytuacja A

Polska jako gospodarz szczytu będzie zabezpieczać całe wydarzenie od strony logistycznej, organizacyjnej, administracyjnej i cybernetycznej. Wszyscy uczestnicy spotkania na pewno będą korzystać z zaoferowanych sieci internetowych oraz sieci wewnętrznych NATO, zarówno na Stadionie Narodowym, w miejscach publicznych, jak i w miejscach zakwaterowania. Uczestnicy będą prawdopodobnie korzystać do komunikowania się z wyodrębnionych sieci o charakterze niejawnym. Istnieje więc wiele możliwości podjęcia prób przełamywania zabezpieczeń, nieautoryzowanego logowania się za pomocą kradzionych danych, wyszukiwania luk oprogramowania, podsłuchania transferu danych lub podstawienia fałszywych stron, które mogą powodować przekierowanie przez narzędzia hakerskie na inne strony. Wystarczy nieopatrzne podłączenie się gościa dyplomatycznego do Wi-Fi hotelu lub restauracji z niezabezpieczonym połączeniem, które będzie jednocześnie podsłuchiwane przez hakera, aby spowodowało to próbę zainfekowania jego komputera za pomocą malware. Dzięki temu byłoby możliwe obejście zabezpieczeń szczytu.

Udane obejście zabezpieczeń może grozić nieautoryzowanym dostępem i kradzieżą różnego rodzaju danych, których wyciek może stanowić zagrożenie dla interesów lub bezpieczeństwa Sojuszu, państw członkowskich, a także osób uczestniczących w szczycie bądź działających w strukturach państwowych tych krajów.

W zależności od dobranego narzędzia oraz przygotowania technologicznego i operacyjnego atakujący jest narażony na namierzenie go i identyfikację oraz podjęcie poszukiwania, a nawet pochwycenia go przez służby państwowe, zespoły CERT lub służby bezpieczeństwa przedstawiciela zaatakowanego państwa.

Sytuacja B

Dyplomaci, specjaliści oraz politycy, którzy uczestniczą w spotkaniu, będą wykorzystywać różne środki przekazu do komunikowania się między sobą. Jedną z podstawowych witryn informacyjnych dla mediów, uczestników i obserwatorów jest witryna internetowa MSZ, na której w trybie bieżącym umieszcza się artykuły o szczycie. Zawiera ona także informacje o Warszawie oraz dotyczące spraw organizacyjnych, przydatnych gościom. Inną witryną wspierającą szczyt jest oficjalna strona NATO, na której również będą umieszczane informacje na jego temat, a także inne artykuły. Z jednej strony na obu portalach nie będzie raczej wrażliwych danych, ale z drugiej – są one niczym cyfrowe wizytówki Sojuszu i RP.

Jeśli doszłoby do zmasowanego ataku DDoS na serwery obsługujące szczyt NATO w chwili jego rozpoczęcia lub zakończenia, to wskazane witryny oraz serwery obsługujące je zawiesiłyby się i przestały prawidłowo funkcjonować. Istnieje także ryzyko, że sam atak mógłby odgrywać rolę zasłony dymnej ułatwiającej inne operacje, na przykład dostęp do wrażliwych danych.

Mogłoby również dojść do prób szantażowania przedstawicieli władzy, aby zaniechali poruszenia na szczycie konkretnej problematyki lub zdecydowali się na zmianę podjętej już decyzji. Pierwsze informacje o ataku byłyby przekazywane przez media społecznościowe, np. Twitter czy Facebook, jeszcze podczas jego trwania. Trudno byłoby zatuszować to zdarzenie przed opinią publiczną. Prawdopodobnie władze odpowiedzialne za przebieg szczytu tłumaczyłyby dysfunkcję środowisk awariami technicznymi, usterkami itd., aby opóźnić narażenie tego wydarzenia na dyskredytację. Znane są jednak przypadki z historii, gdy politycy deklarujący takie teorie sami byli potem atakowani. Zadziałałby także efekt psychologiczny – ludzie zainteresowani sytuacją chcieliby sprawdzić, czy rzeczywiście doszło do ataku DDoS, wchodziliby więc na witryny, jednocześnie bardziej ją obciążając. Istnieje szansa, że gdyby podmiotami ataku była grupa terrorystyczna bądź grupa haktywistów, przyznaliby się oni chętnie do popełnionego czynu dla rozgłosu, własnej gloryfikacji i wzbudzenia niepokoju wśród opinii publicznej. Jeśli jednak dokonałyby go służby specjalne obcych państw, źródło takiego ataku byłoby bardzo trudne do wykrycia, co wiązałoby się z niemożliwością udowodnienia im spowodowania szkody.

4. Podsumowanie badania

Podczas szczytu NATO może zdarzyć się wiele; żadne prognozy nie dają stuprocentowej pewności, że nie dojdzie do którejś z przewidywanych sytuacji. Z tego powodu wydarzenia tak wysokiej rangi muszą być zabezpieczane w szczególny sposób. Należy mieć na uwadze to, że obie sytuacje, do których mogłoby dojść w cyberprzestrzeni, miałyby duży wpływ na sytuację polityczną w świecie rzeczywistym. O ile sytuacji A – ze względu na metodę ataku – można zapobiec, jeśli będą przestrzegane procedury i wysokie standardy bezpieczeństwa, to w przypadku sytuacji B można tylko minimalizować jej konsekwencje. Ponieważ uczestnicy szczytu będą korzystać w wielu miejscach ze swoich urządzeń mobilnych i komputerów – nie tylko na Stadionie Narodowym – ryzyko przełamania zabezpieczeń jest duże, choć można mu zapobiec. Sytuacja B różni się od sytuacji A o tyle, że jest zmasowanym atakiem informatycznym, którego źródło trudno ustalić, a szansa jego odparcia jest niewielka. Nawet jeśli próbowano by zwiększać przepustowość serwerów tak, by mogły udźwignąć obciążenie milionów połączeń naraz, to zniszczenie cybernetycznej infrastruktury niosłoby za sobą wielkie szkody[68].

4.1. Skutki krótko- i długofalowe, wewnętrzne i międzynarodowe

Zaistnienie powyższych incydentów może doprowadzić do wielu komplikacji, nawet gdyby napastnicy nie odnieśli dużego sukcesu. Wynikałoby to w dużej mierze z nagłośnienia problemu przez media i portale społecznościowe. Opisane poniżej skutki są wynikiem dedukcji, co mogłoby się wówczas stać w sferze życia politycznego, społecznego, medialnego, militarnego i dyplomatycznego.

[68] Na podstawie mapy analitycznej badającej DDoS, www.digitalattackmap.com/# [dostęp: 4 VI 2016].

Przede wszystkim same ataki wywołałyby oburzenie, dyskusje i inne reakcje mediów. Temat byłby tzw. jedynką przez pewien okres w gazetach i na portalach, zarówno polskich, jak i zagranicznych. Także na scenie politycznej mogłoby dojść do nasilonego potępienia partii rządzącej przez opozycję, która wykorzystałaby okazję do uzyskania poparcia społecznego – czyli mogłoby dojść do zaognienia konfliktów, zamiast sprawnego rozwiązania problemu. Organizatorzy szczytu oraz państwo polskie (w tym służby specjalne i specjaliści od cyberbezpieczeństwa) byliby narażeni na utratę zaufania społeczeństwa i zostaliby również zdyskredytowani w świecie dyplomacji. Polska dostała możliwość gospodarowania szczytem ze względu na opinię, że jest poważnym uczestnikiem w decyzyjności Sojuszu. Ataki spowodowałyby jednak narażenie naszego kraju na utratę tej dobrej opinii.

W przypadku sytuacji A przełamanie zabezpieczeń mogłoby skutkować narażeniem na ujawnienie kodów źródłowych zabezpieczeń oraz jakości cyberbezpieczeństwa RP. Kradzież wrażliwych danych (w zależności od tego, jakie dane zostałyby ujawnione), mogłaby spowodować zagrożenie życia lub zdrowia funkcjonariuszy rządowych i międzynarodowych bądź narazić stabilność stosunków międzynarodowych na arenie politycznej. Zwiększyłoby się także zagrożenie dla planów i interesów NATO, ponieważ przeciwnik, który by zdobył te wrażliwe dane (np. o systemie antyrakietowym w Polsce czy o wiedzy państw członkowskich na temat konfliktu zbrojnego na Ukrainie i kryzysu na Bliskim Wschodzie), starałby się wyprzedzać Sojusz.

W przypadku sytuacji B zablokowanie witryn internetowych i serwerów z perspektywy społecznej i medialnej również wywołałoby kilkudniowe dyskusje, rozmowy bądź pomówienie służb zabezpieczających wydarzenie, administracji rządowej lub władz Sojuszu, że nie potrafią poradzić sobie z takim zagrożeniem. Innym skutkiem mogłyby być utrudnienia organizacyjno-logistyczne dotykające dyplomatów i specjalistów przybyłych na szczyt. Nie wiadomo, ile mógłby trwać DDoS. Istnieje zatem ryzyko, że sprawca mógłby posiłkować się próbami szantażu.

Zidentyfikowanie sprawcy spowodowałoby podjęcie natychmiastowej próby schwytania go. Jednak gdyby napastnikiem okazały się inne państwo lub organizacja, wywołałoby to międzynarodowy skandal. Informacja o tym, że atakujący podlega obcemu rządowi lub organizacjom, stałaby się bronią przeciwko budowaniu wspólnych relacji międzynarodowych i zmieniłaby nastawienie Sojuszu do państwa agresora. Po przeanalizowaniu sytuacji można dopatrzeć się także pozytywnych skutków ataków. Istnieje bowiem prawdopodobieństwo, że Sojusz lub poszczególne państwa członkowskie zainteresowałyby się tematyką i prężniej realizowały bezpieczeństwo cybernetyczne. Ponadto mogłoby to zachęcić naukowców, studentów lub specjalistów od cyberbezpieczeństwa do większego zaangażowania się w temat bezpieczeństwa cyberprzestrzeni.

4.2. Propozycje reakcji na analizowane incydenty

Bardzo istotną rolę podczas szczytu będą odgrywać zespoły CERT.GOV.PL i CERT Polska działający przy NASK[69]. To zespoły profesjonalistów sprawnie zarządzających wykrywaniem i zwalczaniem incydentów komputerowych. Byłoby wskazane udzielenie im wszelkiego wsparcia technicznego, technologicznego, finansowego, naukowego

[69] Naukowa i Akademicka Sieć Komputerowa (przyp. red.).

i w każdej innej formie, tak aby skuteczniej mogły one wykrywać zdarzenia w cyberprzestrzeni, zapobiegać im, zwalczać ich skutki oraz wspierać odbudowę zaatakowanych systemów.

Utrzymanie cyberbezpieczeństwa nie jest tanim wydatkiem dla przedsiębiorstw. Wiele z nich będzie zaangażowanych w obsługę szczytu. Można więc poszukać sposobów na wsparcie tych podmiotów właśnie w podstawowych zabezpieczeniach internetowych, choćby rekomendując merytoryczne rozwiązania. Nie obciąży to znacznie budżetu państwa, a spowoduje przynajmniej częściowe zapewnienie podstawowej cyberochrony.

Ponadto warto przypominać wszystkim uczestnikom szczytu, aby dbali o bezpieczne połączenie sieciowe swoich urządzeń elektronicznych, w tym kontrolę technologii Bluetooth i NFC na swoich urządzeniach mobilnych, ze względu na wrażliwość danych, z którymi mają do czynienia. Aby zapobiec paraliżowi komunikacyjnemu z powodu potencjalnego ataku DDoS, warto pomyśleć o alternatywnym środku łączności, który będzie znany tylko uczestnikom szczytu.

Podczas spotkania wszystkie systemy łączności i sieci telekomunikacyjne będą utrzymywane i zabezpieczane na jak najwyższym poziomie. Warto jednak przemyśleć użycie certyfikacji SSL z technologią PFS jako środków do częściowego zablokowania włamywacza przed dostępem do całego zasobu danych. Bardzo dobrym zabezpieczeniem jest także dwuskładnikowe logowanie, czyli logowanie do systemów za pomocą hasła oraz kodu przesłanego na telefon bądź spisanego z tokena (np. RSA SecurID). Takie zabezpieczenia są często wykorzystywane w korporacjach, nie powinny więc być zaskoczeniem dla uczestników.

Media bardzo chętnie opowiadają o sytuacjach kryzysowych. Mogą jednak przedstawiać pewne wydarzenia w innym świetle niż obiektywne pokazanie faktów. Nadając wydarzeniu własną interpretację, mogą spowodować dezinformację zarówno we własnym społeczeństwie, jak i wśród mediów obcych krajów. Warto zatem zachować większą powściągliwość przy informowaniu mediów o zaistniałym incydencie, dopóki nie zostanie on precyzyjnie zidentyfikowany bądź zwalczony. Im mniej danych można zdobyć na temat szczytu w ramach tzw. białego wywiadu, tym większe bezpieczeństwo można mu zapewnić.

4.3. Wniosek końcowy

Szczyt NATO w Warszawie może być wydarzeniem przełomowym dla Sojuszu. Stwarza również wysokie wymagania dotyczące zabezpieczenia cybernetycznego. Po przeanalizowaniu aktualnych możliwości i poziomu przygotowania zespołów reagowania służb porządkowych i specjalnych, jest pewne, że bezpieczeństwo szczytu będzie stało na wysokim poziomie. O ile jednak zespoły CERT będą się starały zwalczać objawy incydentów, o tyle widać, że w ogólnym zarysie państwo polskie nadal ma luki technologiczne w zabezpieczaniu cyberprzestrzeni, a poziom cyfryzacji nadal próbuje nadążyć za szybko rozwijającą się technologią. Potrzebna będzie przede wszystkim jedna, zunifikowana ustawa dostosowana do obecnych czasów, ponieważ w tak mocno rozproszonym systemie prawnym, jaki obowiązuje teraz, stosunkowo łatwo znaleźć lukę w przepisach i obejść zabezpieczenia dostępne obywatelom i państwu. Trudno dziś stwierdzić, czy po ataku na Polskę z drugiego końca świata nasz kraj będzie w stanie stanowczo zareagować i na gruncie prawnym wyegzekwować swoje prawa.

Historia pokazuje, że spotkania członków Sojuszu były w przeszłości atakowane; z tych ataków wyciągano wnioski, a następnie na nowo rozwijano systemy, strategie bądź regulacje prawne. Niezależnie od tego, co przyniesie warszawski szczyt, trzeba brać z niego naukę i dążyć do osiągnięcia jak najwyższego poziomu cyberbezpieczeństwa, ponieważ świat zmierza w stronę technologii i jeszcze bardziej uzależni się od komputerów.

O autorach

About the authors

Robert Borkowski – dr hab., profesor nadzwyczajny Krakowskiej Akademii im. Andrzeja Frycza Modrzewskiego, kierownik katedry Służby Specjalne w Systemie Bezpieczeństwa, prezes Polskiego Towarzystwa Bezpieczeństwa Narodowego.
Piotr Chlebowicz – dr hab., adiunkt w Katedrze Kryminologii i Polityki Kryminalnej Wydziału Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego w Olsztynie.
Krzysztof Domeracki – doktorant na Akademii Sztuki Wojennej.
Dorian Duda – aplikant adwokacki, laureat VI edycji konkursu Szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa.
Karol Falandys – dr nauk politycznych.
Dariusz Gradzi – adwokat, kancelaria adwokacka AKGK Adwokaci Kostański Gradzi Kuczara.
Tomasz Kuć – doktorant w Instytucie Nauk Społecznych i Bezpieczeństwa Uniwersytetu Przyrodniczo-Humanistycznego w Siedlcach.
Remigiusz Lewandowski – dr, Wydział Nauk Ekonomicznych i Zarządzania Uniwersytetu Mikołaja Kopernika w Toruniu.
Anna Łasińska – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.
Dariusz Pożaroszczyk – dr, funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.
Krystian Radziejewski – laureat VI edycji konkursu Szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa.
Tomasz Safjański – dr, WSPiA Rzeszowska Szkoła Wyższa w Rzeszowie.
Jakub Sałek – laureat VI edycji konkursu Szefa ABW na najlepszą pracę licencjacką lub magisterską z dziedziny bezpieczeństwa wewnętrznego państwa.
Marek Świerczek – funkcjonariusz Agencji Bezpieczeństwa Wewnętrznego.
Waldemar Walczak – dr, Uniwersytet Łódzki, absolwent studiów doktoranckich.
Michał Wojnowski – dr, Instytut Pamięci Narodowej Oddział w Rzeszowie.

Informacje dla autorów „Przeglądu Bezpieczeństwa Wewnętrznego”

Redakcja zwraca się do autorów nadsyłających teksty do druku o stosowanie następujących zasad:

1. Wszystkie teksty należy przesyłać w postaci zapisu elektronicznego (Word, Open Office) na adres Redakcji: redakcja.pbw@abw.gov.pl.
2. Do artykułu należy dołączyć: bibliografię załącznikową (według schematu opisanego w pkt 10), streszczenie o objętości tekstu do pół strony wydruku komputerowego, notkę o autorze (zawód lub tytuł naukowy, miejsce pracy) oraz pięć słów kluczowych (w celu maksymalnie zwięzłego określenia tematyki artykułu – mają one ułatwić klasyfikację treści oraz wyszukiwanie artykułu w elektronicznych bazach danych; słowa kluczowe nie powinny być powtórzeniem tytułu). Streszczenie i słowa kluczowe powinny być przekazane również w języku angielskim.
3. Autorzy powinni wypełnić *Formularz zgody autora na publikację artykułu w czasopiśmie „PBW”* dostępny na stronie Agencji Bezpieczeństwa Wewnętrznego i przesłać go na adres Redakcji podany w pkt 1.
4. Wszelkie ilustracje, zdjęcia oraz schematy, które autor chciałby umieścić w artykule, powinny być dostarczone w oddzielnych oryginalnych plikach; ich wymiary powinny być nie mniejsze, niż te, które mają być 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, konkursów należy wyróżniać kursywą.
9. Nazwy wystaw, konferencji i sesji naukowych należy pisać antykwą i wyróżnić cudzysłowem.
10. W przypisach powinien być zachowany następujący schemat opisu:
    a) przypis zaczynamy wielką literą (wyjątek stanowi przypis internetowy) i kończymy kropką,
    b) przypis archiwalny: nazwa archiwum, po przecinku – nazwa zespołu, po przecinku – sygnatura, po przecinku – nazwa dokumentu (kursywą) lub jego opis (np.: list, sprawozdanie) i data, po przecinku – numer karty (strony),

PRZYKŁADY:
AIPN, OBUiAD w Krakowie, IPN Kr 144/1, *Materiały Wojewódzkiej Komisji Kwalifikacyjnej. Oświadczenie Pawła Kosiby z dnia 4 X 1990 r.*, k. 57;

APK, UWŚl., sygn. 736, sprawozdanie z działalności Policji Województwa Śląskiego za 1928 r. z 5 I 1929 r., k. 57;

c) druki zwarte: inicjał imienia, nazwisko autora, po przecinku – tytuł (kursywą), po przecinku – ewentualnie tom, po przecinku – miejsce i rok wydania, po przecinku – wydawnictwo, po przecinku – numery stron; po tytule publikacji zamieszczonej w pracy zbiorowej stawiamy przecinek i piszemy: w: i tytuł pracy (kursywą),

PRZYKŁAD:
W. Nowak, *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, 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 – zeszyt, numer, część (w opisie należy stosować cyfry arabskie), po przecinku – numery stron,

PRZYKŁAD:
W. Nowak, *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 13;

e) wydawnictwa internetowe: adres internetowy rozpoczynający się małą literą (bez podkreśleń i hiperłączy), po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:
http://www.pbw.gov/abw/cat.html [dostęp: 1 XII 2011];

f) artykuły lub dokumenty zamieszczone na stronach internetowych: tytuł artykułu (dokumentu) kursywą, dalej (bez przecinka) w nawiasie kwadratowym – informacja o trybie dostępu, po przecinku – adres internetowy, po przecinku w nawiasie kwadratowym – informacja o dacie dostępu (w dacie miesiąc należy podać cyfrą rzymską),

PRZYKŁAD:
EU NAVFOR Somalia – mission [online], http://www.eunavfor.eu/about-us/mission/ [dostęp: 20 VII 2014];

g) podając numer strony, należy stosować skrót: s. 30; zakres stron należy zaznaczyć półpauzą bez świateł, np.: s. 24–27,
h) należy stosować oznaczenia: tamże, tenże, taż (jeżeli tego typu zwroty rozpoczynają przypis, należy stosować wielką literę), inicjał imienia, nazwisko autora, po przecinku – skrót tytułu (kursywą), po przecinku – numery stron; nie stosujemy skrótów: op. cit., loc. cit.,

PRZYKŁAD:

W. Nowak, *Służba*…, s. 12.
Tamże, s. 14;

i) po skrócie: zob. i por. nie stawiamy dwukropka,
j) po skrócie: cyt. za: stawiamy dwukropek.

11. Przy zestawianiu bibliografii załącznikowej kolejne pozycje szeregujemy w porządku alfabetycznym (również akty prawne). Opis każdej pozycji rozpoczynamy od nazwiska autora, po nim umieszczamy inicjał imienia, kropkę, przecinek, a następnie według schematu przypisu – tytuł zapisany kursywą itd. W przypadku druków zwartych na końcu opisu bibliograficznego należy podać łączną liczbę stron, w przypadku artykułu w czasopiśmie lub w pracy zbiorowej – zakres stron.

PRZYKŁADY:

Kowalski W., *Służba więzienna*, „Prokuratura i Prawo" 2009, nr 4, cz. 2, s. 12–20.

Nowak W., *Urząd Ochrony Państwa*, w: *Historia służb specjalnych*, t. 3, K. Kowalski (red.), Warszawa 1999, PWN, s. 32–47.

Sekretna wojna. Z dziejów kontrwywiadu II RP, Z. Nawrocki (red.), Poznań 2014, Zysk i S-ka, 542 s.

12. W tekście głównym należy stosować ogólnie przyjęte skróty (np., itp., m.in., rkps, mps, t., z. itd.), a także z reguły: r. (rok) i w. (wiek).
13. W tekście głównym, podając datę, nazwę miesiąca należy zapisywać słownie, np.: 3 lipca 1969 r. Wyjątek stanowi zapis podany w przypisie, gdy miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.
14. Różne sposoby zapisu daty stosowane w tekście głównym powinny być ujednolicone do następującej formy, np. 12 VIII 1946; nie należy zamieniać na liczbę rzymską nazw miesięcy pisanych słownie w tekstach źródłowych.
15. Przy podawaniu daty dostępu do źródeł internetowych miesiąc zapisujemy cyfrą rzymską bez kropek rozdzielających dzień, miesiąc i rok.
16. W tekście głównym należy podawać pełne imię i nazwisko osoby, która jest wymieniana po raz pierwszy.
17. Należy podawać pełne nazwy instytucji, organizacji, urzędów itp., jeśli są wymieniane w tekście po raz pierwszy.
18. Obce nazwy organizacji oraz skróty od nich utworzone powinny być pisane antykwą (tekstem prostym).
19. Nie należy stosować tzw. twardych spacji.
20. Ortografię i interpunkcję tekstu należy uwspółcześniać.
21. Wszelkie wyróżnienia w oryginalnym tekście dokumentu, dokonane przez jego twórcę, powinny być wyróżnione wytłuszczoną czcionką.
22. Nawiasy ukośne /…/ powinny być zamieniane na nawiasy półokrągłe (…).
23. Skróty słownikowe należy pozostawić bez rozwinięcia.
24. Uzupełnienie odautorskie, od Redakcji itp. należy podawać w nawiasach kwadratowych antykwą.

25. Opuszczenia pochodzące od wydawcy powinny być zaznaczone trzema kropkami w nawiasie okrągłym.
26. Opuszczenia w cytacie pochodzące od autora artykułu należy zaznaczyć trzema kropkami w nawiasie okrągłym.
27. Redakcja zastrzega sobie prawo do zwracania autorom tekstów opracowanych bez uwzględnienia powyższych zasad.
28. Redakcja zastrzega sobie prawo do dokonywania zmian i skrótów w porozumieniu z autorem.
29. Redakcja zwraca uwagę, że *ghostwriting*[*] i *guest authorship*[**] są przejawem nierzetelności naukowej, a wszelkie wykryte przypadki praktyk niezgodnych z zasadami etyki obowiązującej w nauce będą ujawniane, włącznie z powiadomieniem odpowiednich podmiotów (instytucji zatrudniających autorów, towarzystw naukowych, stowarzyszeń edytorów naukowych itp.).
30. Redakcja zwraca uwagę, że 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 przez Redakcję dokumentowane.

[*] Z *ghostwriting* mamy do czynienia wówczas, gdy ktoś wniósł istotny wkład w powstanie publikacji, ale jego udział jako autora nie zostaje ujawniony lub choćby uwzględniony w podziękowaniach dołączonych do tekstu.

[**] Sytuacja określana też jako *honorary authorship* – osoba podana jako autor czy współautor tekstu miała znikomy udział lub wcale nie uczestniczyła w tworzeniu publikacji.