Nr 4 (3) 2011

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

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

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

WARSZAWA 4 (3) 2011

INTERNAL SECURITY REVIEW

WARSZAWA 4 (3) 2011

Rada naukowa

Prof. dr hab. Brunon Hołyst
Prof. dr hab. Krzysztof Indecki
Prof. dr hab. Andrzej Mania
Prof. dr hab. Piotr Mickiewicz
Prof. dr hab. Stanisław Sulowski
Prof. dr hab. Sebastian Wojciechowski
Prof. dr hab. Konstanty A. Wojtaszczyk

Rada konsultacyjna COS ABW

Krzysztof Kozłowski (przewodniczący)
Andrzej Barcikowski
Paweł Białek (wiceprzewodniczący)
Piotr Niemczyk
Antoni Podolski
Bartłomiej Sienkiewicz
Marek Szczur – Sadowski
Piotr Potejko (sekretarz)

Recenzenci

dr hab. Andrzej Krzysztof Kunert
dr hab. prof. UWM Bronisław Młodziejowski

Zespół redakcyjny

Piotr Potejko (redaktor naczelny)
Piotr Tchorzewski (zastępca redaktora naczelnego)
Zbigniew Nawrocki (sekretarz redakcji)
Antoni Podolski (konsultacja merytoryczna)
Anna Przyborowska (redakcja i korekta)

© Copyright by Agencja Bezpieczeństwa Wewnętrznego
Centralny Ośrodek Szkolenia, Emów 2011

ISSN 2080-1335

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

Redakcja:
tel. (+48) 22 58 58 600
fax (+48) 22 58 58 693
e-mail: redakcja.pbw@abw.gov.pl

www.abw.gov.pl

Skład i druk: Biuro Administracyjno-Gospodarcze
Agencji Bezpieczeństwa Wewnętrznego
00-993 Warszawa, ul. Rakowiecka 2A
tel. (+48) 022 58 57 657

Spis treści

Contents

I
ANALIZY

Maria Wągrowska

NATO – pytania o przyszłość

Nowa *Koncepcja strategiczna obrony i bezpieczeństwa członków Organizacji Traktatu Północnoatlantyckiego,* przyjęta 20 listopada 2010 r. na szczycie przywódców 28 państw członkowskich w Lizbonie, to niewątpliwie dokument bardzo ważny[1]. Przedstawia bowiem ogólne założenia strategiczne całej wspólnoty transatlantyckiej na najbliższą dekadę, zakreślając tym samym ramy, w których NATO miałoby działać. A biorąc pod uwagę znaczenie i rolę tej najsilniejszej instytucji bezpieczeństwa i obronności współczesnego świata, *Koncepcja* ta jest najważniejszym dokumentem, jaki pojawił się od 1999 r.

Nie wolno jednak zapominać, że Sojusz Północnoatlantycki relatywnie traci na swoim znaczeniu, gdyż punkt ciężkości światowej polityki przemieszcza się w kierunku Pacyfiku. Czynników, które będą wpływać na jego kształt jest tak wiele, są tak zróżnicowane i powiązane ze sobą, że wyrokowanie o przyszłości Sojuszu w perspektywie nawet jednej dekady, którą brano przecież pod uwagę, koncypując nowy dokument strategiczny, mijałoby się z celem. Nieprzewidywalność rozwoju sytuacji międzynarodowej, i w związku z tym jej niepewność, to cechy obecnego, pozimnowojennego okresu. Te cechy zarysowują się obecnie bardziej niż w pierwszej fazie po zakończeniu zimnej wojny, czyli w latach 90. A nadal nie występują przesłanki, które wskazywałyby na to, że w dającym się przewidzieć czasie wyłoni się jakiś nowy układ międzynarodowego bezpieczeństwa. Na problemy, które przeżywa NATO, należy więc patrzeć i oceniać je przez pryzmat skomplikowanej sytuacji ogólnej, a nie tylko tej organizacji.

Nowy, wyżej wymieniony, dokument ma nie tylko charakter strategiczny. Wskazuje bowiem nie tylko na rolę, jaką NATO chciałoby odgrywać w polityce bezpieczeństwa, lecz także jest koncepcją mogącą przyczynić się do rozwoju polityki obronnej tej organizacji, bardziej celowego planowania obronnego i działań operacyjnych opartych m.in. na nowych zdolnościach oraz nowej strukturze dowodzenia i kierowania.

Na podstawie *Koncepcji strategicznej* można by scharakteryzować profil dzisiejszego Sojuszu jako organizacji spójnej i solidarnej, która jako swój priorytet traktuje kolektywną obronę zarówno terytorium każdego państwa członkowskiego, jak i całego własnego terytorium. Takie właśnie NATO odpowiada Polsce. Szczyt lizboński uznano powszechnie za sukces, zdając sobie sprawę, że to nie dokument końcowy jako taki będzie jego miarą, lecz jego wdrożenie do praktyki. *Teraz najważniejsza będzie operacjonalizacja koncepcji strategicznej, przełożenie jej ogólnych zapisów na konkretne dyrektywy, plany i programy* – podkreśla Stanisław Koziej[2], skłaniając się ku ogólnej opinii specjalistów. Ale tu można postawić jeszcze bardziej konkretne pytanie: czy uda się utrzymać consensus wśród państw członkowskich równocześnie w trzech powiązanych ze sobą sferach wymienionych w dokumencie z Lizbony, tj. co do kształtu polityki bezpieczeństwa NATO, ambicji politycznych Sojuszu do odgrywania ważnej roli międzynarodowej i jego zdolności wojskowych.

---

[1] Dokument o nazwie *Active Engagement, Modern Defence. Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organisation adopted by Heads of State and Government in Lisbon*, www.nato.int/cps/en/natolive/official_texts_68580.htm [dostęp: 20.11.2010]. Tekst polskojęzyczny pochodzący z 17 stycznia br. znajduje się na www.bbn.gov.pl/dokumenty.

[2] W: *Nowa Koncepcja strategiczna NATO a Strategiczny Przegląd Bezpieczeństwa Narodowego*, „Bezpieczeństwo Narodowe" 2011, nr 3/4.

Pewniki i wątpliwości

Mówienie o powodzeniu szczytu lizbońskiego i znaczeniu nowej *Koncepcji Strategicznej* należy od razu opatrzyć zasadniczymi zastrzeżeniami, które będą je relatywizować zarówno jeśli chodzi o spoistość Sojuszu, jak i o jego podstawowe funkcje, łącznie z obronną. Pierwsze generalne zastrzeżenie odnosi się do podejścia Stanów Zjednoczonych, które wprawdzie opowiadają się za wzmocnieniem NATO i więzi transatlantyckich, ale w swojej polityce kierują się przede wszystkim doktryną bezpieczeństwa narodowego, będąc w gotowości i, oczywiście, mając zdolności do samodzielnych działań wojskowych zakrojonych na większą skalę niż jakiekolwiek inne państwo i niekoniecznie uzgodnionych z wszystkimi sojusznikami. Warto tu jednak odnotować, że w opinii obserwatorów nowa *Koncepcja strategiczna* powstawała pod dominującym wpływem dyplomacji politycznej i wojskowej USA. A skoro tak, to oznaczałoby to, że Stany Zjednoczone świadomie wzięły na siebie odpowiedzialność za kształt Sojuszu, w tym za spełnianie przez tę organizację funkcji obronnych. Drugie zastrzeżenie dotyczy postawy Unii Europejskiej, w tym największych państw członkowskich, zwłaszcza Francji, wobec NATO. Nie w każdym aspekcie można ją zakwalifikować jako przejaw dążenia do tego, by UE rozwijała swoją politykę bezpieczeństwa i obrony jako „europejski filar" Sojuszu. I trzecia obiekcja: praktyka ostatnich kilku miesięcy, które upłynęły od lizbońskiego szczytu i przyjęcia nowej *Koncepcji strategicznej* wskazują, że Sojusz Północnoatlantycki ma nadal wiele tych samych lub podobnych problemów, które stały na drodze do większej spójności i solidarności państw członkowskich, również przed przyjęciem najnowszego dokumentu programowego. Dobitnym świadectwem jest tutaj operacja libijska. Najbardziej palące z tych problemów są natury politycznej i zawierają się w następujacych pytaniach zasadniczych:

1) Czy, pomimo pełnej międzynarodowo-prawnej legitymizacji działań przeciwko reżimowi libijskiemu[3] i stosownych decyzji przyjętych przez Sojusz na zasadach wymaganego consensusu, NATO jest spójne i solidarne?
2) Czy fakt, że w ramach NATO istnieją państwa o wyższej od innych determinacji do działania poza obszarem traktatowym, ale we własnym (głównie politycznym i gospodarczym), a nie wspólnym interesie całej organizacji, oraz państwa powstrzymujące się od aktywnego zaangażowania w operacje, nie wskazuje na niebezpieczeństwo podziałów w Sojuszu?
3) Czy NATO, dzieląc się ewentualnie na różne kategorie państw, nie zmierza w tym samym kierunku, co Unia Europejska, która może stać się organizacją różnych prędkości rozwojowych?
4) Jak w związku z tym przedstawiają się główne wyzwania dla państw, które nie chcą brać udziału w danej akcji ze względów politycznych lub nie byłyby w stanie uczestniczyć w operacji wojskowej ze względu na swój skromny potencjał?
5) Czy i jakie konsekwencje dla udziału całego Sojuszu w operacji obronnej państwa czy też państw położonych na obszarze traktatowym NATO, w tym Europy Środkowej i Wschodniej, mogą w takim razie się pojawić?
6) Jakie konsekwencje może mieć operacja libijska dla ewentualnych przyszłych misji NATO poza obszarem traktatowym? A jakie dla współpracy Sojuszu z jego partnerami ?

[3] Fakt, że rezolucja Rady Bezpieczeństwa ONZ nr 1973 może być szeroko interpretowana i wykorzystywana, to sprawa odrębna.

Do tych zasadniczych kwestii politycznych dochodzi wiele pytań dotyczących problematyki wojskowej, głównie zdolności operacyjnych państw członkowskich podczas misji (gdyż pojawiły się uderzające różnice w poziomie ich rozwoju technicznego i technologicznego), pożądanego modelu armii w różnych krajach[4], ich finansowania w taki sposób, by zmniejszać różnice w poziomie modernizacji oraz podziału zadań podczas przyszłych hipotetycznych akcji Sojuszu itp. Kwestie te długo będą absorbować wszystkich zainteresowanych polityką bezpieczeństwa. Dzisiaj trudno jest wyrokować nawet co do tego, czy zapowiadany na jesień 2012 r. szczyt NATO w Waszyngtonie zdoła na te pytania odpowiedzieć. Podczas wykładu wygłoszonego w czasie niedawnej wizyty u prezydenta USA, Sekretarz Generalny NATO stwierdził jedynie, że *szczyt waszyngtoński napisze nowy rozdział w ewolucji i transformacji NATO.*

Kryzys czy ewolucja

Obecnie obowiązujący dokument (*Koncepcja strategiczna*) prezentuje siódmą strategię sojuszniczą od chwili powstania paktu (4 kwietnia 1949 r.), a trzecią w okresie pozimnowojennym. Co ciekawe, dopiero te trzy strategie okresu pozimnowojennego (z 1991 r. z Rzymu, z 1999 r. z Waszyngtonu i z 2010 r. z Lizbony) są strategiami jawnymi, ale nie tylko one są realnie obowiązującymi dokumentami Sojuszu. Oprócz nich istnieją bowiem niepublikowane, niejawne wytyczne ministerialne i inne dokumenty przyjmowane w nieregularnych odstępach czasu, które w dużej części współkształtują praktyczne postępowanie, w tym w sferze obronności państw członkowskich. I tak, uzupełnieniem nowej *Koncepcji strategicznej* z Lizbony ma być, według nieoficjalnych doniesień, kilkusetstronicowy dokument, w którym jest mowa o możliwych konkretnych reakcjach NATO na zagrożenia terrorystyczne, konwencjonalne, nuklearne i inne[5]. Fakt istnienia dokumentów uzupełniających strategię, jakże często pomijany w literaturze przedmiotu, nakazuje powściągliwość w ocenie *Koncepcji* (co nie znaczy, że ocena ta jest negatywna).

Nowa *Koncepcja* musiała uwzględniać wszelkie doświadczenia z udziałem NATO zdobyte w wyjątkowym okresie minionych kilkunastu lat, a więc: przechodzenie od zimnej wojny do obecnego stanu w stosunkach międzynarodowych, zwłaszcza w obszarze euroatlantyckim; poszerzenie Sojuszu na wschód (w tym o Polskę[6]) i połączenie tego procesu z nadaniem nowego kształtu relacjom z Rosją, Ukrainą, Gruzją i pozostałymi państwami postradzieckimi; natężenie terroryzmu w jego różnych formach i próby zwalczania tego zjawiska (zwłaszcza w Iraku i Afganistanie); pojawienie się jakościowo nowych wyzwań i zagrożeń dla bezpieczeństwa, m.in. energetycznego i teleinformatycznego. Sojusz Północnoatlantycki miał (i nadal ma) dwa wielkie problemy związane ze swoją tożsamością, a mianowicie legitymizację funkcjonowania we własnych społeczeństwach oraz trudności z finansowaniem sektora obronnego w państwach członkowskich. Ponadto pogłębia się różnica w nakładach na obronność pomiędzy USA a europejskimi członkami NATO.

---

[4] Chodzi o model z przewagą funkcji obronnych lub ekspedycyjnych.

[5] Porównaj tekst znawczyni problematyki bezpieczeństwa, Judy Dempsey, pt: *NATO Document Adresses Nuclear Disarmament*, „International Herald Tribune" z dnia 30.09.2010 r.

[6] Precyzyjnie mówiąc: przyjęcie do NATO Polski, Czech i Węgier jako pierwszych państw postkomunistycznych nastąpiło 12 marca 1999 r., czyli miesiąc przed pojawieniem się poprzedniej strategii, ale nasze kraje były konsultowane co do jej treści.

W związku z wszystkimi tymi problemami dotyczącymi sytuacji międzynarodowej oraz z uwagi na konieczność znalezienia wspólnego mianownika dla interesów narodowych i celów strategicznych 28 demokratycznych państw, nowa *Koncepcja* nie wyłaniała się w sposób prosty. Kryzys NATO, powstały głównie wskutek rozluźnienia więzi transatlantyckich oraz niepowodzenia operacji afgańskiej, potęgował wątpliwości dotyczące sukcesu prac nad tym dokumentem. Pojawiały się pytania, czy nie będzie on jedynie kompilacją treści z poprzedniej *Koncepcji* i treści nowych. Następnie, przedstawienie przez stronę rosyjską tzw. planu Miedwiediewa, czyli propozycji nowej architektury europejskiej (mimo formalnego jej odrzucenia przez NATO) spowodowało na Zachodzie dyskusję nad jakąś formą modyfikacji systemu bezpieczeństwa europejskiego. Intensywna praca tzw. Grupy Mędrców, powołanej do analizy funkcjonowania NATO i projekcji na przyszłość[7], nie przyniosła przełomu w debacie nad kształtem nowej *Koncepcji*, aczkolwiek przygotowała pod nią grunt, odnosząc się do wszystkich możliwych aspektów bezpieczeństwa. Wśród specjalistów trwał (nadal zresztą nie rozstrzygnięty) spór, czy problemy wewnątrz NATO są pochodną kryzysu tej organizacji, być może nieodwracalnego, czy też ewolucji rozumianej jako adaptacja do wszystkich możliwych wyzwań politycznych, wojskowych, strukturalnych i organizacyjnych. Wątek „kryzys czy ewolucja" jest obecny w debacie również po przyjęciu nowej *Koncepcji strategicznej*, a świadom tego problemu A.F. Rasmussen twierdzi, że *jedną z przyczyn sukcesu NATO jest jego zdolność adaptacji do nowych uwarunkowań*.

Szczególnie ważnym, również z polskiego punktu widzenia, elementem strategicznej debaty o przyszłości Sojuszu (która odżyła po rozpoczęciu operacji libijskiej) jest dyskusja dotycząca kierunku dążeń i funkcjonowania Sojuszu, tj. czy NATO ma być organizacją globalną, mającą polityczne i wojskowe zdolności do interwencji w różnych częściach świata, co zakłada praktycznie wsparcie przez tę organizację dla możliwych akcji amerykańskich, francuskich, brytyjskich, względnie koalicyjnych. Czy też absolutnym priorytetem dla tej organizacji powinna pozostać obrona terytorium? Państwa wschodniej części obszaru NATO, w tym przede wszystkim Polska i Czechy, stały się poniekąd adwokatami drugiej opcji. Na ich postawę (a także na podstawę innych krajów) duży wpływ wywarła wojna gruzińsko-rosyjska z sierpnia 2008 r., jej przebieg oraz faktyczne anektowanie przez Rosję terytoriów abchaskiego i południowoosetyńskiego.

Elementem przesądzającym o kształcie *Koncepcji* stało się dopiero osobiste zaangażowanie Sekretarza Generalnego NATO w jej powstanie. Anders Fogh Rasmussen, wcześniej premier Danii, który przyczynił się do poszerzenia Unii Europejskiej w 2004 r. m.in. o Polskę, został de facto głównym autorem tego dokumentu. Jednakże w trakcie wcześniejszych prac, prowadzonych przez rok (przywódcy państw członkowskich zadecydowali o przygotowaniu nowej *Koncepcji* w roku 2009), udało się w sposób usystematyzowany i transparentny przeprowadzić szeroką debatę publiczną. W pierwszej fazie odbyła się ona z udziałem wielu ośrodków opiniotwórczych i autorytetów z dziedziny politologii[8], neutralizując w dużej mierze panujące w tych środowiskach nastroje sceptycyzmu wobec przyszłości NATO. Był to ważny dla Sojuszu moment psychologiczny. W drugiej fazie obradowała wspomniana Grupa Mędrców, kierowana

[7] Warto dodać, że Grupa zapoznawała się również ze stanowiskiem państw partnerskich NATO, w tym podczas pobytu w Moskwie ze stanowiskiem Rosji.

[8] www.nato.int.

przez byłą sekretarz stanu USA Madeleine Albrihgt (z udziałem m.in. Adama D. Rotfelda, byłego ministra spraw zagranicznych RP), która 17 maja 2010 r. przedłożyła dokument o nazwie *NATO 2020: Assured Security; Dynamic Engagement*[9]. Trzecia i ostatnia faza to właśnie powstanie nowej *Koncepcji Strategicznej*. Jej projekt został przedłożony 27 września ubiegłego roku i szybko zaakceptowany na szczeblu ministerialnym, a następnie podczas lizbońskiego szczytu.

W trakcie dochodzenia do consensusu niezbędnego do przyjęcia *Koncepcji* państwa członkowskie zgodziły się na pewne założenia dotyczące podejścia do zasadniczych roblemów. Było to przede wszystkim powstrzymanie w trakcie debaty poprzedzającej przyjęcie dokumentu wspomnianych negatywnych tendencji w transatlantyckiej polityce obronnej, to znaczy powrót do myślenia o NATO jako o organizacji obrony zbiorowej, ale bez odwrotu od koncepcji Sojuszu ekspedycyjnego, globalnego. W wyniku zarzucenia tego niebezpiecznego trendu jeszcze przed szczytem można się było spodziewać przyjęcia tzw. planów ewentualnościowych, niewycofania się NATO z doktryny odstraszania oraz potwierdzenia tożsamości Sojuszu. Nie przystano bowiem na inną formułę systemu bezpieczeństwa europejskiego niż ta oparta na istniejących strukturach, traktatach i porozumieniach. Osiągnięto postęp w sprawie tworzenia systemu antyrakietowego oraz ponownie zaczęto myśleć o kontroli zbrojeń, w tym konwencjonalnych. Oznaczało to, że ewolucja NATO, zwana też często adaptacją, polegająca na dostosowywaniu się do nowych wyzwań, nie poszła aż tak daleko, by zachwiać podstawami istnienia samej organizacji ujętymi w akcie założycielskim, czyli w *Traktacie Waszyngtońskim*. Przyjęcie tego dokumentu powstrzymało też w pewnej mierze tendencje do renacjonalizacji polityki bezpieczeństwa i obronności niektórych najsilniejszych państw członkowskich oraz głośne preferowanie przez nie europejskiej polityki bezpieczeństwa, rozumianej jako polityka autonomiczna bądź alternatywna wobec NATO[10]. Elementy te stanowią o wartości nowej *Koncepcji*, aczkolwiek dokument ten nie przynosi przełomu.

Materiały ze szczytu lizbońskiego[11] należy traktować we wzajemnym związku. Wyrażają one kompromis – co jest oczywiste przy przyjmowaniu dokumentów przez wiele państw. *Dokumenty szczytu są zapisem kompromisu wynikającego z konieczności godzenia różnorodnych, niejednokrotnie sprzecznych ze sobą postulatów, dotyczących większości aspektów funkcjonowania NATO z jego strategicznymi celami włącznie. W kwestiach budzących kontrowersje przyjęte zapisy są najczęściej nieprecyzyjne, o wysokim stopniu ogólności.* W taki sposób dokumenty te charakteryzują eksperci z Ośrodka Studiów Wschodnich[12]. Należy jednak przede wszystkim wziąć pod uwagę, że kompromisowe formuły nie zmieniają istoty funkcjonowania Sojuszu i w tym sensie mogą być punktem wyjścia do dalszej ewolucji tej organizacji bez naruszania jej funkcji obronnej.

---

[9] Tamże lub: www.nato.int/ebookshop.

[10] Z wojskowego punktu widzenia ważne wydaje się zwłaszcza podkreślenie, że już w listopadzie 2006 r., na szczycie w Rydze, NATO przyjęło tzw. *Kompleksowe wytyczne polityczne* nadające kierunek transformacji. Odnoszą się one głównie do zdolności operacyjnych oraz różnych aspektów planowania obronnego.

[11] Równocześnie z nową *Koncepcją strategiczną* zostały przyjęte dokumenty o nazwach: *Deklaracja Szczytu lizbońskiego*, *Wspólne oświadczenie Rady NATO–Rosja*, *Deklaracja o trwałym partnerstwie pomiędzy NATO a rządem Afganistanu* oraz *Deklaracja przywódców państw uczestniczących w dowodzonej przez NATO misji ISAF w Afganistanie*.

[12] *NATO po szczycie w Lizbonie – konsekwencje dla Europy Środkowej i Wschodniej*, „Biuletyn OSW" 2010, nr 39.

Nieznana rzeczywistość, tradycyjne przesłanie

Największym walorem nowej *Koncepcji strategicznej* jest przyznanie, że środowisko bezpieczeństwa zyskało nową jakość, ale jednocześnie, że w nowych uwarunkowaniach Sojusz pozostaje organizacją zbiorowej obrony, a nie regionalnym systemem bezpieczeństwa czy wręcz – jak w pewnym momencie okresu pozimnowojennego można się było obawiać – „klubem" państw.

Jako główne zadanie NATO określa się zapewnianie wolności i bezpieczeństwa państw członkowskich za pomocą środków politycznych i wojskowych w trzech dziedzinach: kolektywnej obrony (*collective defence*), zarządzania kryzysowego (*crisis management*) i bezpieczeństwa zbiorowego (*cooperative security*). Z przywołaniem art. 5 *Traktatu Waszyngtońskiego*, mówiącego o zakresie gwarancji bezpieczeństwa (a nie o natychmiastowo i automatycznie uruchamianych gwarancjach) podkreśla się, że gdy fundamentalne bezpieczeństwo pojedynczych członków lub całej wspólnoty będzie zagrożone, państwa członkowskie będą się nawzajem wspomagać i bronić.

Zagrożenie atakiem konwencjonalnym na obszar Sojuszu zostało określone jako niewielkie, niemniej jednak wymieniono kilka elementów zagrażających bezpieczeństwu tego obszaru, tj.: proliferację rakiet balistycznych, broni nuklearnej i innych rodzajów broni masowego rażenia, terroryzm (łącznie z opcją posiadania przez ugrupowania terrorystyczne środków nuklearnych, chemicznych, biologicznych i radiologicznych), niestabilność na granicach obszaru NATO oraz ataki cybernetyczne.

Podstawowymi zadaniami Sojuszu pozostają obrona oraz odstraszanie, uwzględniające możliwość użycia broni zarówno nuklearnej, jak i konwencjonalnej. NATO pozostanie aliansem nuklearnym tak długo, jak długo będzie istniała ewentualność użycia broni nuklearnej. W *Koncepcji* wymienia się wiele środków i zdolności rozwiniętych w celu zapobieżenia niebezpieczeństwu, względnie zwalczenia go, w tym zdolność do przeprowadzenia różnego rodzaju operacji wojskowych z udziałem silnych, mobilnych i dyspozycyjnych jednostek, budowę systemu antyrakietowego, zdolność do obrony na wypadek ataków z użyciem środków chemicznych, biologicznych, radiologicznych, nuklearnych i cybernetycznych oraz do zwalczania terroryzmu i ochrony infrastruktury krytycznej.

W drugiej kolejności w *Koncepcji* wymienia się zarządzanie kryzysowe, gdyż, według dokumentu, z kryzysów i konfliktów w miejscach położonych poza obszarem NATO mogą wypływać bezpośrednie zagrożenia dla bezpieczeństwa tego Sojuszu. Stąd zapis o zaangażowaniu w zapobieganie kryzysom, rozwiązywaniu sytuacji pokonfliktowych i odbudowie po konflikcie, który wyniszcza ludność, infrastrukturę i różnego rodzaju obiekty. Jednym z elementów dokumentu jest więc zapis o współpracy strony wojskowej z cywilną.

W sferze bezpieczeństwa zbiorowego – niezależnie od kwestii związanych z kontrolą zbrojeń, rozbrojeniem i nieproliferacją broni i środków masowego rażenia, a także deklaracji „otwartych drzwi" przed nowymi państwami członkowskimi – wiele miejsca zajmuje partnerstwo NATO z innymi organizacjami międzynarodowymi oraz krajami. Dzięki współpracy z Unią Europejską[13], Narodami Zjednoczonymi oraz organizacjami

[13] Współpraca NATO z Unią Europejską napotyka na olbrzymie trudności głównie ze względu na wzajemne blokowanie się Grecji (będącej członkiem obu organizacji) i Turcji (nie należącej do UE) na tle zaszłości w stosunkach dwustronnych, w tym na tle sprawy Cypru.

pozarządowymi struktura ta chciałaby rozwinąć tzw. kompleksowe podejście (*comprehensive approach*), aby przy współpracy wojskowych i cywili móc łatwiej sprostać różnym nowym wyzwaniom. Sojusz zawarł ponad 60 porozumień dotyczących współpracy z różnymi krajami. Chciałby je wykorzystać do umocnienia bezpieczeństwa oraz zaangażowania krajów partnerskich w obszarach, na których prowadzi się misje.

Szczególną uwagę w wyżej wymienionym dokumencie przykuwa formuła odnosząca się do współpracy NATO z Federacją Rosyjską – zarówno ze względu na wagę polityczną tego zagadnienia, jak i na inne aspekty, zwłaszcza dotyczące obrony antyrakietowej, zwalczania terroryzmu, przemytu narkotyków oraz piractwa na akwenach międzynarodowych. W zasadzie żaden z tych aspektów nie jest nowy. Niemniej jednak problem współpracy z Rosją w tych zakresach przyciągał uwagę wszystkich obserwatorów; oczekiwano odpowiedzi na pytania, czy Sojusz zaproponuje temu państwu – i osobiście jego prezydentowi, który przybył do Lizbony na spotkanie Rady NATO–Rosja – jakąś nową formułą tej współpracy, która byłaby wynikiem debaty strategicznej poprzedzającej szczyt. NATO i Rosja pracują nad wspólnym podejściem do zagrożeń, które mogą wystąpić w szeroko pojętym obszarze euroatlantyckim, w tym i postsowieckim. Taka kooperacja może być postrzegana jako trafna nie tylko z politycznego punktu widzenia, gdyż neutralizuje dążenia do modyfikacji europejskiego systemu bezpieczeństwa i tworzenia dodatkowych, względnie nowych, struktur bezpieczeństwa, lecz także „wewnętrznie", dla samego NATO. Pozwala bowiem skoncentrować się na praktycznej działalności państw członkowskich oraz sojuszniczych Sekretariatów Międzynarodowych (politycznych i wojskowych), w tym na przeglądzie zagrożeń dokonanym we współpracy z Rosją[14].

Demonstracja zdolności

Kilka miesięcy, które upłynęły od przyjęcia *Koncepcji*, nie podważa zasadniczych założeń poczynionych w tym dokumencie. Pokazuje natomiast, że Sojusz w każdej chwili może stanąć przed nowymi nieprzewidywanymi wyzwaniami politycznymi. Z kolei jednak wojskowa operacja w obronie ludności cywilnej, a przeciwko reżimowi libijskiemu, nie przeczy założeniom odnoszącym się do roli NATO jako organizacji obrony zbiorowej. Można by nawet spróbować udowodnić, że zdolności militarne i środki walki wykorzystane w jej trakcie demonstrują sojuszniczy potencjał odstraszania. Pokazują bowiem szerokie możliwości ekspedycyjne Sojuszu, który jest w stanie przeprowadzić akcję zbrojną w Afryce Północnej równolegle z zaangażowaniem w Afganistanie (obie operacje – pomimo zróżnicowanego charakteru – angażują największe państwa członkowskie).

Pytanie, które musi się nasuwać z naszego polskiego punktu widzenia, brzmi: czy NATO byłoby w stanie prowadzić skuteczną operację obronną na dużą skalę, wynikającą z jego roli jako organizacji obrony zbiorowej, równocześnie z poważnymi operacjami ekspedycyjnymi? Odpowiedź można znaleźć, śledząc komentarze związane

[14] Przegląd ten został ujęty w dokumencie nieupublicznionym, w którym obie strony ustosunkowały się do terroryzmu, kwestii afgańskiej, piractwa i ochrony infrastruktury krytycznej, nie odnoszącym się jednak do spraw tak zasadniczych, jak zagrożenia związane z bronią masowego rażenia i technologie rakietowe.

z pojawieniem się nowej *Koncepcji strategicznej* oraz tzw. planów ewentualnościowych. Okazuje się, że dowództwo NATO na Europę Północną z siedzibą w Brunssum (Holandia) byłoby w stanie równocześnie dowodzić jedną dużą operacją obronną oraz kilkoma mniejszymi o innym charakterze.

Pytanie o zdolność do przeprowadzenia operacji obronnych odnosi się właściwie tylko do hipotetycznej akcji w regionach Europy Środkowej, Wschodniej i Północnej, gdyż to one mogą być ewentualnie narażone na zagrożenie militarne, które wymagałoby odpowiedzi ze strony całego NATO. W tym miejscu należy postawić kolejne ważne pytanie: czy ze strony NATO miałoby chodzić o operację w odpowiedzi na nieprzyjazny akt z zaskoczenia (czyli poniżej progu wojny), na agresję czy też o jeszcze inną postać ataku? Spektrum możliwych incydentów i akcji zbrojnych jest teoretycznie bardzo szerokie i w związku z tym interpretacja, a przede wszystkim kwalifikacja, takiego aktu – również. Stąd wypływają nadzwyczaj wysokie wymagania wobec planowania obronnego, które musi być wielowariantowe.

W uproszczeniu można by przyjąć, że reakcja na atak o charakterze tradycyjnym byłaby „prostsza", niż na akt nietradycyjny, niekonwencjonalny i nieklasyczny. Czyli: pewność co do wsparcia ze strony sojuszników jest tym większa, im bardziej zagrożenie jest „klasyczne". Przypomnijmy sobie, że po 11 września, czyli po ataku skierowanym przeciwko Ameryce, NATO zadeklarowało przywołanie art. 5 *Traktatu Waszyngtońskiego* i było gotowe wesprzeć Stany Zjednoczone. *Koncepcja strategiczna* i towarzyszące jej dokumenty oraz deklaracje polityczne wskazywałyby na to, że w przypadku zagrożenia o charakterze militarnym, względnie paramilitarnym, moglibyśmy mieć do czynienia z dwiema opcjami wynikającymi albo z wyżej wymienionego artykułu 5, albo z artykułu 4 powyższego traktatu.

NATO a obrona Polski

Artykuł 5 *Traktatu Waszyngtońskiego* ma dla Polski znaczenie zasadnicze – nie tylko z powodów militarnych, politycznych i psychologicznych, ale także ze względu na ukierunkowanie wysiłku zbrojnego naszego kraju. Nieporozumieniem była jednak taka (spotykana w mediach) interpretacja, że przed szczytem NATO w Lizbonie Polsce zależało na utrzymaniu tego artykułu w mocy. Odnośny zapis znalazł się w traktacie założycielskim Sojuszu z 4 kwietnia 1949 r. i nigdy nie został poddany rewizji, ba, nigdy nawet nie wysuwano postulatów dotyczących zrewidowania go. Podnoszono jedynie – i tak też będzie zapewne w przyszłości – kwestię jego poszerzonej interpretacji związanej ze zwiększeniem zadań NATO o misje poza traktatowym obszarem działań (*out of area*). Obecnie, tzn. od szczytu w Rydze w grudniu 2006 r., wielokrotnie zapewniano, że artykuł 5 obowiązuje.

Polsce chodziło natomiast o potwierdzenie w nowej *Koncepcji strategicznej* zasady obrony zbiorowej, wyrażonej właśnie w art. 5 traktatu, a także o uaktualnienie tzw. planu ewentualnościowego (*contingency plan*), a w razie potrzeby – o jego przyspieszoną realizację. Postulat ten nie był zresztą nowy. Pojawiał się już wcześniej w polskich koncepcjach i był przedmiotem zabiegów dyplomacji jeszcze przed wstąpieniem naszego kraju do NATO. Plan ewentualnościowy został Polsce ostatecznie przyznany w roku 2001. Tym razem chodziło o jego adaptację do obecnych i przyszłych hipotetycznych zagrożeń oraz o zagwarantowanie szybszego nadejścia ewentualnej pomocy. Polskie Siły Zbrojne, występując w obronie własnego terytorium, mogą więc liczyć na pomoc wojsk sojuszniczych. Procedury związane z przerzutem obcych wojsk na pol-

skie terytorium mają być szybko realizowane i klarowne[15]. Minister spraw zagranicznych, Radosław Sikorski, wiąże decyzje odnoszące się do wzmocnienia polskiego bezpieczeństwa z budową wiarygodności Polski[16].

Według źródeł prasowych, *contingency plan* dla Polski, czyli rodzaj scenariusza na wypadek zagrożenia bezpieczeństwa, zawiera sojuszniczą pomoc już w pierwszej fazie działań operacyjnych. Główną rolę w dowodzeniu operacją odgrywałoby dowództwo strategiczne NATO zlokalizowane w Brunssum, które wyznaczałoby dowództwo tzw. wysokiej gotowości, odpowiedzialne za działania na terytorium wschodniej Europy i za przerzut oddziałów sojuszniczych do naszego kraju każdą z możliwych dróg (powietrzną, morską i lądową). Polski, według niepotwierdzonych danych, miałyby bronić cztery dywizje własne[17] i pięć sojuszniczych[18]. Główna rola przypadałyby obronie powietrznej, przy czym polski system tej obrony jest zintegrowany z NATO-wskim (w ramach programu NATINADS) od chwili przystąpienia naszego kraju do Sojuszu. Infrastruktura wojskowa na terenie Polski jest już w części przystosowana do wymogów NATO, niemniej opóźnienia w tej dziedzinie też są znaczne. Jak spekulują media, głównymi bazami wykorzystywanymi przez siły sojusznicze mogłyby być odpowiednio dostosowane pod tym kątem lotniska w Krzesinach k. Poznania oraz porty w Świnoujściu, Gdyni[19] i we wschodniej części Niemiec. Z pomocą miałyby przybywać oddziały amerykańskie, brytyjskie, niemieckie i holenderskie. Myśląc o konieczności przyjęcia wsparcia sojuszniczego na własnym terytorium, Polska jest przygotowana, aby pełnić rolę państwa gospodarza (według zasady: *Host Nation Support* – HNS), które jest w stanie zapewnić oddziałom sojuszniczym (uzbrojeniu, sprzętowi i całemu wyposażeniu) odpowiednie zaplecze. Pobyt i stacjonowanie wojsk sprzymierzonych na terenie danego kraju jest możliwe z prawnego punktu widzenia na podstawie stosownych regulacji obowiązujących w NATO i znanych pod ogólną nazwą SOFA. Niejawny charakter planu ewentualnościowego powoduje, że nie jest znana obecna faza prac nad tym wyjątkowo ważnym przedsięwzięciem.

Niezależnie od *contingency plan*, pomyślanego na wypadek agresji na większą skalę, ważnym elementem byłaby pomoc ze strony NATO-wskich Sił Odpowiedzi – SON (*NATO Responce Forces* – NRF), jako sił mogących reagować „natychmiast", względnie „szybko", na zagrożenia. NRF (20 tys. żołnierzy) od dłuższego czasu są przygotowywane przez NATO do ewentualnej reakcji. Są one zdolne do działania poza

[15] To znaczy, chodziło o skrócenie procedur, które wymagały czasochłonnych konsultacji w ramach Rady Północnoatlantyckiej (najwyższego organu NATO), aczkolwiek siły powietrzne NATO mogłyby przystąpić do akcji natychmiastowej. Plany pomocy wojskowej mają właściwie wszystkie państwa europejskie, w szczególności te położone na granicy terytorium NATO, czyli głównie Norwegia, chociaż kraj ten nie otrzymał ostatnio uaktualnionego planu. We wrześniu 2007 r. w Norwegii powstał oficjalny raport, w którym znalazła się teza o znikomym znaczeniu tzw. *contingency plan* dla tego państwa. Planem ewentualnościowym po raz pierwszy zostaną objęte również państwa nadbałtyckie. Plan dla Litwy, Łotwy i Estonii zakłada, według danych prasowych, przerzucenie z Zachodu drogą morską i powietrzną (a z Polski lądową) dwóch dywizji (amerykańskiej i niemieckiej). Byłyby one wspierane przez lotnictwo.

[16] Por.: *Exposé* ministra spraw zagranicznych, 2011,41979.html.

[17] Prawdopodobne, że byłyby to: 1. Warszawska Dywizja Zmechanizowana, 11. Lubuska Dywizja Kawalerii Pancernej, 16. Pomorska Dywizja Zmechanizowana i 12. Szczecińska Dywizja Zmechanizowana.

[18] Chodziłoby o jednostki USA stacjonujące w RFN, jak np. 7. Armię, 3. Dywizję Brytyjską, holenderską 11. Brygadę Mobilną, ewentualnie 13. Dywizję Grenadierów Pancernych z Lipska lub nawet niemiecką 7. Dywizję stacjonującą w okolicach Dűsseldorfu.

[19] Mogą one przyjąć duże jednostki pływające, czyli do 200 m długości i o zanurzeniu powyżej 10 m.

obszarem obowiązywania *Traktatu Waszyngtońskiego*, ale jeszcze nie w pełni gotowe do przeprowadzenia znaczniejszej akcji. Według koncepcji polskiej, siły te powinny być wielofunkcyjne, tzn. zdolne do interwencji również w obronie terytorium Polski, stanowiąc część sił wzmocnienia[20], które miałyby przyjść naszemu krajowi z pomocą.

Plan pomocy dotyczący ewentualnego zagrożenia bezpieczeństwa oraz wsparcie Sił Odpowiedzi mają dla Polski kapitalne znaczenie jako tzw. „widoczne" gwarancje bezpieczeństwa (*visible assurances*). Należy przyjąć, że są one realne, to znaczy, że w przypadku ewidentnego niebezpieczeństwa NATO udzieliłoby Polsce pomocy militarnej. Można natomiast spekulować, czy gwarancje te byłyby w takim samym stopniu rzeczywiste, gdyby w ocenie naszych sojuszników zagrożenia nie były aż tak ewidentne, jak agresja i trudne do zakwalifikowania przez Sojusz jako wymagające udzielenia pomocy i interwencji zbrojnej. Tymczasem nie można wykluczyć wystąpienia zagrożeń z pogranicza tych „najpoważniejszych" i „nie aż tak poważnych", ale charakteryzujących się wysoką intensywnością. Rozwiązanie tego typu problemów stanowi duże wyzwanie dla polityki bezpieczeństwa.

Sfera funkcjonowania NATO, mająca odniesienia do zarządzania i reagowania kryzysowego oraz do odpowiedniego przygotowania również instytucji cywilnych na wypadek pojawienia się zagrożeń, nabiera coraz większego znaczenia. W Kwaterze Głównej NATO powstał[21] w związku z tym specjalny 100-osobowy wydział zajmujący się analizą nowych zagrożeń i możliwymi reakcjami na nie. Jest to Wydział ds. Nowych Wyzwań dla Bezpieczeństwa (*Emerging Security Challenges Division*). NATO stara się animować współpracę pomiędzy cywilnymi instytucjami zajmującymi się zarządzaniem kryzysowym w państwach członkowskich i partnerskich oraz rozwijać współpracę cywilno-wojskową, by również w ten sposób przygotować się do reakcji na pojawienie się ewentualnych niebezpieczeństw. Ten stosunkowo nowy kierunek działań powinien być w Polsce uwzględniany w większym stopniu niż jest.

W nowej *Koncepcji strategicznej* nie ma już jednak mowy o tym, że odpowiedź na nowe zagrożenia wynikałaby z artykułu 5. *Traktatu Waszyngtońskiego*. Zamiast tego podkreśla się, że NATO jest koniecznym forum konsultacji we wszystkich kwestiach dotyczących integralności terytorialnej, niezależności politycznej i bezpieczeństwa państw członkowskich, zgodnie z zasadami ujętymi w artykule 4. tego traktatu. Jest to pewna zmiana w porównaniu z zapisami wcześniejszymi. Strategia z 1999 r. (pkt 31) poszerzała zastosowanie art. 5 o sytuacje kryzysowe w obszarze euroatlantyckim – z odwołaniem do prawa międzynarodowego i współpracy z innymi organizacjami międzynarodowymi. W tym miejscu należy jednak ponownie zastrzec, że jedynie pod warunkiem dogłębnej znajomości procesów planistycznych w ramach NATO można wyrokować o zakresie gwarancji bezpieczeństwa.

W kontekście powyższego warto zwrócić uwagę na status bezpieczeństwa Rzeczpospolitej Polskiej (i innych państw członkowskich z Europy Środkowej, położonych na styku ze Wschodem). Jest on o tyle niższy od statusu państw zachodnioeuropej-

[20] Decyzją ministrów obrony państw NATO z lutego 2010 r. SON/NRF mają wyznaczony 4-letni plan szkoleń aplikacyjnych, sztabowo-dowódczych oraz poligonowych, z których pierwsze miałyby odbyć się w Polsce w połowie 2013 r. W roku 2011 w XVI i XVII składzie NRF znajduje się 300 wojskowych z 1. Pomorskiej Brygady Logistycznej z Bydgoszczy.

[21] Wydział ten funkcjonuje od sierpnia 2010 r.

skich, że z jednej strony nasz region jest w większym stopniu narażony na ewentualność wystąpienia zagrożeń, a z drugiej – mniej jest tu zaznaczona obecność wojskowa Sojuszu. Obecność militarna NATO, która jest w naszej części Europy ograniczona z wielu względów historycznych, politycznych, wojskowych i finansowych, uważana jest za jedną z gwarancji bezpieczeństwa. Wychodzi się bowiem z założenia, że Sojusz broniłby własnych zgrupowań sił zbrojnych, dowództw, obiektów czy instalacji. Prezencja wojskowa należy więc również do „widocznych" gwarancji bezpieczeństwa. Tymczasem w Polsce znajduje się tylko jedna komórka NATO[22], jedyna w całej Europie Środkowo-Wschodniej. Jest to Centrum Szkolenia Sił Połączonych (*Joint Force Training Centre* – JFTC) z siedzibą w Bydgoszczy. Komórka ta zatrudnia ok. 100 osób personelu podporządkowanego dowództwu NATO ds. transformacji i przeprowadza szkolenia na szczeblu taktycznym.

Obecnie brak przesłanek, które pozwoliłyby twierdzić, że w dającym się przewidzieć czasie można by oczekiwać dyslokacji znaczniejszych sił czy też obiektów NATO w Polsce. Jest to związane m.in. z realizowaną już reformą i redukcją dowództw sojuszniczych, podyktowaną zarówno względami merytorycznymi, jak i oszczędnościowymi. Procesy te polegają na: ograniczeniu liczby dowództw różnego szczebla z 11 do 6 (przy czym redukcja nie dotyczy wspomnianej Kwatery w Brunssum), zmniejszeniu liczby agend NATO-wskich z 14 do 3 oraz ograniczeniu personelu z 13 tys. osób do ok. 9 tys.

Do „widocznych" gwarancji bezpieczeństwa – a pojęcie to nie zostało konkretnie zdefiniowane i funkcjonuje raczej jako umowne – zalicza się również przeprowadzanie różnego rodzaju ćwiczeń, treningów i szkoleń, obecność (chociażby tymczasową) wojsk sojuszniczych oraz rozbudowę infrastruktury wojskowej służącej ewentualnemu przerzutowi i stacjonowaniu sił sprzymierzonych. Trzeba przy tym zaznaczyć, że ćwiczenia sojusznicze przybierają częstokroć formę aplikacyjną, czyli ćwiczeń sztabowych, względnie sztabowo-dowódczych. Niekoniecznie musi to umniejszać ich rangę, gdyż, zgodnie z doświadczeniami, ważne jest samo ich przygotowywanie. Niemniej jednak nie odbywają się one w atmosferze pełnej mobilizacji, jak zapewne miałoby to miejsce w wypadku ćwiczeń poligonowych. Dla Polski duże znaczenie miałoby przeprowadzenie realnych ćwiczeń Sił Odpowiedzi (SON/NRF) w połowie 2013 r., gdyż przygotowując ich scenariusz wspólnie z sojusznikami, można by wprowadzić do niego elementy, na których przećwiczeniu szczególne zależałoby stronie polskiej. „Widoczną" gwarancją bezpieczeństwa (w sensie obecności wojskowej Sojuszu na polskim terytorium) byłaby dyslokacja NATO-wskiego systemu antyrakietowego. Jednak analizowanie jego potencjalnego wpływu na bezpieczeństwo naszego kraju i byłoby obecnie przedwczesne[23].

[22] W Europie Środkowej nie mieści się żadne ważniejsze dowództwo ani agencja NATO. Dowództwo Korpusu Północ-Wschód z siedzibą w Szczecinie zalicza się do dowództw niższego szczebla. Skrzydło Ciężkiego Lotnictwa Transportowego w bazie Papa na Węgrzech może wykonywać również inne zadania niż tylko dla NATO. Wyspecjalizowane w poszczególnych dziedzinach tak zwane Centra Doskonałości (zwalczajace cyberterroryzm czy CBRN) trudno zaliczyć do ośrodków najwyższego znaczenia. Poza tym są one otwarte również dla państw spoza NATO. Z wojskowego punktu widzenia bodajże najważniejszym elementem jest misja „Baltic Air Policing", czyli regularne do 2014 r. (przez na ogół 4 samoloty), ale rotacyjne (co cztery miesiące inne państwo NATO) patrolowanie przestrzeni powietrznej państw bałtyckich.

[23] W niniejszym artykule pomija się różne możliwe formy amerykańskiej prezencji wojskowej w Polsce i w Europie Środkowej, gdyż siły tego państwa mogą znaleźć się w naszym kraju na zasadach porozumień dwustronnych.

Rosja jako partner

Skala pomocy Polsce, zwłaszcza gdyby rzeczywiście miała być tak znacząca, jak to przewiduje plan ewentualnościowy (przy zastrzeżeniu, że został on przedstawiony na podstawie doniesień w mediach), może świadczyć o pewnym przewartościowaniu polityki państw Sojuszu Północnoatlantyckiego względem Federacji Rosyjskiej w porównaniu z okresem sprzed lata 2008 r., czyli sprzed operacji rosyjskich sił zbrojnych w Gruzji. Przypomnijmy, że do tamtego momentu Sojusz uwzględniał politykę FR tak dalece, że Moskwa zaczynała ingerować w wewnętrzne sprawy paktu, wykorzystując mechanizmy przewidziane w dokumentach dotyczących współpracy. Pozwalało to Rosji m.in. na blokowanie rozbudowy infrastruktury wojskowej w tzw. nowych państwach NATO oraz na powstrzymywanie procesu poszerzania Sojuszu na wschód (co nie znaczy, że polityka rosyjska była jedynym czynnikiem torpedującym).

W nowych okolicznościach, czyli po rosyjskiej interwencji w Gruzji, w polityce bezpieczeństwa i obronności NATO uwidoczniły się dwa ważne elementy, które można traktować jako sygnały pod adresem Rosji, że dotychczasowa polityka tej organizacji wobec niej się zmienia. Najważniejszym z nich były deklaracje (w tym ze strony amerykańskiej) związane z negocjowaniem z Rosją układu START-III odnośnie do redukcji broni strategicznej oraz do planów utrzymania w mocy doktryny odstraszania jako jednej z naczelnych zasad NATO. Jednocześnie podtrzymywano chęć intensyfikacji dialogu o różnych aspektach bezpieczeństwa i konkretnej współpracy z FR. Takie podejście nasuwa skojarzenia z tzw. doktryną Harmela z lat 1966 - 67 (od nazwiska ówczesnego ministra spraw zagranicznych Belgii), od której w okresie zimnej wojny wzięła początek tzw. dwuczłonowa (dwutorowa) polityka NATO wobec Związku Radzieckiego i Układu Warszawskiego[24]. Naturalnie, trudno formułować i stosować taką samą politykę wobec dzisiejszej Rosji, niemniej oba elementy, tj. odstraszania i dialogu w polityce wobec Federacji Rosyjskiej, są wyraźne i, jak się wydaje, są najlepszą formułą z wszystkich możliwych w obecnej fazie stosunków międzynarodowych. Formuła ta umożliwia m.in. rozwiązywanie konkretnych kwestii, w tym afgańskiej (która w momencie przyjmowania nowej *Koncepcji strategicznej* była uznawana za priorytową dla NATO i, pomimo skoncentrowania się obecnie na operacji libijskiej, taką pozostaje), możliwości tranzytu ładunków niewojskowych[25] NATO z tego kraju, zwalczania przemytu narkotyków z tego kraju (m.in. szkolenie urzędników celnych), sprzedaży przez Rosję dla NATO ok. 20 śmigłowców Mi-17 oraz ewentualnie wozów opancerzonych.

Sojusz chce ustanowić długofalowe stosunki partnerskie z Afganistanem, opierając się na porozumieniu z władzami tego państwa oraz na stworzeniu przy pomocy sił międzynarodowych funduszu, który mógłby pomagać w odbudowie tego kraju po roku 2014. Problem afgański jest ważnym elementem dialogu politycznego NATO z Rosją, ale – w przeciwieństwie do kwestii kontroli zbrojeń nuklearnych oraz budowy systemu antyrakietowego – nie ma dla tych relacji charakteru strategicznego.

---

[24] Polityka ta doprowadziła m.in. do tak zwanej dwuczłonowej uchwały Sojuszu w 1979 r., na której podstawie rozmieszczono w pięciu państwach NATO amerykańską broń średniego zasięgu typu *Cruise Missile i Pershing II* (w odpowiedzi na rozmieszczenie radzieckich rakiet w Afganistanie), nie zrywając jednak docelowo dialogu politycznego.

[25] Ale nie oddziałów bojowych, co też stawało na porządku obrad.

Ani nowa *Koncepcja strategiczna,* ani inne dokumenty strategiczne NATO, w tym dotyczące relacji z Rosją, nie prezentują jednoznacznego stanowiska w sprawie kontroli zbrojeń nuklearnych. Sojusznicy podtrzymują wprawdzie swoje przekonanie, że posiadanie broni strategicznej pozostaje najwyższą gwarancją ich bezpieczeństwa, niemniej pozostawiają otwartą opcję rozbrojenia nuklearnego w przyszłości. Tak bowiem można odczytywać deklarację o dążeniu do dalszego rozbrojenia i świata bez broni atomowej. Równocześnie sojusznicy odwołują się do redukcji atomowej broni substrategicznej, przeprowadzonej w latach 90., co można zrozumieć jako oczekiwanie, iż jako pierwsze winny nastąpić redukcje po stronie rosyjskiej. Postuluje się podwyższenie stopnia transparencji oraz odsunięcie broni rosyjskiej jak najdalej od granic NATO (co już przedtem znalazło się w postulatywnej formie w wystąpieniach amerykańskich). Z polskiej perspektywy kwestia nuklearnej broni taktycznej w Europie jest zasadnicza. Z jednej strony chodzi o rosyjskie systemy, które mogą zagrozić naszemu bezpieczeństwu, z drugiej zaś o to, że taktyczna broń atomowa posiadana przez Zachód i stacjonowana w Europie stanowi podstawowy element doktryny odstraszania NATO[26], czyli że może być uznawana za jedną z rękojmi naszego bezpieczeństwa. Kwestia ta zapewne jeszcze długo pozostanie przedmiotem analiz, a ewentualnie potem negocjacji na temat ograniczenia lub nawet eliminacji wszystkich kategorii tej broni.

Sprawa systemu antyrakietowego, która pozostaje skomplikowana dla samego NATO, może zostać rozwiązana we współpracy z Rosją również w sposób optymalny dla Sojuszu. W myśl dokumentów NATO-wskich ze szczytu lizbońskiego, miałyby być ustanowione mechanizmy pozwalające na wymianę informacji o tworzeniu odrębnych – sojuszniczego i rosyjskiego – systemów obrony antyrakietowej oraz o ich ewentualnym przyszłym współdziałaniu, ale nie o ich integracji. System sojuszniczy ma się opierać na rozmieszczonych w Europie elementach amerykańskiej tarczy antyrakietowej oraz na systemach, dzięki którym chronione są zgrupowania europejskich wojsk NATO na naszym kontynencie. Obecnie Sojusz bardzo intensywnie pracuje nad rozbudową i rozwojem systemu antyrakietowego.

Pomimo wizyty prezydenta FR w Lizbonie podczas szczytu NATO, Sojusz nie zaproponował Rosji żadnej wyższej formuły współdziałania niż w dotychczasowej postaci (Stała Rada NATO–Rosja). Jednak trzeba mieć na uwadze, że pewne czynniki mogą to postanowienie zrelatywizować. Mianowicie: dotychczasowe formuły współpracy i tak pozwalały Rosji na dość daleko idące ingerowanie w sprawy NATO. W niektórych sytuacjach państwo to może więc ponownie powrócić do roli wyjątkowego, szczególnie wpływowego partnera Sojuszu. Stosunki poszczególnych państw członkowskich NATO, zwłaszcza Francji, Niemiec i Włoch, z Rosją już tak wiele razy układały się w sprawach o znaczeniu strategicznym (system bezpieczeństwa, polityka energetyczna, zakupy broni) w sposób odmienny od całokształtu relacji, że mo-

[26] Stany Zjednoczone posiadają w Europie, według własnych danych, 240 bomb atomowych przenoszonych samolotami. Bomby tzw. wolno spadające w liczbie 180 są rozmieszczone na samolotach głównie w bazie Ramstein (RFN), pozostałe w bazach USA we Włoszech i w Turcji. Broń atomową posiada również Wielka Brytania i Francja. Ocenia się, że Zachód posiada w Europie arsenał mniejszy o ok. 85% niż w okresie zimnej wojny. Trzy państwa dysponują różnymi typami broni taktycznej, począwszy od tych, które mają zasięg ok. 25 km. Tymczasem potencjał rosyjski, skoncentrowany przede wszystkim w okręgu kaliningradzkim, jest oceniany jako niewiadomy (w niektórych analizach jest mowa o 2 - 3 tys. systemów). Stąd najważniejszym postulatem jest przejrzystość co do posiadanych potencjałów.

żemy być świadkami różnych, trudnych i zaskakujących sytuacji. Moskwa – szczególnie gdyby udała jej się konsolidacja na obszarze postradzieckim przede wszystkim z Ukrainą, Białorusią i Kazachstanem – mogłaby zyskać na znaczeniu politycznym i gospodarczym do tego stopnia, że stałaby się jeszcze bardziej atrakcyjnym partnerem. Najprawdopodobniej odsunęłoby to w czasie przyjęcie do Sojuszu kolejnych państw, zwłaszcza Ukrainy i Gruzji[27], a tym bardziej jakże gorąco dyskutowanej opcji przyjęcia do NATO samej Rosji.

Streszczenie

Wraz z przyjęciem nowej *Koncepcji strategicznej* w listopadzie 2010 r., Sojuszowi Północnoatlantyckiemu wyznaczono ramy działania na najbliższą dekadę. Ale dynamiczny rozwój sytuacji międzynarodowej, oznaki renacjonalizacji polityki bezpieczeństwa państw członkowskich Sojuszu, problemy w stosunkach transatlantyckich, obniżanie nakładów na obronność przez państwa europejskie i inne zjawiska mogą zaszkodzić wspólnemu stanowisku NATO wobec nowych wyzwań i zagrożeń, zarówno tych klasycznych, jak i tych tzw. asymetrycznych, dla bezpieczeństwa państw członkowskich.

Uprawnione jest zatem pytanie, czy w konsekwencji nie pojawią się problemy z solidarnym udziałem całego NATO – o ile zaszłaby taka potrzeba – w ewentualnej operacji obronnej państwa czy też grupy państw członkowskich, w tym z Europy Środkowej i Wschodniej? Tak zwany plan ewentualnościowy, czyli plan pomocy wojskowej na wypadek zagrożenia naszych granic i terytorium, został niedawno uaktualniony. Potwierdzono, że Polskę objęto pełnymi gwarancjami bezpieczeństwa, takimi samymi, jak pozostałych 27 państw wspólnoty euroatlantyckiej. Polska chciałaby ponadto uzyskać rękojmie bezpieczeństwa – poniekąd pośrednie – w postaci sprawnych sił szybkiego reagowania NATO oraz wojskowej obecności sojuszników na swym obszarze.

Do czynników wpływających na bezpieczeństwo w Europie należy również, o czym była mowa w niniejszym artykule, budowa zaufania i skuteczna kontrola zbrojeń. Bez nich trudno mówić o poprawie stosunków np. z Federacją Rosyjską.

ABSTRACT

Since the adoption of the New Strategic Concept in November 2010, NATO has had the framework of its activities set for the next decade. However, the dynamic international developments, indications of security policy re-nationalisation by the NATO member states, problems of Trans-Atlantic relations, decrease in European countries budget spending on defence and other developments may impair the Alliance's cohesion due to constantly arriving new challenges and threats to member states, both classical and so called asymmetrical ones.

[27] Oba te państwa zostały wymienione w *Deklaracji Końcowej*, która potwierdziła zasadę „otwartych drzwi" do Sojuszu (zgodnie z art. 10 *Traktatu Waszyngtońskiego*). Niemniej jednak podczas lizbońskiego szczytu nie odbyły się nawet posiedzenia komitetów NATO–Ukraina i NATO–Gruzja, co najprawdopodobniej było wynikiem presji rosyjskiej. W podejściu do obu państw zaznaczyła się istotna różnica: w przypadku Ukrainy odnotowano pozablokowy status tego państwa, w przypadku Gruzji natomiast podkreślono integralność terytorialną.

Therefore, it seems justified to ask the question whether there would be no problems as regards the loyal participation of the entire NATO – if such a need arises - in possible defensive operation of a single member state or a group of member states, including those located in Central and East Europe. The contingency plan, that is the plan of military support in case of threat to our borders and territory, has been recently updated, confirming that our country enjoys full security guarantees of remaining 27 states of the Euro-Atlantic Community. Poland would additionally like to obtain the security warranties - in a way indirect in its nature – relating to the NATO's efficient rapid response forces and the military presence of allies on the territory of Poland.

Factors influencing security include also building trust and effective arms control. Without them, it will be difficult to speak about improvement in the quality of relations with Russian Federation.

Jacek Gawryszewski

Projekt restrukturyzacji systemu służb policyjnych Republiki Federalnej Niemiec

Projektowana reforma systemu instytucji odpowiedzialnych za bezpieczeństwo wewnętrzne i porządek publiczny w RFN to rezultat realizacji ustaleń umowy koalicyjnej, na której podstawie powstał obecny rząd kanclerz Angeli Merkel. Podpisana w dniu 26 października 2009 r. przez liderów CDU, CSU i FDP umowa zakładała między innymi przeprowadzenie reformy systemu służb policyjnych, zarówno na poziomie federalnym, jak i na szczeblu krajów związkowych. Z inicjatywą umieszczenia tej klauzuli w umowie koalicyjnej wyszedł Wolfgang Schäuble, szef resortu spraw wewnętrznych w poprzednim gabinecie Kanclerz Merkel, pełniący obecnie funkcję ministra finansów. Był on autorem wstępnej koncepcji zmian systemu, opracowanej jeszcze w 2005 r. Wśród priorytetów tej koncepcji znalazły się:

- racjonalne wykorzystanie środków budżetowych,
- optymalizacja procedur,
- uzyskanie efektu synergii przy zarządzaniu istniejącymi zasobami,
- separacja kompetencji,
- ograniczenie liczby ośrodków decyzyjnych,
- wdrożenie procedur optymalizujących koordynację działań,
- fuzja jednostek realizujących te same lub podobne zadania,
- intensyfikacja współpracy elementów systemu, funkcjonujących na szczeblu federalnym i na poziomie administracji krajów związkowych.

Obecny model sytemu służb policyjnych (uprawnień policyjnych nie posiadają zarówno Federalny Urząd Ochrony Konstytucji – BfV, jak i Krajowe Urzędy Ochrony Konstytucji – LfV) Republiki Federalnej Niemiec powstał w marcu 1951 r., kiedy na mocy ustaw powołane zostały Federalny Urząd Kryminalny (BKA) oraz Federalna Służba Ochrony Granic (BGS). Integralną częścią systemu tych służb, choć nie podlegającą władzom federalnym, są Krajowe Urzędy Kryminalne (LKA) oraz policje poszczególnych krajów związkowych. Uprawnienia policyjne posiadają także Kryminalny Urząd Celny (ZKA) i Śledczy Urząd Celny (ZFA), wchodzące w skład Administracji Celnej podlegającej Federalnemu Ministerstwu Finansów. ZKA i ZFA to struktury federalne, posiadające jednostki terenowe w krajach związkowych. Aktualny stan zatrudnienia w służbach policyjnych funkcjonujących na szczeblu federalnym oraz na poziomie krajów związkowych to około 250 tys. urzędników.

Federalny Urząd Kryminalny (Bundeskriminalamt – BKA)

BKA jest strukturą federalną podlegającą Ministerstwu Spraw Wewnętrznych. Aktualnie zatrudnia 5300 urzędników, z których 2780 wykonuje czynności policyjne. Podstawą jej działania jest ustawa o Federalnym Urzędzie Kryminalnym z dnia 7 lipca 1997 r. (zmiany precyzujące kompetencję BKA w zakresie zwalczania terroryzmu międzynarodowego wprowadzono na mocy poprawki z dnia 25.12.2008 r.). BKA nie posiada struktur terenowych. Krajowe Urzędy Kryminalne (LKA) de jure nie podlegają Federalnemu Urzędowi Kryminalnemu, stanowiąc część administracji krajów związkowych. Siedziby poszczególnych jednostek orga-

nizacyjnych Federalnego Urzędu Kryminalnego znajdują się w Wiesbaden, Meckenheim i w Berlinie. BKA zajmuje się analizą zjawisk kryminalnych występujących na obszarze Niemiec. Posiada wyłączne uprawnienia do prowadzenia pod nadzorem Federalnej Prokuratury Generalnej (lub na jej zlecenie) czynności procesowych w sprawach dotyczących szczególnie groźnych przestępstw kryminalnych o charakterze międzynarodowym, terroryzmu, przestępstw gospodarczych oraz stanowiących potencjalne zagrożenie dla wewnętrznego bezpieczeństwa państwa (szpiegostwo, proliferacja BMR, sabotaż, przestępstwa kryminalne motywowane politycznie). Ponadto prowadzi czynności procesowe w przypadkach szczególnie groźnych zjawisk przestępczych o zasięgu krajowym. Do wyłącznych kompetencji BKA należy ochrona osób pełniących kierownicze funkcje w konstytucyjnych organach władz federalnych, ochrona świadków oraz zwalczanie międzynarodowego terroryzmu. BKA wspomaga również Krajowe Urzędy Kryminalne w zapobieganiu i zwalczaniu szczególnie groźnych zjawisk przestępczych, w tym przede wszystkim grup przestępczych o wysokim stopniu organizacji. Funkcja koordynacyjna BKA polega na przygotowywaniu analiz różnych fenomenów przestępczości, między innymi pod kątem intensywności ich występowania, stopnia zagrożenia dla porządku publicznego, stosowanego modus operandi, rodzaju i wielkości szkód oraz perspektyw ewentualnej eskalacji zjawisk niepożądanych. Federalny Urząd Kryminalny opracowuje i publikuje doroczne raporty statystyczne dotyczące szczególnie groźnych zjawisk przestępczych występujących na terenie RFN (przestępstwa narkotykowe, finansowe, internetowe, handel ludźmi, nielegalny obrót bronią palną i amunicją, kradzieże dzieł sztuki, dóbr kultury itp.). Administruje również zasobami bazodanowymi obejmującymi kartoteki kryminalne, poszukiwanie osób i dane identyfikacyjne (DNA i odciski linii papilarnych) oraz dysponuje ośrodkami naukowo-badawczymi, w których wykonuje się ekspertyzy kryminalistyczne (w tym zakresie kompetencji BKA wspomaga Krajowe Urzędy Kryminalne). Innym aspektem koordynacyjnej funkcji omawianej służby jest współpraca z Krajowymi Urzędami Kryminalnymi w sprawach dotyczących przestępstw o charakterze międzynarodowym. Zadania te realizowane są między innymi przy pomocy rozbudowywanego od 1983 r. systemu misji łącznikowych (aktualnie 65 oficerów łącznikowych w 53 placówkach w 50 krajach świata) oraz akredytowanych przy BKA oficerów łącznikowych. BKA pełni poza tym rolę krajowego biura INTERPOLU i EUROPOLU oraz administruje systemami SIS i SIRENE. W ramach swoich kompetencji prowadzi także czynności procesowe w sprawach z zakresem produkcji narkotyków i obrotu nimi, nielegalnego obrotu bronią palną i amunicją oraz materiałami wybuchowymi, nielegalnego obrotu lekami oraz produkcji i obrotu fałszywymi środkami płatniczymi i „prania brudnych pieniędzy" (zawsze, gdy zachodzi podejrzenie, że przestępstwa te mają charakter międzynarodowy). Wyłączną kompetencją BKA jest prowadzenie czynności procesowych w sprawach z zakresu międzynarodowego terroryzmu, politycznie motywowanych prób zamachów na osoby pełniące kierownicze funkcje w konstytucyjnych organach administracji federalnej, szantażu urzędników konstytucyjnych organów władzy oraz szczególnie groźnych przypadków sabotażu komputerowego. Na zlecenie Federalnego Ministerstwa Spraw Wewnętrznych lub na wniosek administracji krajów związkowych BKA prowadzi również czynności procesowe dotyczące szczególnie groźnych przestępstw kryminalnych lub przestępstw kryminalnych o zasięgu federalnym. Uczestniczy też w różnego typu misjach międzynarodowych, organizowanych przede wszystkim w celu szkolenia funkcjonariuszy Policji.

W roku 2009 Federalny Urząd Kryminalny prowadził 240 postępowań w sprawach z zakresu przestępczości zorganizowanej oraz 412 postępowań w sprawach dotyczących bezpieczeństwa państwa.

Policja Federalna (Bundespolizei – BPOL)

Policja Federalna, utworzona w dniu 30 czerwca 2005 r. po likwidacji Federalnej Służby Ochrony Granic (BGS), działa na podstawie ustawy z dnia 19.10.1994 r. Jest to struktura posiadająca oddziały terenowe we wszystkich krajach związkowych RFN. Komenda Główna Policji Federalnej znajduje się w Poczdamie. W PBOL zatrudnionych jest obecnie 41 000 osób, z czego 31 500 wykonuje czynności policyjne. Do zadań Policji Federalnej należą: ochrona granic i przejść granicznych w międzynarodowych portach lotniczych, morskich i rzecznych, zwalczanie handlu ludźmi i zapobieganie temu procederowi, zwalczanie nielegalnej emigracji, przestępstw związanych z naruszaniem przepisów pobytowych, paszportowych, azylowych oraz ustaw – o obrocie i posiadaniu broni palnej oraz o obrocie substancjami medycznymi. Do jej wyłącznych kompetencji należy również ochrona infrastruktury kolejowej, w tym dworców (bezpieczeństwo pasażerów), linii kolejowych, obiektów zaplecza, linii energetycznych oraz urządzeń sterujących i nadzorujących ruch pociągów. Ponadto struktura ta odpowiada za bezpieczeństwo i ochronę cywilnego ruchu lotniczego (ochrona terminali, obiektów infrastruktury, kontrola personelu itp.). Wśród pozostałych kompetencji BPOL wymienić należy: ochronę siedzib konstytucyjnych organów państwa, współpracę z BKA w zakresie ochrony VIP-ów, współpracę z Ministerstwem Spraw Zagranicznych w zakresie ochrony placówek dyplomatycznych i konsularnych RFN, ochronę niemieckich placówek dyplomatycznych w krajach objętych konfliktami zbrojnymi (aktualnie Irak, Afganistan i Libia). Do zadań Policji Federalnej należy wspieranie służb policyjnych w krajach związkowych w przypadku konieczności użycia pododdziałów specjalnych (między innymi GSG 9) oraz w sytuacjach klęsk żywiołowych lub katastrof (zapewnia środki transportu lotniczego). PBOL odpowiada również za obsługę przelotów krajowych członków konstytucyjnych organów władzy oraz zaproszonych przez nich gości oficjalnych. Na zlecenie Federalnego Urzędu Ochrony Konstytucji PBOL realizuje kontrolę operacyjną środków łączności wykorzystywanych przez osoby podejrzewane o działalność szpiegowską.

Policja Federalna posiada uprawnienia do prowadzenia czynności procesowych w przypadku podejrzenia popełnienia wykroczeń lub przestępstw w obszarze:
- ochrony granic i przejeść granicznych,
- ochrony infrastruktury kolejowej,
- ochrony cywilnego transportu lotniczego,
- nielegalnej migracji i handlu ludźmi.

Kompetencje w zakresie prowadzenia czynności procesowych w sprawach dotyczących przestępczości zorganizowanej ma 9 spośród 68 terenowych jednostek BPOL. W skali federalnej czynności te realizuje około 3000 funkcjonariuszy. W roku 2009 policja ta prowadziła 204 431 postępowań, w tym w sprawach dotyczących wykroczeń i przestępstw popełnionych w obiektach infrastruktury kolejowej (48% wszystkich spraw), naruszeń przepisów o migracji (15,7%), drobnych kradzieży, fałszowania dokumentów podróży, fałszowania świadectw, zaświadczeń itp. (34,4%). W tym samym okresie prowadziła 30 śledztw dotyczących handlu ludźmi oraz 172 śledztwa w zakresie przestępczości zorganizowanej o szczególnie groźnym charakterze. Od kil-

ku lat struktura ta rozbudowuje system misji łącznikowych. Obecnie posiada 22 oficerów akredytowanych w 21 krajach.

Administracja Celna

Zgodnie z art. 108 Konstytucji RFN Administracja Celna odpowiada za prawidłowy pobór ceł, kontrolę obrotu wyrobami alkoholowymi, kontrolę poboru podatków konsumpcyjnych oraz monitoruje realizację różnego typu embarg i ograniczeń w międzynarodowym obrocie handlowym i prowadzi czynności kontrolne w zakresie nielegalnego zatrudnienia. W związku z wprowadzeniem z dniem 1 stycznia 2011 r. podatku od obrotu paliwem jądrowym oraz tzw. podatku lotniczego (opłaty związane z lotniczym transportem pasażerskim) zajmować się będzie również poborem tych obciążeń.

Aktualnie w Administracji Celnej zatrudnionych jest 39 700 osób. W ramach jej struktury organizacyjnej funkcjonują: Federalne Dyrekcje Finansowe (5), Celny Urząd Kryminalny – ZKA, Główne Urzędy Celne (43) oraz Śledcze Urzędy Celne – ZFA (8). Wszystkie podmioty instytucjonalne wchodzące w skład systemu mają uprawnia do prowadzenia czynności śledczych i kontrolnych, a także realizują działania o charakterze prewencyjnym. Czynności kontrolne i prewencyjne obejmują przede wszystkim sferę poboru podatków konsumpcyjnych, ograniczeń i embarg w międzynarodowym obrocie towarowym i technologicznym oraz gotówkowe i bezgotówkowe przepływy finansowe. W ramach tych czynności, realizowanych aktualnie przez 6400 pracowników, Administracja Celna posiada uprawnienia do prowadzenia postępowań przygotowawczych. Główne Urzędy Celne mają prawo do prowadzenia czynności procesowych wyłącznie w przypadku istnienia uzasadnionego podejrzenia popełnienia wykroczeń klasyfikowanych jako przestępstwa podatkowo-celne, o czym decyduje prokuratura. W takich przypadkach istnieje także możliwość przekazania prowadzenia czynności śledczych Celnym Urzędom Śledczym (ZFA) lub Krajowym Urzędom Kryminalnym (LKA). Ponadto Administracja Celna ma możliwość nakładania kar grzywny w przypadku stwierdzonych naruszeń przepisów podatkowych w obszarze międzynarodowego obrotu towarowego, gotówkowego i bezgotówkowego obrotu finansowego, przepisów regulujących rynkowy obrót wewnętrzny oraz realizacji międzynawowych ograniczeń i embarg w obrocie towarowym oraz technologicznym.

Decyzja o przeprowadzaniu czynności procesowych przez Główne Urzędy Celne bądź Celne Urzędy Kryminalne podejmowana jest na podstawie tzw. zasady szkodliwości i zasięgu czynu niedozwolonego oraz stopnia komplikacji procedur. I tak, w przypadku wykroczeń klasyfikowanych umownie jako „drobne" czynności procesowe prowadzą Główne Urzędy Celne; w przypadkach określonych jako „przestępczość ciężka" lub „zorganizowana" natomiast powierza się je Celnemu Urzędowi Kryminalnemu lub Celnym Urzędom Śledczym, które zatrudniają obecnie odpowiednio 800 i 2450 osób. Do tej grupy przestępstw zalicza się między innymi oszustwa podatkowe, tzw. paserstwo podatkowe, oszustwa finansowe związane z przydziałem różnego typu subwencji oraz przestępstwa z zakresu międzynarodowego procederu „prania brudnych pieniędzy". W praktyce Celny Urząd Kryminalny koncentruje swoją działalność na koordynacji działań Śledczych Urzędów Celnych, przygotowywaniu dokumentów analitycznych i statystycznych, opinii oraz różnego typu ekspertyz. Z zasady Celny Urząd Kryminalny prowadzi samodzielnie postępowania procesowe wyłącznie w przypadku ciężkich naruszeń przepisów o międzynarodowym obrocie towarowym lub naruszenia przyjętych przez społeczność międzynarodową ograniczeń w obrocie bronią,

amunicją i materiałami wybuchowymi. W szczególnych przypadkach postępowania te prowadzone są przez specjalne grupy zadaniowe (Finansowe Grupy Śledcze – GFG), powoływane wspólnie z Federalnym Urzędem Kryminalnym.

Wyłączną kompetencją Celnego Urzędu Kryminalnego jest techniczne zabezpieczenie wykorzystania środków techniki operacyjnej (podsłuch, podgląd, kontrola korespondencji) w sprawach dotyczących nielegalnego obrotu bronią i amunicją oraz proliferacji BMR. W roku 2009 Celny Urząd Kryminalny oraz Śledcze Urzędy Celne prowadziły 15 540 postępowań procesowych, z czego 75 procedur dotyczyło przestępczości zorganizowanej (w tym 31 – międzynarodowego obrotu narkotykami, a 39 – przestępstw podatkowo-celnych związanych z nielegalnym obrotem wyrobami tytoniowymi)). W ramach prowadzonych czynności procesowych ZFA mają uprawnienia do stosowania środków techniki operacyjnej, wykorzystywania osobowych źródeł informacji oraz funkcjonariuszy „pod przykryciem". W 27 przypadkach czynności operacyjno-śledcze w sprawach dotyczących międzynarodowego obrotu narkotykami i substancjami psychoaktywnymi ZFA prowadziły wspólnie z Krajowymi Urzędami Kryminalnymi w ramach tzw. Śledczych Grup Antynarkotykowych (GER), powoływanych na mocy przepisów szczebla krajowego.

W ramach kompetencji związanych z realizacją współpracy międzynarodowej Administracja Celna posiada 16 misji łącznikowych.

Komisja Werthebacha

Ocenę aktualnego funkcjonowania systemu służb policyjnych RFN oraz opracowanie założeń jego reformy powierzono niezależnej komisji eksperckiej, utworzonej w ramach Federalnego Ministerstwa Spraw Wewnętrznych. Komisję powołał w dniu 19.04.2010 r. były szef resortu Thomas de Maiziere (obecnie minister obrony). W jej składzie znaleźli się:

- Senator dr Eckert Werthebach, b. Szef Federalnego Urzędu Ochrony Konstytucji – przewodniczący,
- Dr Ulrich Kersten, b. Szef Federalnego Urzędu Kryminalnego – członek,
- Kay Nehm, b. Federalny Prokurator Generalny – członek,
- Wolfgang Riotte, b. Sekretarz Stanu w Federalnym Ministerstwie Spraw Wewnętrznych – członek,
- Karl-Heine Matthias, b. Szef Celnego Urzędu Kryminalnego – członek,
- Dr Rolf Ritsert, Dyrektor Wyższej Szkoły Policji – członek.

Rolę doradców komisji pełnili eksperci z Federalnego Ministerstwa Finansów, policyjnych central związkowych, ministerstw spraw wewnętrznych krajów związkowych, Krajowych Urzędów Kryminalnych, terenowych komend policji, Celnego Urzędu Śledczego oraz Federalnego Urzędu Bezpieczeństwa Teleinformatycznego (BSI). Członkowie komisji wizytowali Centrale Federalnego Urzędu Kryminalnego, Policji Federalnej, Celnego Urzędu Kryminalnego, Centrum Przeciwdziałania Terroryzmowi (GTAZ) oraz Centrum Analityczno-Strategiczne ds. Zwalczania Nielegalnej Migracji (GASIM). Ponadto zapoznali się z pracą terenowych jednostek Policji Federalnej, oddziałów Celnego Urzędu Kryminalnego i posterunków Policji Federalnej na przejściach granicznych w międzynarodowych portach lotniczych, morskich i rzecznych. Z prac komisji wyłączono obszar przeciwdziałania i zwalczania terroryzmu oraz pozostające w wyłącznych kompetencjach Federalnego Urzędu Kryminalnego sprawy związane z wewnętrznym bezpieczeństwem państwa (przestępstwa szpiegostwa, ochrona

informacji niejawnych, proliferacja BMR, ekstremizm polityczny). Komisja nie zajmowała się problematyką związaną z funkcjonowaniem służb specjalnych, co wynikało z faktu, iż służby te nie posiadają uprawnień policyjnych (konstytucyjna zasada separacji służb, tzw. *trennungsgebot*).

Komisja określana przez media jako „Komisja Werthebacha" działała do 2 grudnia 2010 r., a efektem jej pracy był 150-stronicowy dokument, przedstawiony oficjalnie przez szefa resortu spraw wewnętrznych Thomasa de Maiziere. Sprawozdanie Komisji zawiera szczegółowy opis istniejących rozwiązań, ich ocenę oraz zalecenia dotyczące proponowanych zmian. Jak podkreślali przedstawiciele Federalnego Ministerstwa Spraw Wewnętrznych, raport wyżej wymienionej Komisji nie jest projektem reformy systemu służb policyjnych, a jedynie prezentacją rezultatów swoistego audytu przepisów, struktur organizacyjnych, procesów zarządzania i zasad, na których podstawie określa się kompetencje poszczególnych podmiotów. W trakcie prezentacji sprawozdania podkreślono, że resort nie dysponuje jeszcze żadnym harmonogramem działań, których celem byłoby przygotowanie projektów zmian obowiązujących przepisów.

Komisja Werthebacha oceniła funkcjonowanie istotnych z punktu widzenia realizacji zadań integralnych elementów systemu, wśród których znalazły się:
- ośrodki decyzyjno-sztabowe,
- ośrodki analityczno-koordynacyjne,
- zbiory bazodanowe,
- ośrodki szkoleniowe,
- wykorzystanie sprzętu technicznego,
- wykorzystanie realizacyjnych pododdziałów specjalnych,
- wykorzystanie jednostek zwartych,
- funkcjonowanie misji łącznikowych,
- funkcjonowanie międzyinstytucjonalnych grup zadaniowych.

W toku prac Komisji analizowano efektywność i optymalność wykorzystania istniejących zasobów i środków przy realizacji zadań w następujących obszarach kompetencji:
- przestępczość narkotykowa,
- handel ludźmi i nielegalna migracja,
- przestępczość finansowa,
- ochrona obiektów infrastruktury kolejowej,
- ochrona wewnętrznych i zewnętrznych granic UE,
- proliferacja BMR,
- przestępczość bankowa,
- zwalczanie procederu „prania brudnych pieniędzy",
- ochrona osób pełniących kierownicze funkcje w konstytucyjnych organach władzy,
- ochrona niemieckich placówek dyplomatycznych.

Komisja zwracała szczególną uwagę na przypadki istnienia luk w systemie bezpieczeństwa, realizowanie tych samych zadań przez różne jednostki, dublowanie się struktur koordynacyjnych oraz niejasne zasady, na których podstawie odbywa się wymiana informacji między poszczególnymi strukturami. Analizy i oceny aktualnego stanu dokonano pod kątem ewentualnego przeprowadzenia fuzji Federalnego Urzędu Kryminalnego, Policji Federalnej i wybranych struktur Administracji Celnej (posiadających uprawnienia śledcze). Konsolidacja struktur i kompetencji umożliwiłaby, w opinii Komisji, koherentną realizację zadań bez konieczności tworzenia dodatkowych komórek koordynacyjnych. Podkreślano przy tym, iż założenie to, oparte na ist-

niejących przepisach, z uwgi na federalną organizację struktur państwa, jest wyjątkowo trudne do realizacji. Fundamentalna i wynikająca z zapisów konstytucyjnych reguła funkcjonowania systemu służb policyjnych, według której za porządek publiczny odpowiada administracja krajów związkowych, jest jedną z istotnych przeszkód w stworzeniu nowego, opierającego się na postulacie centralizacji, modelu.

Na podstawie obowiązujących regulacji prawnych oraz przeprowadzonego audytu rozwiązań strukturalnych i funkcjonalnych, realizowanego pod kątem podwyższenia efektywności działania służb policyjnych przy jednoczesnej optymalizacji wykorzystania środków, Komisja Werthebacha zarekomendowała restrukturyzację obecnego systemu poprzez połączenie Policji Federalnej i Federalnego Urzędu Kryminalnego. Ze względu na odmienność zadań zaleciła jednak pozostawienie tych służb poza nowym systemem Administracji Celnej, sugerując dokonanie w bliskiej perspektywie czasowej niezbędnych zmian w zakresie trybu współpracy służb celnych i policyjnych.

Nowa struktura o roboczej nazwie „Policja Federalna" miałby w opinii Komisji przejąć wszystkie dotychczasowe kompetencje BPOL i BKA. Jej trzon organizacyjny składałaby się z czterech podstawowych elementów:

- jednostki ds. zwalczania przestępczości kryminalnej, do której zadań należałaby koordynacja współpracy międzynarodowej oraz opracowywanie analiz, sytuacyjnych raportów statystycznych i ekspertyz,
- jednostki realizującej czynności w zakresie prewencji, ochrony granic oraz bezpieczeństwa transportu kolejowego i cywilnego ruchu lotniczego,
- jednostki wsparcia technicznego,
- jednostki administracyjno-logistycznej.

Do jednostki ds. zwalczania przestępczości kryminalnej wszedłby Departament ds. Przestępczości Zorganizowanej, Departament ds. Ochrony Państwa Federalnego Urzędu Kryminalnego, Dyrekcja ds. Zwalczania Przestępczości Zorganizowanej oraz Dyrekcja ds. Współpracy Międzynarodowej Policji Federalnej.

Do struktury jednostki realizującej czynności w zakresie prewencji weszłaby Dyrekcja ds. Ochrony Porządku, Dyrekcja ds. Analiz, Dyrekcja ds. Ochrony i Bezpieczeństwa Granic, Transportu Kolejowego oraz Ruchu Lotniczego, poddziały specjalne Policji Federalnej i pododdział specjalny Federalnego Urzędu Kryminalnego. W jej składzie znalazłyby się także tzw. oddziały zwarte, funkcjonujące obecnie w ramach Policji Federalnej.

W skład jednostki wsparcia technicznego weszłyby Departament Wsparcia, Instytut Techniki Kryminalistycznej, Instytut Kryminalistyki, Departament Techniki Informatycznej Federalnego Urzędu Kryminalnego oraz Dyrekcja Informatyki i Technik Komunikacyjnych Policji Federalnej. Ponadto w jej strukturze znalazłyby się: Grupa Transportu Lotniczego, GSG 9, Grupa Poszukiwań, Grupa Saperska, Oddział Rozpoznania Radiowego Policji Federalnej, Oddział Reagowania, Oddział Negocjacyjny oraz Odział Zabezpieczenia Saperskiego Federalnego Urzędu Kryminalnego.

W strukturze jednostki zabezpieczenia logistycznego znalazłyby się piony administracyjne Policji Federalnej oraz Federalnego Urzędu Kryminalnego oraz ośrodki szkoleniowe.

W ocenie Komisji Wethebacha, restrukturyzacja służb policyjnych w zaproponowanej przez nią formie, oprócz optymalizacji wykorzystania sił i środków, uprościłaby system zarządzania oraz pozwoliłaby na wyeliminowanie przypadków powielania się kompetencji wielu służb oraz luk w systemie bezpieczeństwa. Podkreśla się przy tym, iż opracowanie szczegółowego projektu i harmonogramu zmian wymagać będzie

kolejnych, kompleksowych konsultacji na poziomie administracji federalnej i krajów związkowych. Proponuje się jednocześnie, aby planowana reforma realizowana była etapami.

Do czasu opracowania projektu reformy Komisja Werthebacha zarekomendowała szybkie wdrożenie przygotowanych zaleceń, których celem jest przede wszystkim usprawnienie koordynacji i współpracy między poszczególnymi jednostkami. W opinii ekspertów, realizacja tych zaleceń będzie integralnym elementem kolejnych etapów reformy.

W rezultacie przeprowadzonego audytu oraz analizy sposobu realizacji zadań przez poszczególne służby Komisja Werthebacha sformułowała następujące zalecenia:

- wyłączne kompetencje w zakresie przygotowywania analiz, raportów statystycznych i sytuacyjnych dotyczących wszelkiego typu zjawisk przestępczych powierzyć Federalnemu Urzędowi Kryminalnemu (powyższe nie dotyczy przygotowywania ekspertyz z obszaru wyłącznej kompetencji poszczególnych służb, np. dotyczących procedur bezpieczeństwa transportu lotniczego lub bezpieczeństwa placówek dyplomatycznych),
- podjąć działania na rzecz ujednolicenia systemów bazodanowych (np. INPOL, INZOLL, AFIS) przy jednoczesnym wzmocnieniu funkcji Federalnego Urzędu Kryminalnego w zakresie centralnego administratora zasobów,
- na mocy porozumień międzyinstytucjonlanych poszerzyć zakres dostępu poszczególnych służb policyjnych do zasobów bazodanowych (dotyczy także baz administrowanych na szczeblu krajowym),
- wyłączne kompetencje w zakresie przeprowadzania procedur sprawdzeniowych w stosunku do osób i podmiotów gospodarczych zajmujących się obsługą cywilnego transportu lotniczego powierzyć Policji Federalnej,
- zintensyfikować współpracę i koordynację działań między Policją Federalną i Administracją Celną w zakresie spraw związanych z kontrolą transportowanych drogą lotniczą materiałów i substancji niebezpiecznych oraz broni palnej i amunicji (dotyczy także procedur w zakresie monitoringu realizacji ograniczeń i embarg w obszarze międzynarodowego obrotu towarowego i technologicznego),
- zintensyfikować współpracę między jednostkami Policji Federalnej i jednostkami policyjnymi krajów związkowych w zakresie ochrony infrastruktury transportu kolejowego (dotyczącą między innymi poszerzenia zakresu dostępu jednostek policji krajów związkowych do systemów monitorujących dworce kolejowe oraz koordynacji działań patroli interwencyjnych),
- pozostawić w kompetencjach Policji Federalnej zapobieganie i ściganie przestępstw o niskiej i średniej szkodliwości, popełnionych w obszarze jej działania (granice lądowe – 30 km, granica morska – 50 km),
- powołanie grupy eksperckiej złożonej z przedstawicieli resortów spraw wewnętrznych szczebla federalnego i krajowego w celu przygotowania regulacji dotyczących podziału zadań w zakresie zapobiegania i ścigania przestępstw o niskiej i średniej szkodliwości między Policję Federalną i jednostki policji krajów związkowych,
- powierzenie wyłącznych kompetencji w zakresie zwalczania międzynarodowego piractwa morskiego Federalnemu Urzędowi Kryminalnemu,
- przekazanie BKA kompetencji odnośnie do ochrony osób pełniących kierownicze funkcje w konstytucyjnych organach władz federalnych,
- przekazanie BPOL zadań dotyczących ochrony siedzib konstytucyjnych organów władz federalnych,
- przekazanie zadań z zakresu ochrony personelu placówek dyplomatycznych RFN Policji Federalnej przy jednoczesnym pozostawieniu w kompetencjach Federalnego

Urzędu Kryminalnego oceny zagrożeń w poszczególnych krajach,
- uszczegółowienie przepisów regulujących podział kompetencji między Policją Federalną i Administracją Celną w zakresie zapobiegania i ścigania przestępstw w pasach przygranicznych,
- utworzenie modułów szkoleniowych dla funkcjonariuszy Policji Federalnej i urzędników Administracji Celnej realizujących obowiązki służbowe w pasie przygranicznym,
- utworzenie wspólnych jednostek sztabowych Policji Federalnej i Administracji Celnej koordynujących działania w pasie przygranicznym,
- utworzenie wspólnych jednostek sztabowych Policji Federalnej i Administracji Celnej w obszarze granicznym państw Strefy Schengen,
- intensyfikacja współpracy między Policją Federalną i Administracją Celną w zakresie przygotowywania ekspertyz i ocen zagrożeń,
- utworzenie wspólnych grup operacyjnych Policji Federalnej i Administracji Celnej realizujących zadania w obszarze granicznym państw Strefy Schengen,
- intensyfikacja wymiany informacji między jednostkami Policji Federalnej i placówkami Administracji Celnej w zakresie realizacji czynności kontrolnych w międzynarodowych portach lotniczych,
- utworzenie wspólnych modułów Policji Federalnej i Administracji Celnej realizujących kursy szkoleniowe w zakresie procedur kontrolnych w międzynarodowych portach lotniczych,
- utworzenie wspólnych grup zadaniowych Federalnego Urzędu Kryminalnego i Celnego Urzędu Kryminalnego, realizujących czynności śledcze w zakresie zwalczania przestępczości narkotykowej,
- intensyfikacja współpracy między Federalnym Urzędem Kryminalnym i Celnym Urzędem Kryminalnym w zakresie zwalczania nielegalnego obrotu lekami,
- przyznanie Federalnemu Urzędowi Kryminalnemu dodatkowych uprawnień w zakresie możliwości przejmowania do prowadzenia śledztw od innych służb policyjnych szczebla federalnego lub krajowego,
- połączenie Grupy Wsparcia Interwencyjnego (ZUZ) Celnego Urzędu Kryminalnego z GSG 9 Policji Federalnej,
- konieczność częściowej integracji systemu misji łącznikowych Federalnego Urzędu Kryminalnego, Policji Federalnej i Administracji Celnej,
- poszerzenie kompetencji Celnego Urzędu Śledczego w zakresie prowadzenia czynności procesowych o sprawy związane z nielegalnym zatrudnieniem,
- wdrożenie mechanizmu koordynacji służb policyjnych w zakresie prowadzenia szkoleń zawodowych i kursów kształcenia zawodowego,
- wdrożenie procedur umożliwiających odbywanie praktyk i staży w poszczególnych służbach,
- przekazanie zadań realizowanych przez Centrum Koordynacji i Analiz ds. Nielegalnej Migracji (GASIM) do Federalnego Urzędu Kryminalnego,
- utworzenie przez Federalny Urząd Kryminalny oraz Federalny Urząd Bezpieczeństwa Teleinformatycznego (BSI), przy współpracy z resortami spraw wewnętrznych szczebla krajowego, wspólnego centrum ds. koordynacji działań w zakresie zwalczania cyberprzestępczości.

Reforma obecnego modelu proponowana przez Komisję Werthebacha zakładała utworzenie nowej formacji policyjnej poprzez organizacyjne i funkcjonalne połączenie Policji Federalnej, Federalnego Urzędu Kryminalnego oraz wybranych struktur Administracji Celnej. Projektowana jednostka (Policja Federalna) ma być jedyną strukturą fede-

ralną o uprawnieniach policyjnych, odpowiedzialną za zapobieganie i zwalczanie różnych fenomenów przestępczości kryminalnej oraz realizację zadań w obszarze prewencji.

Powstanie nowej struktury, określanej przez media oraz niektóre środowiska eksperckie mianem „superpolicji" lub „niemieckim FBI", w opinii przedstawicieli Federalnego Ministerstwa Spraw Wewnętrznych nie jest celem projektowanej reformy, ale środkiem umożliwiającym efektywną neutralizację aktualnie występujących zagrożeń w obszarze bezpieczeństwa państwa i porządku publicznego, a także kompleksowe rozpoznawanie i zwalczanie nowych zjawisk.

Dyskusja o restrukturyzacji systemu niemieckich służb policyjnych rozpoczęła się już na początku 2005 r. Jej rzecznikiem był przede wszystkim były minister spraw wewnętrznych Wolfgang Schäuble. W jego opinii model powstały 60 lat temu jest, pomimo systematycznie rosnących wydatków budżetowych, coraz mniej efektywny. Krytycznie o istniejącym systemie wypowiadała się także część ekspertów, w których opinii jego niewydolność to rezultat braku konsekwentnej i kompleksowej strategii resortu, uwzględniającej dynamiczne zmiany środowiska zewnętrznego. W tym kontekście zwracano przede wszystkim uwagę na fakt, iż w momencie przekształcenia Federalnej Służby Ochrony Granic w Policję Federalną, będącym pośrednim skutkiem zmian politycznych w Europie, zaniechano przeprowadzenia kompleksowej restrukturyzacji tego systemu. Praktycznie ograniczono się wówczas do zmiany nazwy nowej formacji i drobnych modyfikacji. Automatyczna zmiana BGS w Policję Federalną przy jednoczesnym braku choćby ograniczonej reformy pozostałych elementów systemu, tj. Federalnego Urzędu Kryminalnego i Administracji Celnej, systematycznie pogłębiała jego dysfunkcjonalność, która przejawiała się w autonomizacji niektórych elementów systemu, powstawaniu nieefektywnych z punktu wiedzenia realizacji zadań struktur poziomych, wydłużaniu procesów decyzyjnych i systematycznym wzroście liczby ośrodków koordynacji. Powstaniu Policji Federalnej, która przejęła praktycznie wszystkie dotychczasowe zadania Federalnej Służby Ochrony Granic, nie towarzyszyły także niezbędne w opinii środowisk eksperckich równoczesne zmiany organizacyjne na poziomie administracji krajów związkowych. Ten aspekt pozostaje do dziś najbardziej polemicznym zagadnieniem trwającej w tej sprawie debaty. Rządy krajów związkowych, powołując się na przepisy Konstytucji, nie zgadzają się na utratę części swoich prerogatyw w sferze bezpieczeństwa i porządku publicznego. Modyfikacja istniejących rozwiązań wymagałaby wprowadzenia zmian w ustawie zasadniczej, co, biorąc pod uwagę aktualny układ sił w Bundestagu oraz w parlamentach krajów związkowych, jest praktycznie niemożliwe. Zwolennicy przeprowadzenia reformy stoją jednak na stanowisku, że obowiązujące regulacje prawne oraz wynikające z nich rozwiązania systemowe nie uwzględniają, lub uwzględniają w niewielkim stopniu, pojawianie się w ostatniej dekadzie XX w. nowych zagrożeń, praktycznie we wszystkich sferach bezpieczeństwa wewnętrznego. Wśród nich wymienia się: przestępczość transgraniczną (nielegalny obrót narkotykami, handel bronią, nielegalną emigrację, handel ludźmi, fałszowanie i obrót środkami płatniczymi), przestępczość internetową, finansową, piractwo, terroryzm, kradzież praw autorskich, przestępstwa bankowe itp. Jak twierdzi wielu ekspertów, struktura organizacyjna i rozwiązania funkcjonalne niemieckich służb policyjnych w wielu aspektach są archaiczne i mogą coraz częściej powodować powstawanie niebezpiecznych luk w systemie, przy jednoczesnym nakładaniu się kompetencji w innych obszarach działania. Restrukturyzacja tego systemu poprzez fuzję poszczególnych jego elementów spotkała się z ostrą krytyką ze strony dwóch największych policyjnych central związkowych, tj. Związku Zawodowego Policji (GdP) i Związku

Zawodowego Policji Niemieckiej (DpolG). Związkowcy zarzucili Komisji Werthebacha posługiwanie się nierzetelnymi danymi, a sprawozdanie i wnioski określili jako nierzeczowe i nietrafne. Ich zdaniem, postulowane przez Komisję połączenie w jeden organizm służb policyjnych o tak odmiennych kompetencjach w żaden sposób nie ułatwi realizacji zadań. Poza tym skuteczne zarządzanie instytucjonalnym molochem nie jest możliwe. Największe obawy central związkowych budzi w takim przypadku nieuchronna redukcja etatów, likwidacja niektórych placówek, redukcja stanowisk administracyjnych, likwidacja niektórych stanowisk kierowniczych oraz niektórych elementów struktur sztabowych. W reakcji na sprawozdanie Komisji GdP i DpolG zapowiedziały akcje protestacyjne podobne do tych, jakie miały miejsce w 2004 r., kiedy Federalny Minister Spraw Wewnętrznych Otto Schilly zapowiedział przeniesienie Centrali Federalnego Urzędu Kryminalnego z Wiesbaden do Berlina. W wyniku zdecydowanej postawy związków zawodowych Ministerstwo zrezygnowało z tych planów, a ze stanowiska odwołano Ulricha Kerstena, Szefa BKA.

Przedstawiciele Policji Federalnej oraz Federalnego Urzędu Kryminalnego stoją na stanowisku, iż proponowany przez Komisję Werthebacha nowy model systemu służb policyjnych nie uwzględnia suwerenności obu podmiotów, która jest efaktem zarówno kilkudziesięcioletniej tradycji, jak i praktyki. BKA najbardziej obawia się utraty swoich kompetencji w obszarze koordynacji współpracy międzynarodowej, BPOL zaś, że jej rola zostanie sprowadzona wyłącznie do obszaru prewencji.

W ocenie wyżej wymienionej Komisji dotychczasowy model systemu organizacji służb policyjnych RFN nie odpowiada aktualnym standardom w zakresie ochrony porządku publicznego i bezpieczeństwa wewnętrznego. Częściowe zmiany tego modelu były raczej wynikiem postępującej autonomizacji poszczególnych jego elementów niż kompleksowej, uwzględniającej pojawienie się nowych zagrożeń, reformy. Niewątpliwym utrudnieniem dla skonstruowania nowego, koherentnego i efektywnego systemu jest federalny charakter państwa, który w obszarze szeroko rozumianego bezpieczeństwa wymusza utrzymanie równowagi między instytucjami obu poziomów administracji. Audyt przeprowadzony przez Komisję Werthebacha wykazał istnienie wielu struktur, których kompetencje powielają się (np. zwalczanie międzynarodowej przestępczości narkotykowej) lub są niedostatecznie precyzyjnie zdefiniowane (prowadzenie czynności procesowych w zakresie zwalczania przestępczości zorganizowanej). Jednocześnie wykazał istnienie wielu luk kompetencyjnych (np. zwalczanie cyberprzestępczości lub rozpoznawanie zagrożeń w obszarze bezpieczeństwa cywilnego transportu lotniczego).

Celem proponowanych przez Komisję zmian jest przede wszystkim konsolidacja zadań i jednostek, co w opinii ekspertów oznacza w pewnym sensie odwołanie się do rozwiązań funkcjonujących na poziomie krajów związkowych, w których służby policyjne realizujące zadania z zakresu prewencji i zwalczania przestępczości kryminalnej funkcjonują w ramach tej samej jednostki.

W dniu 15 marca 2011 r. nowy minister spraw wewnętrznych Niemiec Hans-Peter Friedrich oświadczył, iż resort rezygnuje z planów przeprowadzenia reformy służb w zakresie rekomendowanym przez Komisję Werthebacha. Podkreślił jednocześnie, iż decyzja ta nie oznacza odłożenia prac nad zmianą obecnego sytemu. Stwierdził, że szczególnie pilną sprawą w tym kontekście jest racjonalizacja współpracy służb w obszarze cyberprzestępczości, poprawa efektywności wykorzystania środków technicznych oraz integracja procesów szkolenia i doskonalenia zawodowego. Dodał, że ewentualne gruntowne reformy muszą uwzględnić zarówno stanowisko policyjnych central związkowych, jak i opinię przedstawicieli poszczególnych służb.

Bibliografia:

1. *Kooperative Sicherheit. Die Sonderpolizeien des Bundes im föderalen Staat Bericht und Empfeflunegn der Kommission „Evaluierung Sicherheitsbehörden“* – Berlin, 09.12.2010 r.
2. Ustawa Zasadnicza Republiki Federalnej Niemiec z 23.05.1949 r.
3. *Ustawa o Policji Federalnej* z 19.10.1994 r.
4. *Ustawa o Federalnym Urzędzie Kryminalnym* z 07.07.1997 r.
5. *Ustawa o Celnym Urzędzie Kryminalnym i Śledczych Urzędach Kryminalnych* z 16.08.2002 r.
6. *Ustawa o Federalnym Urzędzie Ochrony Konstytucji* z 20.12.1990 r.

Streszczenie

Założenia reformy systemu niemieckich służb policyjnych przygotowała komisja powołana 19.04.2010 r. przez ówczesnego ministra spraw wewnętrznych Thomasa de Maiziere, zwana od nazwiska jej przewodniczącego, byłego Szefa Federalnego Urzędu Ochrony Konstytucji – Eckerta Werthebacha – „Komisją Werthebacha”. Komisja ta, złożona z ekspertów ds. bezpieczeństwa, przeprowadziła kompleksowy audyt istniejącego systemu, którego zręby powstały jeszcze na początku lat 50. ubiegłago wieku. W sprawozdaniu opublikowanym w grudniu 2010 r. stwierdzono, że obecne rozwiązania organizacyjne i funkcjonalne powodują z jednej strony powielanie się kompetencji poszczególnych służb, z drugiej zaś tworzą groźne dla bezpieczeństwa wewnętrznego kraju luki, w szczególności w sferze zwalczania przestępczości zorganizowanej o charakterze transgraniczym. Komisja rekomendowała gruntowaną przebudowę systemu zarówno na poziomie federalnym, jak i krajów związkowych, w tym przede wszystkim fuzję Policji Federalnej z Federalnym Urzędem Kryminalnym.

Zalecenia wyżej wymienionej Komisji wywołały liczne, krytyczne opinie ze strony największych policyjnych central związkowych oraz szefów poszczególnych służb. Zwracano uwagę, że proponowany model systemu, który optymalizowałby wykorzystanie istniejących sił i środków, wiązałby się z koniecznością nowelizacji Konstytucji, zgodnie z którą kwestie bezpieczeństwa wewnętrznego leżą w kompetencjach krajów związkowych, a nie władz federalnych.

Według oficjalnego stanowiska nowego szefa resortu spraw wewnętrznych Hansa-Petera Friedricha, Ministerstwo rezygnuje z dotychczasowych planów reformy służb policyjnych do czasu przygotowania nowej koncepcji uwzględniającej zarówno postulat optymalizacji wykorzystania istniejacych zasobów, jak i potrzeby dotyczące skutecznej neutralizacji nowych zjawisk przestępczych.

ABSTRACT

The Reform of the German police was prepared by a commission appointed on the 19.04.2010, by the former Minister Thomas de Maiziere, called after the former Head of the Federal Constitution Protection Office - Eckert Werthebacha – “Werthebach Commission”. This commission, composed of experts in the field of security, carried out an audit of the existing system, which was established at the beginning of the 50’s. The commission’s report published in December 2010, concluded that the current arrangements lead to duplication of competences, and create, dangerous to the country’s internal security, legal gaps, especially in the sphere of countering cross-border

organized crime. The Commission recommended the reconstructing the system both on the federal and local levels, suggesting a merge of the Federal Police of the Federal Crime Office.

The Commission's recommendations led to criticism from police unions and heads of services. They have underlined the fact that the proposed model for reconstruction that would optimize the use of existing forces and resources would require amending the Constitution according to which the internal security matters are the responsibility of the lands.

According to Hans - Peter Friedrich, the new Minister for Internal Affairs, the Ministry will cancel the plans for the reform of the police until the preparation of a new concept, which would take into account both the demand to optimize use of existing resources and the need for effective neutralization of the new crimes.

II
PRAWO

Jacek Mąka

KONTROLA OPERACYJNA I PODSŁUCH – OCENA NA TLE PRAKTYCZNEGO STOSOWANIA

Stosowanie podsłuchu jako metody procesowego lub operacyjnego[1] pozyskiwania danych dotyczących przestępstw i ich sprawców jest wykorzystywane przez organy ścigania na całym świecie, w tym również w Polsce. W znaczeniu potocznym p o d s ł u c h kojarzy się z dokonywaną skrycie ingerencją w komunikację międzyludzką. Stąd też zapewne wywodzi się pejoratywna konotacja tej instytucji w powszechnym jej odbiorze, o czym warto wiedzieć, podejmując rozważania na ten temat.

Rozważania te, związane przede wszystkim z wpływem stosowania podsłuchu na nasz system prawny, skłaniają do podjęcia próby analizy określającej zakres wzajemnego oddziaływania i relacji historycznych tej instytucji z polskim ustawodawstwem. Dostępne dla autora materiały źródłowe pozwalają stwierdzić, iż pierwsze regulacje kodeksowe dotyczące podsłuchu zostały *per facta concludenta* ujęte w kodeksie postępowania karnego z dnia 19 marca 1928 r. (z mocą obowiązującą od 1 lipca 1929 r.; Dz.U. z 1929 r., Nr 33, poz. 313)[2]. W rozdziale trzecim dotyczącym rewizji i zatrzymań rzeczy, w przepisie art. 158 § 1 kpk zawarto między innymi zapisy o obowiązku urzędów pocztowych i telekomunikacyjnych do wydawania na żądanie sądu lub prokuratora korespondencji i przesyłek otrzymywanych przez oskarżonego lub adresowanych do niego[3].

Wzmiankę o funkcjonowaniu podsłuchu w systemie prawnym II Rzeczypospolitej odnaleźć można również w kodeksie karnym z 11 lipca 1932 r. (Dz.U. z 1932 r., Nr 60, poz. 571)[4]. Przepis art. 253 tego kodeksu w rozdziale XXXVII dotyczącym naruszenia tajemnicy poddawał penalizacji czyny przestępne polegające między innymi na przyłączaniu się do przewodu służącego do przekazywania wiadomości oraz

[1] Głównym przedmiotem rozważań ujętych w niniejszej publikacji będzie stosowanie podsłuchu operacyjnego, realizowane w systemie prawnym naszego kraju (trybie ustaw policyjnych) w postaci kontroli operacyjnej. Formuła procesowa podsłuchu (kontrola i utrwalanie rozmów), realizowana w trybie rozdziału 26 kpk (art. 237 i nast.), będzie miała w ramach poniższych rozważań znaczenie subsydiujące.

[2] Przed uchwaleniem i wejściem w życie kodeksu postępowania karnego z 1929 r. postępowanie w sprawach karnych na terenie II Rzeczypospolitej normowały ustawy procesowe zaborców, tj. rosyjska ustawa postępowania karnego z 1864 r., austriacka ustawa o postępowaniu karnym z 1873 r. oraz niemiecki kodeks postępowania karnego z 1877 r. Na przepisy wyżej wymienionych ustaw (odpowiednio art. 358 ustawy rosyjskiej, § 141 ustawy austriackiej oraz § 103 ustawy niemieckiej) powoływał się Komendant Główny Policji Państwowej w *Instrukcji Nr 125* z 1922 r. w sprawie rewizji przesyłek pocztowych.

[3] Przepis art. 158 § 1 kpk zawierał następujące brzmienie: *Urzędy pocztowe, telegraficzne i kolejowe są obowiązane na żądanie sądu wydawać sądowi lub prokuratorowi korespondencję i przesyłki, wysyłane przez oskarżonego i do niego adresowane.*

[4] Przed wejściem w życie kodeksu karnego z 1932 r. podstawowymi źródłami prawa karnego w II Rzeczypospolitej były: na obszarze byłego zaboru rosyjskiego – kodeks karny rosyjski z 1903 r, byłego zaboru austriackiego – ustawa karna austriacka z 1852 r, na ziemiach byłego zaboru pruskiego zaś – kodeks karny niemiecki z 1871 r.

na podstępnym uzyskiwaniu wiadomości telefonicznej lub telegraficznej bez wymaganego uprawnienia[5].

Instrukcja dla organów bezpieczeństwa z 1925 r., w części IV dotyczącej przestępstw politycznych, przewidywała natomiast między innymi możliwość zastosowania w ramach tzw. przeciwdziałania przedśledczego, a więc operacyjnego, *kontroli korespondencji listowej i telegraficznej* wobec osób podejrzewanych o udział w przestępstwach politycznych, do których zaliczano zdradę stanu, zdradę kraju, zdradę wojenną, przestępstwa zagrażające porządkowi wewnętrznemu kraju oraz przestępstwa zwiazane ze służbą w wojsku[6].

Okres wskazanych kilkunastu lat związanych z kreowaniem przez II Rzeczypospolitą własnego, niezależnego od systemu państw zaborczych ustawodawstwa prawnego, w tym karnego i policyjnego, stanowił jednocześnie okres inicjowania podstaw i zasad funkcjonowania w polskim systemie prawnym instytucji podsłuchu jako czynności procesowej związanej z posługiwaniem się przede wszystkim telegrafem jako technicznym środkiem komunikacji.

Kolejna cezura historyczna związana była z okresem powojennym, zdominowanym przez jedną formację polityczną. Obowiązujące w systemie państwa totalitarnego regulacje prawne musiały uznawać prymat fasadowej zgodności z nadrzędnymi zasadami ustrojowymi dotyczącymi praw jednostki, praworządności postępowania organów władzy państwowej itp[7]. W rezultacie przez prawie 40 lat przepisy prawa, zarówno przed nowelizacją ustawy karnej materialnej i procesowej w 1969 r., jak i po jej uchwaleniu, regulowały kwestię podsłuchów w sposób lakoniczny, wzorowany na założeniach przedwojennych ustaw karnych z 1929 i 1932 r. Charakterystyczne dla tamtego okresu było również to, iż regulacje pozakodeksowe nie zawierały żadnych odniesień do prawnych możliwości stosowania podsłuchu przez ówczesne służby policyjne, w szczególności przez Służbę Bezpieczeństwa i ogólnie Milicję Obywatelską. W dalszym ciągu wszelkie przepisy określające zasady funkcjonowania tych służb były utajnione, w formalny sposób określone w postaci wewnętrznych instrukcji i zarządzeń[8].

Następny etap istotny z historycznego punktu widzenia wiąże się z wprowadzeniem pod koniec 1982 r. zarówno do regulacji kodeksowych, jak i ustawodawstwa policyjnego, jakościowo nowych zmian dotyczących podsłuchu. Niewątpliwy wpływ na powyższą decyzję miały zapewne napięcia polityczne i społeczne związane z wprowadzeniem stanu wojennego w 1981 r. i drastyczny rygor prawny szeregu

[5] Przepis art. 253 § 1 kk stanowił expressis verbis, że *kto bez wymaganego uprawnienia otwiera zamknięte pismo, dla niego nie przeznaczone, albo przywłaszcza sobie lub niszczy cudzą korespondencję, zanim adresat się z nią zapoznał, albo przyłącza się do przewodu, służącego do podawania wiadomości, albo podstępnie uzyskuje nieprzeznaczoną dla niego wiadomość telefoniczną lub telegraficzną, podlega karze aresztu do 2 lat lub grzywny.*

[6] W. Stępek, Z. Hoffmann-Krystyańczyk, *Służba śledcza. Podręcznik dla organów bezpieczeństwa*, Poznań 1925, s. 176.

[7] Szersze odniesienie do powyższego zagadnienia, obrazujące również zakres zainteresowania doktryny problematyką podsłuchu przedstawił w ówczesnej literaturze T. Taras w publikacji pt. *O dopuszczalności i legalności podsłuchu telefonicznego*, „Annales Universitatis Mariae Curie-Skłodowska", Lublin 196, vol. VII, Sectio G, s. 48 - 50.

[8] J. Mąka, *Ustawa o czynnościach operacyjno-rozpoznawczych. Czy jest potrzebna w obecnym stanie prawnym w Polsce?*, „Prokuratura i Prawo" 2009, nr 4, s. 127.

ustaw i regulacji dotyczących ustawodawstwa tamtego okresu. Podjęte w latach 1982 - - 1984 zmiany nowelizujące ustawę *Kodeks postępowania karnego*[9] oraz uchwalenie *Ustawy z 1983 r. o urzędzie Ministra Spraw Wewnętrznych i zakresie działania podległych mu organów*[10], a także rozporządzenie wykonawcze ministra spraw wewnętrznych do wyżej wymienionej ustawy[11], posiadały czytelną konotację polityczną, obliczoną na złagodzenie wskazanego wyżej obrazu restrykcji ustawodawstwa stanu wojennego.

Jednocześnie po raz pierwszy został zarysowany na tle wymienionych regulacji prawnych system *ex ante* nadzoru prokuratorskiego nad stosowaniem podsłuchu w polskim systemie prawnym, zarówno w postaci procesowej, ujętej w przepisie ówczesnego art. 198 kpk, jak i operacyjnej, regulowanej przez przepis art. 14 wyżej wymienionej ustawy. Znaczenie tego okresu dla oceny historycznej ewolucji instytucji podsłuchu w polskim systemie prawnym jest istotne nie tylko z punktu widzenia jej jednoznacznego usankcjonowania w regulacjach tak kodeksowych, jak i policyjnych, lecz także określenia systemu nadzoru prokuratorskiego nad jej stosowaniem. Przyjęte rozwiązanie odgrywało istotną rolę i miało wpływ na kształt ustawodawstwa dotyczącego tego środka w okresie następnych kilkunastu lat oraz w trakcie zmian polityczno-transformacyjnych po upadku systemu komunistycznego.

Wraz z okresem zachodzących po 1990 r. przemian ustrojowych rozpoczął się kolejny rozdział funkcjonowania instytucji podsłuchu w polskim systemie prawnym. W uchwalonych w tym roku przepisach ustawowych regulujących funkcjonowanie nowo powoływanych służb policyjnych, tj. Policji[12] i Urzędu Ochrony Państwa[13], przyjęto zapisy dopuszczające możliwość stosowania środka, o którym mowa, przez wyżej wymienione służby. Co istotne, generalne zasady dotyczące statusu prawnego, trybu i kontroli stosowania podsłuchu zostały w dużej mierze oparte na założeniach wyżej cytowanej ustawy z 1983 r. Podsłuch policyjny w dalszym ciągu pozostawał instytucją prawa operacyjnego, możliwą do zarządzenia jedynie przed wszczęciem postępowania karnego w ramach czynności prewencyjnych lub wykrywczych. W podobny sposób, dość nieprecyzyjnie, określono zakres przedmiotowy przestępstw uprawniający do ubiegania się o zastosowanie podsłuchu (bezpieczeństwo, obronność, porządek konstytucyjny). Analogicznie do założeń ustawy z 1983 r. określono również system nadzoru nad jego stosowaniem, przyjmując system kontroli prokuratorskiej, sprawowanej przez Prokuratora Generalnego.

---

[9] Pewnego rodzaju przełomem w tym zakresie było ujęcie wprost w ustawie karnoprocesowej instytucji podsłuchu procesowego po nowelizacji ustalonej przez przepisy art. 13 ustawy z dnia 18 grudnia 1982 r. o szczególnej regulacji prawnej w okresie zawieszenia stanu wojennego (Dz.U. z 1982 r. Nr 41, poz. 273). Przepis art. 198 po raz pierwszy, nowatorski w ówczesnym systemie prawnym, regulował warunki zastosowania podsłuchu (po wszczęciu postępowania karnego), określił organy uprawnione do zarządzenia stosowania tego środka (sąd lub prokurator) oraz jego zakres rodzajowy (korespondencja, przesyłki, treści rozmów telefonicznych), sposób dokumentowania tych czynności (protokół), a także zasady postępowania z materiałami nie mającymi znaczenia dla toczącego się postępowania (obowiązek zniszczenia).

[10] Dz.U. z 1983 r., Nr 38, poz. 172.

[11] Dz.U., Nr 6, poz. 28.

[12] Dz.U. z 1990 r., Nr. 30, poz 179.

[13] Dz.U. z 1990 r., Nr. 30, poz. 180.

[14] Dz.U. z 2001 r., Nr. 45, poz. 498.

Ostatni ważny etap cezuralny znajduje uzasadnienie w podjętej w 2001 r. przez ustawodawcę decyzji zmieniającej dotychczasowy system nadzoru nad stosowaniem podsłuchu, poddając go *ex ante* kontroli sądowej. W rezultacie wprowadzenia w życie przepisów nowelizujących ustawę o Straży Granicznej[14], o Policji[15] oraz o Żandarmerii Wojskowej i wojskowych organach porządkowych[16] dotychczasowy nadzór prokuratorski zastąpiono kontrolą sądową, co nie oznacza bynajmniej, iż rola prokuratury w zakresie nadzoru została zdeprecjonowana (zagadnienie to będzie przedmiotem rozważań w dalszej części niniejszej publikacji). Agencja Bezpieczeństwa Wewnętrznego została objęta wymienionymi regulacjami w 2002 r., w wyniku uchwalenia ustawy o ABW oraz AW regulującej sukcesję prawną po rozwiązaniu Urzędu Ochrony Państwa[17].

Przez ponad 80 lat udokumentowanego źródłami prawa funkcjonowania podsłuchu w polskim systemie prawnym instytucja ta przechodziła kolejne etapy oddziaływania na ustawodawstwo, co zostanie zaprezentowane poniżej. W ramach podsumowania tego wątku warto zwrócić uwagę na dwie szczególnie ważne kwestie. Pierwsza z nich dotyczy konieczności zahamowania gwałtownie wzrastającej po 1990 r. przestępczości, w tym związanej z powstawaniem struktur mafijnych w naszym kraju. Na przestrzeni lat 90. następował proces ustawowej ewolucji znaczenia pojęcia p o d s ł u c h z rozumianego jako czynność operacyjna w rozumiane jako czynność *de iure* procesowa (w rozumieniu zasad transformacji procesowej).

W rezultacie, na gruncie obecnych regulacji policyjnych ustawodawca zdecydował się nadać materiałom pozwalającym na wszczęcie postępowania karnego lub mającym znaczenie dla wszczętego już postępowania (zgromadzonym podczas stosowania podsłuchu) status czynności stricte dowodowej, co wynika m.in. z brzmienia chociażby przepisu art. 27 ust. 15 ustawy o ABW oraz AW. Stosowanie tego zapisu w praktyce opiera się na przekazywaniu do prokuratury zawiadomienia o możliwości popełnienia przestępstwa, a materiały z podsłuchu stanowią załącznik do wymienionej dokumentacji, który traktowany jest jako środek dowodowy w postępowaniu karnym. Przedstawiciele doktryny w przeważającej części z aprobatą odnieśli się do wymienionego kierunku postępowania ustawodawcy[18].

---

[15] Dz.U. z 2001 r., Nr. 100, poz. 1084.

[16] Dz.U. z 2001 r., Nr. 123, poz. 1353.

[17] Dz.U. z 2002 r., Nr. 74, poz. 676.

[18] W literaturze przedmiotu poglądy dotyczące wskazanej filozofii postępowania ustawodawcy znalazły akceptację m.in. S. Hoca w jego publikacji pt. *Refleksje na marginesie art. 10 ustawy o Urzędzie Ochrony Państwa*, „Wojskowy Przegląd Prawniczy" 1992, nr 3, s. 34; S. Pikulskiego w publikacji pt. *Działania operacyjne Policji*, „Wojskowy Przegląd Prawniczy" 1996, nr 2, s. 61; R. Kmiecika, w: *Prawnodowodowych aspektach ochrony programów komputerowych w postępowaniu karnym (problematyce wszczęcia postępowania),* „Prokuratura i Prawo" 1997, nr 6, s. 16; K. Marszała, w: *Procesie karnym*, Katowice 1998, s. 181; A. Tarachy, w: *Wykorzystaniu wyników czynności operacyjno-rozpoznawczych w procesie karnym,* pozycji opublikowanej w: *Nowym kodeksie postępowania karnego. Zagadnieniach węzłowych*, Kraków 1998, Zakamycze**,** s. 184 - 188. Stanowisko sprzeciwiające się możliwości wykorzystania podsłuchu w toku postępowania karnego zostało wyrażone w literaturze m.in. przez P. Tomaszewskiego, w: *Uwagach do artykułu na temat „Refleksje na marginesie art. 10 ustawy o Urzędzie Ochrony Państwa"*, „Wojskowy Przegląd Prawniczy" 1992, nr 3, s. 40; S. Waltosia, w: *Procesie karnym. Zarysie systemu*, Warszawa 1998, Wydawnictwo Prawnicze PWN, s. 370; P. Hofmańskiego, E. Sadzika, K. Zgryzka, w: *Kodeksie postępowania karnego. Komentarzu* pod red. P. Hofmańskiego, t. I, Warszawa 1999, s. 863.

Druga z przywoływanych konstatacji dotyczy problemu skali używania przez państwo podsłuchu i obserwowanych w tym względzie tendencji. Na przestrzeni ostatnich 20 lat daje się zauważyć proces powoływania kolejnych służb policyjnych, które wyposaża się w szeroki wachlarz technik operacyjnych. Kilka lat temu prawo stosowania tego rodzaju uprawnień, w tym również podsłuchu, przyznano szeregowi nowo powołanych instytucji, takich jak Centralne Biuro Antykorupcyjne, Służba Wywiadu Wojskowego i Służba Kontrwywiadu Wojskowego.

Tak więc, ustawowe uprawnienia w zakresie stosowania podsłuchu w obecnie obowiązującym stanie prawnym przysługują dziewięciu służbom i instytucjom (Centralnemu Biuru Antykorupcyjnemu, Agencji Bezpieczeństwa Wewnętrznego, Służbie Kontrwywiadu Wojskowego, Żandarmerii Wojskowej, Policji, Straży Granicznej, organom kontroli skarbowej oraz Agencji Wywiadu i Służbie Wywiadu Wojskowego), na zasadach określonych odpowiednio w odnośnych przepisach ustaw o ABW oraz AW, a także o SKW i SWW[19].

Jeśli uwzględnimy również okrojone w tym względzie, pozbawione możliwości stosowania kontroli operacyjnej, kompetencje Biura Ochrony Rządu sprowadzające się do prawa wykonywania czynności operacyjnych związanych z rozpoznawaniem zagrożeń dotyczących chronionych obiektów[20] oraz regulacje z 2010 r. przyznające uprawnienia w zakresie tzw. rejestracji obrazu i dźwięku w miejscach publicznych organom Służby Celnej[21], to należy stwierdzić, że aktualnie prawo do realizacji czynności operacyjno-rozpoznawczych posiada jedenaście różnego rodzaju służb.

Nadmierne rozpraszanie ustawowych zadań, równoległość kompetencji operacyjnych wielu służb w obszarze tych samych często rodzajów zagrożeń, oprócz dysfunkcjonalności związanej z występowaniem tego rodzaju zjawiska niesie za sobą również problem skutecznej ich koordynacji. Odrębne znaczenie dla oceny przedmiotowego stanu rzeczy ma aspekt kosztów finansowych, jakie dla budżetu państwa generuje wykonywanie tego typu obowiązków przez kilka służb.

W wymiarze przedmiotowym podsłuch może być stosowany w szerokim zakresie spraw operacyjnych od stricte kryminalnych, pozostających w kompetencji Policji (obejmujących największą ilość realizowanych wniosków), poprzez przestępstwa graniczne, korupcyjne, skarbowe (właściwe dla Straży Granicznej, CBA i organów skarbowych), aż po przestępstwa związane z bezpieczeństwem państwa, szpiegostwem, terroryzmem, których zwalczanie leży w obszarze ustawowych zadań ABW i SKW. Punktem wyjścia do dyskusji podejmującej próbę uporządkowania obecnego stanu prawnego w dziedzinie podsłuchów winna być świadomość, że żadna z ustaw policyj-

[19] W przepisach art. 6 ust. 3 ustawy o ABW oraz AW, a także ustawy o SKW i SWW (Dz.U. z 2006 r., Nr 104, poz. 709) zawarto analogicznie brzmiące zapisy dające uprawnienia do działania służbom wywiadowczym (AW oraz SWW) na terytorium Rzeczypospolitej Polskiej, w związku z działalnością poza granicami kraju, a realizacja czynności, o których mowa w art. 27 ustawy o ABW oraz AW (dotyczącym kontroli operacyjnej) oraz w art. 31 ustawy o SKW i SWW (również dotyczącym kontroli operacyjnej) wyłącznie za pośrednictwem Agencji Bezpieczeństwa Wewnętrznego oraz Służby Kontrwywiadu Wojskowego.

[20] Przepis art. 17 ust. 2 w zw. z art. 19 ustawy o Biurze Ochrony Rządu (Dz.U. z 2004 r., Nr 163, poz. 1712).

[21] Przepis art. 75b ustawy o Służbie Celnej (Dz.U. z 2009 r., Nr 168, poz. 1323).

nych nie zawiera definicji tej instytucji[22]. We wszystkich ustawach funkcjonuje pojęcie tzw. kontroli operacyjnej, obejmującej:

- kontrolowanie treści korespondencji,
- kontrolowanie zawartości przesyłek,
- stosowanie środków technicznych umożliwiających uzyskiwanie w sposób niejawny informacji i dowodów oraz ich utrwalanie, a w szczególności treści rozmów telefonicznych i innych informacji przekazywanych za pomocą sieci telekomunikacyjnych[23].

Konfrontując obecne brzmienie tych przepisów z wykonywaniem podstawowych obowiązków służbowych, należy przede wszystkim stwierdzić daleko posunięty anachronizm ustawowego określenia pojęcia p o d s ł u c h. Dzisiejszy obraz komunikacji międzyludzkiej, obejmujący również relacje przestępne, odzwierciedla się w możliwości korzystania z nowoczesnych form przekazu technologicznego, z internetu, komunikacji drogą elektroniczną, za pomocą kodowanych połączeń głosowych itp[24].

Istotne znaczenie ma nieostrość aktualnych zapisów związanych z wykładnią ustawowego pojęcia: ś r o d k i t e c h n i c z n e u m o ż l i w i a j ą c e u z y s k i w a n i e w s p o s ó b n i e j a w n y i n f o r m a c j i i d o w o d ó w o r a z i c h u t r w a l a n i e, a w s z c z e g ó l n o ś c i t r e ś c i r o z m ó w t e l e f o n i c z n y c h i i n n y c h i n f o r m a c j i p r z e k a z y w a n y c h z a p o m o c ą s i e c i t e l e k o m u n i k a c y j n y c h.

W wymiarze praktycznym wymienione wątpliwości sprowadzają się często do formułowania trywialnych pytań. Czy można uznać, że intencje ustawodawcy wypełni sytuacja, w której służby policyjne będą chciały utrwalić przy pomocy środków technicznych przebieg rozmowy między przestępcami odbywającej się w pomieszczeniu? Czy będzie spełniać wymogi do zastosowania ś r o d k a t e c h n i c z n e g o utrwalającego w sposób niejawny informacje i dowody sytuacja, w której organy uprawnione do wykorzystywania podsłuchów będą zamierzały skopiować w postaci binarnej zawartość dysku komputera czy innego nośnika, na którym w ich ocenie znajdują się istotne dowody popełnienia przestępstwa? Czy wreszcie służby policyjne mogą (na co

[22] Odniesienie do tej problematyki zawierają również systemy prawne innych krajów, w tym m.in. Słowacji i Ukrainy. Obowiązująca na Słowacji ustawa Nr 166 z 2003 r. dotycząca stosowania podsłuchów podejmuje próbę zdefiniowania pojęcia p o d s ł u c h poprzez formę rodzajową, skoncentrowaną na środkach technicznych. Zgodnie z wyżej wymienioną ustawą pojęcie p o d s ł u c h zawiera w sobie m.in. pojęcie: ś r o d k i e l e k t r o t e c h n i c z n e, r a d i o t e c h n i c z n e, f o t o t e c h n i c z n e, o p t y c z n e, m e c h a n i c z n e i i n n e u r z ą d z e n i a l u b i c h c z ę ś c i s k ł a d o w e. Ukraińska ustawa o telekomunikacji z dnia 18.11.2003 r. zawiera natomiast ustawową definicję pojęcia p o d s ł u c h, rozumianego jako *przejęcie informacji z systemów łączności polegające na zastosowaniu urządzeń technicznych dających możliwość podsłuchiwania, utrwalania i odtwarzania informacji przekazywanych przez systemy łączności. Informacja ta może zawierać zarówno dane o wzajemnym połączeniu sieci telekomunikacyjnych, jak i o treści informacji przekazanej przez system łączności*.

[23] Analizując obecne brzmienie przepisów dotyczących kontroli operacyjnej, można, stosując pewne uproszczenie, przyjąć, iż instytucja ta posiada dwie postacie rodzajowe: kontrolę pocztową (korespondencji) oraz kontrolę techniczną (w potocznym rozumienia tego słowa obejmującą podsłuch). Operacyjny, czyli realizowany w trybie ustaw policyjnych, a nie kodeksu postępowania karnego, charakter tych czynności stanowi dopełnienie brzmienia nazewniczego tej instytucji, czyli kontroli operacyjnej.

[24] Swoistą egzemplifikacją nowoczesnych metod działań przestępnych z użyciem współczesnych narzędzi internetowych jest chociażby rozwijające się na szeroką skalę zjawisko bankowej przestępczości elektronicznej, czyli tzw. phishing, przynoszący olbrzymie straty w sektorze działalności finansowej w wielu państwach.

wprost wskazują regulacje wielu krajów, a nasz ustawodawca wydaje się unikać tego zagadnienia) w celu zainstalowania podsłuchu dostać się niejawnie do pomieszczeń czy środków transportu? Rozważania na ten temat zostaną przedstawione w dalszej części niniejszego artykułu.

Funkcjonowaniu jednolitej wykładni interpretacji obowiązujących przepisów nie sprzyja również fakt kompetencyjnego rozproszenia na poziomie organów kontrolnych w postaci prokuratury i sądu. Tylko stosunkowo niewielka liczba procedur związanych z wnioskowaniem o podsłuch pozostaje we właściwości Prokuratury Generalnej i Sądu Okręgowego w Warszawie. Zdecydowana większość z nich przeprowadzana jest (zwłaszcza w przypadku wniosków pochodzących od policji i straży granicznej) zgodnie z właściwością na poziomie prokuratur okręgowych i sądów okręgowych właściwych miejscowo. W przypadku procedur inicjowanych przez organy Żandarmerii Wojskowej i Służby Kontrwywiadu Wojskowego wnioski rozpatrywane są w ramach właściwości struktur wojskowego wymiaru sprawiedliwości.

Jednym z istotnych elementów, nie do końca precyzyjnie określonym w regulacjach dotyczących kontroli operacyjnej, jest kwestia zasad dostępu prokuratury i sądu do materiałów operacyjnych uzasadniających zastosowanie tego środka. Warto w tym miejscu zaznaczyć, iż wszystkie ustawy policyjne zawierają zapisy dotyczące ostateczności posługiwania się podsłuchem w trakcie działań operacyjnych.

Przywołując wskazaną zasadę *in fine* z przepisów ustawy o ABW oraz AW (art. 27 ust. 1), jej ultymatywny charakter można wywnioskować ze wskazanej przez ustawodawcę reguły postępowania umożliwiającej Agencji ubieganie się o zastosowanie kontroli operacyjnej jedynie wtedy, *gdy inne środki okazały się bezskuteczne albo zachodzi wysokie prawdopodobieństwo, że będą nieskuteczne lub nieprzydatne*. Należy przy tym podkreślić, że w rezultacie nowelizacji przepisów kodeksu postępowania karnego i niektórych ustaw policyjnych z czerwca 2011 r. dyrektywa ostateczności stosowania podsłuchu zostanie doprecyzowana poprzez jednoznaczne stwierdzenie, iż kontrola operacyjna może być stosowana wtedy, gdy inne środki operacyjne *okazały się bezskuteczne lub będą nieprzydatne*[25]. Zaostrzone zostaną więc, w porównaniu z obecnym stanem prawnym, kryteria oceny nieprzydatności stosowania innych metod operacyjnych. Uznając podsłuch za metodę aktywnie wkraczającą w sferę praw i wolności obywatelskich, ustawodawca zdecydował się limitować działalność służb policyjnych w tym zakresie. Sugeruje jednocześnie posługiwanie się w trakcie działań operacyjnych środkami uznanymi za mniej inwazyjne, niejako łagodniej ingerującymi w sferę prywatności.

Problem w tym, iż porównując poszczególne metody operacyjne pod kątem ich inwazyjności, trudno oprzeć się wrażeniu nie do końca przemyślanej filozofii rozumowania ustawodawcy. Obejmując jedynie stosowanie podsłuchu rygorystycznym systemem kon-

[25] W rezultacie wejścia w życie w dniu 10.06.2011 r. przepisów *Ustawy z dnia 4 lutego 2011 r. o zmianie ustawy Kodeks postępowania karnego oraz niektórych innych ustaw* (Dz.U. z 2011 r., Nr 53, poz. 273) zostaną doprecyzowane niektóre przepisy dotyczące między innymi ustaw policyjnych, odnoszące się do kontroli operacyjnej. Poza wskazaną zmianą w zakresie dyrektywy subsydiarności obejmą one również zasady szerszego niż dotychczas dostępu do materiałów operacyjnych dla prokuratury i sądu. Uściślone zostaną także reguły postępowania z materiałami uzyskanymi podczas stosowania podsłuchu oraz zasady stosowania tzw. zgody następczej.

troli sądowej i hierarchizując przez to swoją ocenę różnych środków pracy operacyjnej, ustawodawca wydaje się jednocześnie nie dostrzegać tego, że inne metody uznane przez niego za „mniej szkodliwe" w praktyce operacyjnej są zdecydowanie bardziej dolegliwe.

Bardziej niż podsłuch w chronioną zasadą ostateczności sferę praw człowieka ingerują na przykład działania z wykorzystaniem tajnego agenta, prowokacji, tzw. zakupu kontrolowanego i kontrolowanego wręczenia korzyści majątkowej[26]. Zasadnicza różnica autopsyjna pomiędzy wymienionymi metodami polega na tym, iż w przypadku podsłuchu służby policyjne biernie rejestrują zachowanie osób, wobec których wymieniony środek jest stosowany. Przy wykorzystywaniu prowokacji i tajnego agenta mamy zaś do czynienia z możliwością bezpośredniego oddziaływania przez te środki na rozpracowywaną osobę. Poprzez zastosowanie różnego rodzaju aktywnych technik stymulacyjnych, oddziałujących na zachowanie i podejmowane decyzje, służby mogą w o wiele prostszy sposób ingerować w sferę oświadczeń woli czy innych zachowań. Techniki operacyjne oparte na prowokacji czy innych możliwościach interaktywnego oddziaływania nie są jednakże objęte kontrolą sądową, pozostając w gestii nadzoru prokuratorskiego.

Określenie zakresu dostępu do materiałów operacyjnych służb policyjnych przed wydaniem stosownej zgody prokuratury i postanowienia sądu dotyczącego możliwości zastosowania podsłuchu w zasadniczy sposób wpływa na efektywność mechanizmów kontrolnych chroniących przed ryzykiem potencjalnych nadużyć i nieprawidłowości. W obecnym stanie prawnym kwestia ta nie jest dostatecznie uregulowana, zwłaszcza w przypadku dostępu prokuratora do materiałów uzasadniających wypisanie wniosku o przeprowadzenie kontroli operacyjnej.

W świetle art. 27 ust. 10 ustawy o ABW oraz AW (pozostałe ustawy policyjne zawierają analogiczne zapisy) sąd przed wydaniem postanowienia o zastosowaniu kontroli operacyjnej w tzw. trybie niecierpiącym zwłoki oraz przy przedłużeniu wcześniej zarządzonego podsłuchu zapoznaje się z materiałami uzasadniającymi wniosek, które zostały zgromadzone podczas stosowania kontroli operacyjnej zarządzonej w danej sprawie.

Na marginesie tak uregulowanej kwestii dostępu do akt operacyjnych należy podnieść jeden istotny problem. A mianowicie: z punktu widzenia praktyki, największy wpływ na skuteczność mechanizmów kontrolnych ma możliwość zapoznania się przez sąd z materiałami operacyjnymi uzasadniającymi wniosek na etapie zarządzenia podsłuchu, czyli zastosowania go po raz pierwszy, a nie na etapie przedłużającym stosowanie tego środka. Wtedy bowiem następuje miarodajna i realna konfrontacja wiarygodności informacji uzyskanych przez służby policyjne z kryteriami zarówno zasadności, jak i legalności zarządzenia podsłuchu. Ten etap jest najważniejszy, zwłaszcza dla oceny kryteriów zasadności wniosku, co ma również bezpośredni związek z omawianą wyżej regułą ostateczności stosowania tego środka. Pozwala też efektywnie ocenić, czy starania danej służby w sprawie zianstalowania podsłuchu są w pełni udokumentowane sprawdzonymi wcześniej wiarygodnymi informacjami o możliwości zaangażowania osoby, którą zamierza się podsłuchiwać, w działalność przestępną.

Podsumowując ten wątek rozważań, należy uznać, iż ustawodawca niedostatecznie skupił się na skuteczności mechanizmów kontrolujących stosowanie podsłuchu.

[26] J. Mąka, *Instytucja prowokacji w świetle praktyki służb policyjnych*, „Prokuratura i Prawo" 2010, nr 1/2, s. 173 - 174.

Kładąc nacisk na procedurę przedłużenia wniosku o zatosowanie tej instytucji, z pola widzenia stracił moment znacznie istotniejszy, związany z rozpoczęciem całej procedury, tj. etap zarządzenia kontroli operacyjnej. To w tym miejscu istnieje potencjalne ryzyko wystapienia nieprawidłowości czy patologii w skutecznym nadzorze nad zasadnością wnioskowania o podsłuch.

To, że obecnie ustawodawca expressis verbis nie wskazuje prokuratury jako organu uprawnionego do dostępu do wiedzy operacyjnej zgromadzonej w toku rozpracowania nie oznacza oczywiście, że prokurator jest pozbawiony powyższej prerogatywy. W każdym przypadku, na zasadzie uzgodnień poczynionych między służbami policyjnymi a prokuraturą, przed wydaniem decyzji o możliwości zastosowania podsłuchu prokurator zapoznaje się z wiedzą i dokumentacją operacyjną uzasadniającą wniosek o zasadności zastosowania tego środka.

Przywoływana powyżej nowelizacja przepisów dotyczących zarządzenia podsłuchu wydaje się jednak dostrzegać problem dostępu prokuratora i sądu do akt operacyjnych. Po pierwsze, do każdego wniosku o zastosowanie podsłuchu służby policyjne są zobowiązane dołączyć (jak należy rozumieć, w celu przedstawienia prokuratorowi i sądowi) materiały uzasadniające potrzebę jego zastosowania, a po drugie sądowi zostanie przyznana prerogatywa w zakresie możliwości zapoznania się z materiałami również w ramach procedury zarządzenia wniosku, a nie tylko jego przedłużenia lub rozpoznania w ramach tzw. trybu niecierpiącego zwłoki[27].

Z zagadnieniem stosowania podsłuchu ściśle łączy się problem postępowania z uzyskanymi tą drogą informacjami, w tym stanowiącymi tajemnicę zawodową, które podlegają szczególnej ochronie prawnej w związku z obowiązkiem zachowywania szczególnego rodzaju informacji w tajemnicy. Obecnie można wyodrębnić kilkadziesiąt regulacji ustanawiających zasady ochrony danych związanych z wykonywaniem określonych zawodów, co jednocześnie określa zakres podmiotowy tajemnicy. Zakres przedmiotowy tajemnicy zawodowej opiera się na istnieniu przesłanki formalnej łączącej wykonywany zawód z faktem posiadania informacji skutkujących powstaniem zależności dyskrecji, czyli tzw. anonimatu.

Obowiązujące regulacje policyjne nie zawierają żadnych odniesień do problematyki reguł i zasad postępowania w trakcie stosowania podsłuchu z informacjami pochodzącymi od osób objętych szczególną ochroną prawną związaną z wykonywanym zawodem, osób kontaktujących się z tymi osobami itp. W zaistniałej sytuacji istotnych wskazówek i przesłanek traktowania zakresu ochrony informacji związanych z funkcjonowaniem tajemnic zawodowych mogą dostarczyć przepisy *Kodeksu postępowania karnego*, zwłaszcza części odnoszącej się do instytucji zakazów dowodowych. Jak podkreśla się w literaturze, zakazy dowodowe stanowią specjalny rodzaj ochrony różnego rodzaju uprawnień, wartości, sfer i uczuć, które z racji swojej funkcji chroniącej wymienione dobra prawne wchodzą w kolizję z interesem wymiaru sprawiedliwości. Istota zakazów dowodowych polega więc na tym, że ustawodawca decyduje się w tej szczególnej sytuacji chronić określone dobra prawne niejako kosztem ograniczeń w możliwości ustalenia prawdy materialnej w procesie[28].

[27] Zob. przepis art. 27 ust. 1a oraz 10 *Ustawy z dnia 4 lutego 2011 r. o zmianie ustawy Kodeks postępowania karnego oraz niektórych innych ustaw.*

[28] Z. Kwiatkowski, *Zakazy dowodowe w procesie karnym*, Katowice 2001, Wydawnictwo Uniwersytetu Śląskiego, s. 11.

Podstawowego znaczenia dla przedmiotu niniejszych rozważań należy upatrywać w szczególności w analizie i wykładni przepisów art. 180 § 1 kpk określającego *in fine*, iż *osoby zobowiązane do zachowania tajemnicy służbowej lub tajemnicy związanej z wykonywaniem zawodu lub funkcji mogą odmówić zeznań co do okoliczności, na które rozciąga się ten obowiązek, chyba że sąd lub prokurator zwolni te osoby od obowiązku zachowania tajemnicy.*

Poza prawem odmowy zeznań drugą, i zarazem główną, instytucją służącą ochronie tajemnicy zawodowej jest zakaz statuowany przepisem art. 180 § 2 kpk, w którym ustawodawca otoczył szczególną ochroną przedstawicieli sześciu wymienionych w nim profesji, tj. notariuszy, adwokatów, radców prawnych, doradców podatkowych, lekarzy i dziennikarzy. Zgodnie z wymienionym przepisem osoby reprezentujące wskazane zawody mogą być przesłuchiwane co do faktów objętych tajemnicą zawodową tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a fakty te nie mogą być ustalone na podstawie innego dowodu.

W kontekście wyżej wymienionej problematyki warte odnotowania są również stanowiska Sądu Najwyższego i Trybunału Konstytucyjnego dotyczące w szczególności bezwzględnego zakazu zwalniania osób zobligowanych do zachowania tajemnic określonych w przepisie art. 180 § 3 kpk z zachowniem tych tajemnic. W uchwale z dnia 22 listopada 2002 r. (I KZP 26/02) SN stwierdził, iż zakaz zwalniania dziennikarza z obowiązku zachowania w tajemnicy danych umożliwiających identyfikację autora materiału procesowego, listu do redakcji lub innego materiału o powyższym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, dookreśla istotę treści tajemnicy dziennikarskiej. Wymieniony zakaz ma charakter bezwzględny i nie może być naruszany poprzez zastosowanie art. 2 § 1 pkt 1 kpk oraz art. 9 kpk[29]. W postanowieniu z dnia 15 grudnia 2004 r. natomiast (III KK 278/04) SN wyraził stanowisko, że istnieje co prawda bezwzględny zakaz zwalniania dziennikarza z obowiązku zachowania tajemnicy dziennikarskiej w zakresie danych, o których mowa w art. 180 § 3 kpk, ale nie oznacza to, że nie można go przesłuchać na te okoliczności, jeśli on sam chce takie zeznania złożyć[30].

Problematyka dopuszczalności uchylania tajemnicy adwokackiej na podstawie art. 180 § 2 kpk, w zakresie zgodności z konstytucją wymienionego przepisu, stała się również przedmiotem stanowiska wyrażonego przez Trybunał Konstytucyjny. W wyroku z dnia 22 listopada 2004 r. (SK 64/2003) TK stwierdził, iż dotarcie do tajemnicy w procesie karnym jest zgodne z ustawą zasadniczą. Wskazał również, że interes osób korzystających z pomocy prawnej, z uwzględnieniem informacji dotyczących sfery ich prywatności przekazanej do wiadomości prawnikowi, może znaleźć się w konflikcie z innymi dobrami objętymi ochroną, w szczególności *dotyczącymi interesu całego społeczeństwa*. W ocenie TK możliwość uchylenia tajemnicy zawodowej służy realizacji wymienionego dobra, tj. skutecznemu funkcjonowaniu wymiaru sprawiedliwości.

Poza naszym krajem, o czym była mowa powyżej, problem reguł traktowania tajemnic zawodowych podczas stosowania podsłuchu jest dostrzegany i regulowany przez

[29] Glosę aprobującą stanowisko SN w wymienionym zakresie wyraziła w literaturze A. Gerecka-Żołyńska, „Orzecznictwo Sądów Polskich" 2004, nr 1, s. 5.

[30] W literaturze glosę aprobującą wymieniony w postanowieniu pogląd Sądu Najwyższego wyraziła A. Gerecka-Żołyńska, „Orzecznictwo Sądów Polskich" 2006, nr 11, s. 128; glosę krytyczną przedstawiła natomiast D. Szumiało-Kulczycka, „Prokuratura i Prawo" 2005, nr 12, s. 123.

systemy prawne innych państw. We Francji przykładowo podsłuch w stosunku do adwokatów można zastosować dopiero po poinformowaniu o tym zamiarze prezesa Rady Adwokackiej[31]. Podobne reguły dotyczące możliwości stosowania podsłuchu w stosunku do adwokatów, lekarzy oraz dziennikarzy zawarto w belgijskiej ustawie o metodach pozyskiwania danych przez służby operacyjne i bezpieczeństwa. Przepis art. 18 cytowanej ustawy zawiera dyspozycję poinformowania o fakcie zastosowania podsłuchu wobec przedstawicieli wymienionych profesji przewodniczących właściwych korporacji zawodowych (Przewodniczącego Kolegium Adwokatów i Stowarzyszeń Prawniczych, Przewodniczącego Krajowej Rady Lekarskiej i Przewodniczącego Stowarzyszenia Zawodowego Dziennikarzy[32]). Osoby te zobligowane są do zachowania uzyskanych informacji w tajemnicy, pod rygorem odpowiedzialności karnej.

Najbardziej rozbudowane przepisy dotyczące procedur postępowania w przypadku zarejestrowania rozmów mających charakter przywileju prawnego zawierają regulacje brytyjskie. W formie wyodrębnionego zbioru przepisów, ujętego w § 3 *Kodeksu postępowania w sprawach o przechwytywanie informacji*, zawarto szczegółowe odniesienie się do tej problematyki, tj. zasady przechwytywania komunikacji[33]. W zapisie tego paragrafu dotyczącym ogólnych zasad postępowania z informacjami poufnymi oraz szczegółowych interpretacji poszczególnych pojęć, ustawodawca brytyjski nakazuje zachować szczególną rozwagę i wrażliwość organów ścigania w przypadku, gdy *obiekt przechwytywania zachowuje wysoki stopień prywatności lub gdzie pojawiają się informacje poufne*. Definiując wspomnianą kategorię informacji, przywoływany kodeks wskazuje, że informacje poufne wchodzą w zakres zagadnień objętych:

- tajemnicą prawną (*legal privilege*) obowiązującą w relacjach klient–adwokat,
- tajemnicą powodowaną względami o charakterze osobistym (*confidential personal information*), związanym z poufnością danych medycznych dotyczących zdrowia fizycznego, psychicznego, przekonań religijnych i wiary,
- tajemnicą informacji o charakterze dziennikarskim (*confidential journalistic material*), obejmującą zarówno materiał gromadzony z zamiarem zachowania go w tajemnicy, jak również komunikację posiadającą status informacji dziennikarskich i w takim celu posiadaną.

W przepisie § 3 pkt 6 zawarto wytyczną dla służb stosujących podsłuch, by każdy wniosek, z którym może łączyć się przechwycenie komunikacji prawnie uprzywilejowanej, oprócz powodów, dla których wykorzystanie tego środka uznaje się za konieczne, zawierał również ocenę prawdopodobieństwa przechwycenia takich informacji. Dodatkowo wniosek powinien zawierać oświadczenie, że celem lub jednym z celów jest przechwycenie komunikacji uprzywilejowanej. Wskazana wiedza jest niezbędna sekretarzowi stanu do oceny zasadności wystąpienia z wnioskowaniem o podsłuch. Może on bowiem w tego rodzaju sytuacjach ustanowić dodatkowe warunki i obostrzenia dotyczące jego stosowania, takie chociażby, jak konieczność sporządzania regularnych raportów z efektów stosowania nakazu, co z kolei może rzutować na decyzję o kontynuacji wykorzystywania tego środka.

---

[31] Ustawa z dnia 10 lipca 1991 r. o tajemnicy komunikowania się w systemach telekomunikacyjnych, Nr 91 - 646, przepis art. 100 ust. 7.

[32] *Ustawa z dnia 4 lutego 2010 r. o metodach uzyskiwania danych przez służby operacyjne i bezpieczeństwa* (data wejścia w życie – 01.09.2010 r.), Nr 2 010 009 144.

[33] *Interception of Communications, Code of Practise*, London 2000.

Niezależnie od powyższego, przypadki, w których komunikacja uprzywilejowana została przechwycona i zatrzymana, powinny być zgłoszone do urzędu Komisarza ds. Przechwytywania Komunikacji.

Zgodnie § 3 pkt 4 *Code of Practice* przywileju prawnego nie stosuje się wobec komunikacji dotyczącej działalności kryminalnej. Komunikacja objęta przywilejem prawnym traci swoją ochronę, gdy zaistnieją przesłanki świadczące przykładowo o tym, że zawodowy doradca prawny zamierza zachować lub wykorzystać informacje dla celów kryminalnych, bez względu na to, czy robi to świadomie, czy nieświadomie.

Jednoznaczną konkluzją oceniającą istniejący stan rzeczy w zakresie problematyki korelacji procedur podsłuchowych z zagadnieniem szczególnej ochrony niektórych rodzajów tajemnic zawodowych, w tym zwłaszcza tajemnicy adwokackiej, lekarskiej i dziennikarskiej w ustawodawstwie polskim jawi się konieczność podjęcia tej niewątpliwie trudnej problematyki, a nie jej dalsze unikanie. W naszym kraju ustawodawca koncentruje swoją uwagę głównie na problemie pozyskiwania danych z podsłuchu, a powinien na określeniu precyzyjnego trybu i zasad ich dalszej waloryzacji procesowej.

Gdy porusza się problem istotnych zagadnień pomijanych przez regulacje polskiego systemu prawnego w ramach przywoływanych już propozycji nowelizujących *Kodeks postępowania karnego* i poszczególne ustawy policyjne, dziwić może brak zainteresowania problemem rejestracji przebiegu rozmów odbywających się z wyłączeniem systemów i sieci telekomunikacyjnych, w szczególności w postaci podsłuchu pomieszczeń. Tym bardziej, że problematyka ta jest jednym z newralgicznych obszarów współpracy służb policyjnych i organów ochronnych, w tym zwłaszcza prokuratury, a nierzadko także różnicy zdań między nimi.

Przywołując przedmiot rozważań związanych z koniecznością zmiany znaczenia i interpretacji pojęcia k o n t r o l a o p e r a c y j n a w części dotyczącej tzw. środków technicznych, warto zauważyć kolejną już dysfunkcjonalną analogię pomiędzy polskim systemem prawnym a systemami innych krajów.

W przepisach cytowanego już brytyjskiego *Kodeksu postępowania w sprawach o przechwytywanie informacji*, w § 4 pkt. 2, wymienia się dane dotyczące osoby, wobec której nakaz ma być zastosowany, lub pomieszczenia, w którym podsłuch ma być założony. W pkt. 3 tego przepisu wskazuje się na wymóg określenia *opisu komunikacji, która ma zostać przechwycona*.

W ustawie węgierskiej o służbach bezpieczeństwa narodowego (z 1995 r.) zagadnienie zakresu definicji p o d s ł u c h u jest jeszcze bardziej jednoznaczne. Zgodnie z przepisem art. 57 pkt pkt a i b uprawnione służby operacyjne, po uzyskaniu zgody odpowiednio sędziego lub ministra sprawiedliwości, mogą:

- potajemnie przeszukać mieszkanie i wyniki zarejestrować, korzystając ze środków technicznych,
- monitorować i rejestrować wydarzenia zachodzące w mieszkaniach z wykorzystaniem środków technicznych.

W ostatniej części powyższego przepisu, w art. 56 pkt d, ujęto uprawnienie do stosowania podsłuchu w rozumieniu analogicznym do definicji kontroli operacyjnej z polskich ustaw policyjnych (w części dotyczącej wspomnianych ś r o d k ó w t e c h n i c z n y c h), czyli do *przechwytywania komunikacji transmitowanej publicznymi liniami telefonicznymi lub innych usługodawców i rejestrowania jej z wykorzystaniem środków technicznych*.

W litewskiej ustawie o czynnościach operacyjnych z 2002 r. kwestię związków pomiędzy środkami technicznymi związanymi z przechwytywaniem komunikacji a tzw. podsłuchem pokojowym ujęto w sposób najbardziej rozbudowany, określając przy tym ramy prawne i tryb stosowania tej instytucji w praktyce. Zgodnie z art. 7 pkt 3 wyżej wymienionej ustawy, określającym uprawnienia i obowiązki służb operacyjnych, służby policyjne po uzyskaniu ustalonej w przepisach m.in. art. 10 (kontrola operacyjna) i art. 11 (niejawna penetracja pomieszczeń i środków transportu) zgody ze strony prokuratora i sądu mają prawo:

- potajemnie uzyskać dostęp do pomieszczeń mieszkalnych i niemieszkalnych, środków transportu oraz dokonać ich oglądu; tymczasowo zająć dokumenty i dokonać ich oglądu, pobrać do przeprowadzenia badań próbki materiałów, surowców oraz innych obiektów bez ogłaszania o ich zajęciu.

Przepis art. 10 pkt 4 ppkt 2 dotyczący danych, jakie winien zawierać wniosek o zastosowanie niejawnej kontroli przesyłek pocztowych i używania środków technicznych w trybie specjalnym, czyli odpowiednik kontroli operacyjnej z polskich ustaw policyjnych, wskazuje m.in. na wymóg wskazania danych *o osobie, wobec której przewiduje się stosowanie kontroli lub określenie obiektu*.

Możliwość niejawnego dostępu do pomieszczeń i środków transportu, jako odrębna metoda działania litewskich służb policyjnych, została ujęta w przepisie art. 11 przywoływanej ustawy. Zgodnie z brzmieniem pkt. 1 wyżej wymienionej regulacji stosowanie tej metody jest poddane nadzorowi sądowo-prokuratorskiemu. W tzw. przypadkach niecierpiących zwłoki natomiast (art. 11 pkt 2) zgodę na jej zastosowanie może wydać prokurator, który w ciągu 24 godzin musi wystąpić o jej autoryzację i zatwierdzenie przez sąd. We wniosku o zastosowanie niejawnego dostępu do pomieszczeń należy, zgodnie z art. 11 pkt pkt 1 - 5, określić dane funkcjonariusza przedkładającego wniosek, podać informacje dotyczące pomieszczeń i środków transportu, które planuje się poddać oglądowi, wymienić dokumenty, materiały i surowce, które chce się przejąć, oraz argumenty uzasadniające wniosek, czas trwania czynności (okres do 3 miesięcy z możliwością dalszego przedłużenia) i ich zakładany efekt.

Przywołane wyżej regulacje w wymiarze praktycznego stosowania sprowadzają się przede wszystkim do zasad wyznaczających służbom operacyjnym sposób postępowania przy zakładaniu podsłuchu w pomieszczeniach. Wyznaczają one w jasny, nie budzący wątpliwości interpretacyjnych, sposób ramy postępowania służb oraz granice ingerencji w chronione gwarancjami konstytucyjnymi obszary swobód obywatelskich. Tak skonstruowane regulacje wypełniają istotną funkcję kontrolną, chroniącą przed potencjalnymi nadużyciami i nieprawidłowościami ze strony organów stosujących te reguły w praktyce.

Jednoznacznie ujmowanym we wszystkich polskich ustawach policyjnych celem stosowania podsłuchu jest cel procesowy. Wymóg ten obliguje szefów służb uprawnionych do jego stosowania do przekazywania prokuraturze tych materiałów zgromadzonych w wyniku wykorzystania tego środka, które zawierają dowody pozwalające na wszczęcie postępowania karnego lub które mają znaczenie dla toczącego się już postępowania[34].

[34] W ustawie o kontroli skarbowej (art. 36d pkt 1) materiałom uzyskanym w czasie stosowania podsłuchu przez organy kontroli skarbowej nadaje się (niezależnie od waloru procesowego, ujętego w pkt. 2 tego przepisu) znaczenie istotne z punktu widzenia postępowania kontrolnego lub postępowania w sprawach o przestępstwa skarbowe czy wykroczenia skarbowe. W takiej sytuacji materiały przekazywane są właściwemu miejscowo organowi kontroli skarbowej.

Co do zasady, wszystkie inne materiały i dane uzyskane w wyniku stosowania kontroli operacyjnej winny podlegać komisyjnemu zniszczeniu.

Istotne jest jednakże to, iż obowiązujące przepisy, zarówno na poziomie ustawy o ABW oraz AW, jak i przepisów wykonawczych[35] do niej, w minimalnym nawet zakresie nie odnoszą się do wskazanej problematyki. Przede wszystkim nie została określona procedura kwalifikowania statusu materiałów pochodzacych z podsłuchu. Nie ustalono również trybu nadzoru i kontroli nad przebiegiem realizacji wymienionych procedur[36].

Wiele wątpliwości pojawia się również przy praktycznym stosowaniu przepisów dotyczących obowiązku niszczenia materiałów uzyskanych w wyniku zastosowania wyżej wymienionego środka, które nie spełniają wymogów procesowych i nie mają znaczenia dla bezpieczeństwa państwa. Przede wszystkim ustawodawca nie zdecydował się przyjąć jednolitego kryterium dotyczącego okresu, w jakim poszczególne organy stosujące kontrolę operacyjną zobligowane byłyby do ich zniszczenia. W przypadku służb specjalnych i organów wywiadu skarbowego wymogiem jest zniszczenie „niezwłoczne", co należy interpretować jako zobowiązanie do podjęcia natychmiastowych czynności w tym zakresie. W przypadku zaś Policji i Żandarmerii Wojskowej ustawodawca określił ten obowiązek w inny sposób, obligując wymienione służby do zniszczenia nieistotnych dla celów procesowych materiałów w okresie dwóch miesięcy od ich uzyskania. Jednoznaczna ocena *ratio legis*, jakie przemawiały i decydowały o takim kierunku rozwiązań, jest trudna do sformułowania.

Wskazana regulacja jest bezdyskusyjnie słuszna przy założeniu pełnienia funkcji gwarancyjnej i kontrolnej, mającej uniemożliwiać służbom policyjnym przechowywanie materiałów z podsłuchu i posługiwanie się nimi, zwłaszcza materiałami dotyczącymi wrażliwych sfer obyczajowych itp. W tym zakresie stanowi ona jednocześnie wyraz braku zaufania do organów uprawnionych do stosowania podsłuchu. W praktyce jednak może stanowić przedmiot kontrowersji i zarzutów wobec służb policyjnych, zwłaszcza w sytuacjach związanych ze stosowaniem kontroli operacyjnej w sprawach o korupcję, kiedy część materiałów kwalifikowana jest jako spełniająca kryteria dowodu procesowego i przekazywana przez służby policyjne do dalszego procedowania w ramach postępowania karnego, a pozostała część, uznawana za niespełniającą wymogów procesowych i niemającą znaczenia dla bezpieczeństwa państwa, jest niezwłocznie, zgodnie z wymogiem ustawowym, niszczona. Pełnomocnicy procesowi w tego rodzaju postępowaniach nawet po wielu latach od momentu zastosowania w danej sprawie podsłuchu kierują do sądu, na etapie postępowania jurysdykcyjnego, wnioski dowodowe o dostarczenie całości materiałów ze stosowanej wcześniej kontroli operacyjnej. Jako powód często wskazują obiekcje co do wiarygodności wyselekcjonowanej, i to przez same służby, części z zarejestrowanych rozmów osób oskarżonych.

---

[35] *Rozporządzenie Prezesa Rady Ministrów z dnia 3 października 2002 r. w sprawie sposobu dokumentowania przeprowadzonej przez Agencję Bezpieczeństwa Wewnętrznego kontroli operacyjnej, przechowywania i przekazywania wniosków i zarządzeń oraz przechowywania, przekazywania, przetwarzania i niszczenia materiałów uzyskanych podczas stosowania tej kontroli* (Dz.U. z 2002 r., Nr. 173, poz. 1414).

[36] Przywoływana już ustawa nowelizująca *Kodeks postępowania karnego* oraz niektóre ustawy policyjne z dnia 10 marca 2011 r. (Dz.U. z 2011 r., Nr 53, poz. 273) wprowadza od 10 czerwca 2011 r. nowy tryb rozstrzygania o zasadności zachowywania materiałów istotnych dla bezpieczeństwa państwa. Zgodnie z projektowanymi zmianami o ewentualnym zachowaniu wymienionych materiałów będzie decydował Sąd Okręgowy w Warszawie, na pisemny wniosek Szefa ABW złożony po uzyskaniu pisemnej zgody na to Prokuratora Generalnego (przepis art. 27 ust. 15f ustawy o ABW oraz AW).

Zdarza się również, iż o zachowanie materiałów z podsłuchu w sprawach związanych z toczącymi się postępowaniami karnymi występują sami prokuratorzy (być może w obawie o zaistnienie sytuacji, o której była mowa powyżej). Otwarte pozostaje w związku z tym pytanie, jak mają zachować się w takich przypadkach przedstawiciele służb policyjnych, zobligowani przez ustawodawcę z jednej strony do niszczenia nieprzydatnych materiałów, a z drugiej do działań, które mogą stanowić zaniechanie ciążącego na nich obowiązku prawnego?

Zasadnicze znaczenie dla rozważań związanych z podsłuchem, zwłaszcza w kontekście niedoskonałości przepisów prawnych regulujących stosowanie tego środka, ma zagadnienie nadzoru nad jego stosowaniem. Przyjmując za punkt odniesienia regulacje obowiązujące w tym zakresie w innych państwach, można stwierdzić, iż polski model kontroli sądowej nie jest zbyt upowszechniony[37].

W Niemczech, których rozwiązania prawne dotyczące podsłuchu i ogólnie metod działania tajnych służb czy służb policyjnych są często przedmiotem odwołań i poszukiwania wzorców przy okazji dyskusji toczonych na ten temat w naszym kraju, filozofia samego systemu metod inwigilacji i istoty nadzoru nad nim jest dość złożona i niejednolita. Ten stan rzeczy jest w dużej mierze historyczną spuścizną modelu kreowania systemu bezpieczeństwa w tym kraju bezpośrednio po zakończeniu II wojny światowej (określanego często w literaturze jako *trennugsgebot*[38]), realizowanego z obawy o odrodzenie się idei nazizmu.

Na gruncie *Ustawy z 26 czerwca 2001 r. o ograniczeniu tajemnicy korespondencji i treści przesyłanych w sieciach telekomunikacyjnych*[39], zgodnie z przepisem paragrafu 10 tej ustawy, organem właściwym do wydania zarządzenia o zastosowaniu podsłuchu jest właściwy organ landowy[40] lub upoważnione przez urząd kanclerski właściwe ministerstwo federalne (minister spraw wewnętrznych lub minister obrony)[41].

Na podstawie § 3 pkt 1 wyżej wymienionej ustawy ograniczenie praw obywatelskich polegające na zastosowaniu podsłuchu może nastąpić wtedy, gdy zaistnieją prze-

[37] Analogiczne pod względem filozofii rozwiązania oparte na systemie nadzoru prokuratorsko-sądowego zawarto w ustawodawstwie litewskim (przepis art. 10 ust. 1 ustawy o czynnościach operacyjnych Republiki Litewskiej z 20.06.2002 r., Nr IX-965). Sądowa kontrola podsłuchu obowiązuje również w Czechach (przepis rozdziału dotyczący podsłuchu i nagrania czynności telekomunikacyjnej w art. 88 kodeksu postępowania sądowego funkcjonującego w ramach ustawy Nr 141 z dnia 29 listopada 1961 r. z późniejszymi zmianami). Słowacja również przyjęła system nadzoru sądowego nad stosowaniem podsłuchu operacyjnego, wykorzystywanego zarówno przez służby bezpieczeństwa (ustawa Nr 72/1993), jaki i stricte policyjne (ustawa Nr 171/1993).

[38] Wynikający z konstytucji Republiki Federalnej Niemiec nakaz „separacji", „rozdziału" (*trennungsgebot*) służb specjalnych od służb policyjnych jest historyczną konsekwencją decyzji władz alianckich delegalizujących po zakończeniu II wojny światowej tajną niemiecką policję polityczną (gestapo). Na mocy tych postanowień administracja niemiecka została zobowiązana do ustanowienia regulacji prawnych skutkujących separacją organów bezpieczeństwa realizujących czynności operacyjne od instytucji policyjnych uprawnionych do wykonywania czynności procesowych. Nakaz rozdziału obowiązuje zarówno na poziomie federalnym, jak i landowym. Znajduje on swoje odzwierciedlenie w zakresie kompetencji poszczególnych służb policyjnych i służb bezpieczeństwa, na poziomie organizacyjnym i funkcjonalnym.

[39] Bundesgesetzblatt 2001, I, 1254, 2298.

[40] Powyższa procedura ma zastosowanie w przypadku wniosków o podsłuch pochodzących z landowych struktur Federalnego Urzędu Ochrony Konstytucji (*Bundesamt für Verfassungsschutz*).

[41] Wskazany tryb jest stosowany odnośnie do wniosków o zastosowanie podsłuchu pochodzących z Federalnego Urzędu Ochrony Konstytucji (j.w.), Wojskowej Służby Kontrwywiadu (*Amt für den Militarischen Abschirmdienst*) i Federalnej Służby Wywiadu (*Bundesnachrichtendienst*).

słanki popełnienia przestępstw m.in. zdrady stanu, zagrożenia obronności kraju, naruszenia porządku konstytucyjnego, zagrożenia terrorystycznego, rozprzestrzeniania broni masowego rażenia, przestępstw przeciwko bezpieczeństwu sojuszniczemu jednostek wojskowych państw członkowskich NATO stacjonujących na terenie Niemiec oraz naruszenia przepisów ustawy o cudzoziemcach. Istotne przy tym jest to, że zgodnie z § 3 pkt 2 ustawy z 2001 r. o ograniczeniu tajemnicy kontroli korespondencji i treści przesyłanych w sieciach telekomunikacyjnych krąg osób, wobec których wydaje się zarządzenie o zastosowanie podsłuchu, nie obejmuje tylko i wyłącznie osoby podejrzewanej o związek z wyżej wymienionymi przestępstwami, ale również osoby, co do których istnieje przypuszczenie, że mogą przekazywać lub odbierać od takiej osoby informacje, albo że soba podejrzewana o związek z wyżej wymienionymi przestępstwami korzysta z ich łącza telekomunikacyjnego.

Niemiecka ustawa o Federalnym Urzędzie Kryminalnym oraz o współpracy federacji z krajami związkowymi w sprawach kryminalno-policyjnych (Bundeskriminalgesetz – BKAG) z dnia 7 lipca 1997 r., ze zmianami wprowadzonymi w dniu 25 grudnia 2008 r.[42] w art. 1 ustawy o przeciwdziałaniu zagrożeniu terroryzmem międzynarodowym przez Federalny Urząd Kryminalny, przewiduje nadzór sądowy nad stosowaniem zarówno podsłuchu internetowego, jak i telekomunikacyjnego. Przepis § 20k pkt 1 powyższej ustawy zawiera możliwość zastosowania przez BKA niejawnej ingerencji w systemy teleinformatyczne, polegającej na wykorzystaniu urządzeń techniki specjalnej w celu przeniknięcia do użytkowanych przez osobę podsłuchiwaną systemów teleinformatycznych i pobrania z nich danych.

Przesłanki formalnoprawne stanowiące podstawę wnioskowania o podsłuch teleinformatyczny, związane z zagrożeniem życia, zdrowia lub wolności człowieka albo innego dobra społecznego stanowiącego podstawy trwałości państwa, muszą, zgodnie z przepisem § 20k pkt pkt 1 i 2 pozostawać w związku z przeciwdziałaniem zagrożeniu terroryzmem międzynarodowym. Przepis § 20 pkt pkt 5 i 6 ustawy przewiduje możliwość zastosowania tego środka na okres 3 miesięcy, a nastepnie ewentualnego przedłużenia go o następne 3 miesiące. Jednocześnie jego wykorzystanie poddaje kontroli sądowej.

Zbliżone pod względem formalnym rozwiązania obowiązują BKA jeśli chodzi o podsłuch telekomunikacyjny. Przepis § 20l wyżej wymienionej ustawy, stanowiący podstawę do wnioskowania o omawiany środek, zezwala tej służbie na niejawne monitorowanie i rejestrację przekazów w sieci telekomunikacyjnej podsłuchiwanej osoby w przypadku wystąpienia poniższych przesłanek:

- zagrożenia ze strony takiej osoby dla niepodległości państwa albo dla życia, zdrowia i wolności osób lub mienia o znacznej wartości,
- możliwości dokonania przez osobę, wobec której planuje się stosować podsłuch, motywowanych politycznie zamachów na osoby piastujące najwyższe funkcje w państwie,
- podejrzenia przekazywania informacji przeznaczonych dla określonego kręgu odbiorców lub pochodzących od osób związanych z zagrożeniami ujętymi w pierwszej przesłance,

[42] Bundesgesetzblatt IS. 3083.

- podejrzenia, że osoby wskazane w przesłance pierwszej będą korzystały z ich łącz telekomunikacyjnych lub aparatów.

Analogicznie jak w przypadku podsłuchu informatycznego, sąd zarządza (art. § 20l pkt 3) podjęcie czynności związanych z założeniem podsłuchu telekomunikacyjnego w przypadku wniosków rozpatrywanych w trybie niecierpiącym zwłoki i w ciągu 3 dni ustosunkowuje się do podjętych czynności (działania tego typu zarządzane są przez szefa lub zastępcę szefa BKA).

W Wielkiej Brytanii zasadnicze znaczenie dla określenia procedur postępowania w sprawach o podsłuch posiada cytowany już *Kodeks postępowania w sprawach o przechwytywanie informacji*, stanowiący dopełnienie wskazówek zawartych w rozdziale pierwszym ustawy o organach śledczych z 2000 r. Na podkreślenie zasługuje fakt, że powyższa ustawa przyznaje wymienionemu kodeksowi znaczenie dowodowe zarówno w sprawach karnych, jak i cywilnych.

Zgodnie z § 8 pkt 1 wyżej wymienionego *Kodeksu* nakaz uprawniający do przechwytywania informacji wydawany jest przez urząd sekretarza stanu (*the Secretary of State*) w Ministerstwie Spraw Wewnętrznych. W wypadkach niecierpiących zwłoki, w przypadku niemożności wydania nakazu przez sekretarza stanu, zarządzenie o podsłuchu może być wydane przez urzędnika wyższej rangi (*senior official*). Jednak w ciągu 5 dni tego rodzaju nakaz winien być przez sekretarza stanu autoryzowany.

Na podstawie § 2 pkt 3 *Kodeksu* sekretarz stanu przed wydaniem nakazu przechwycenia komunikacji musi być przekony o konieczności zastosowania podsłuchu z uwagi na występowanie przesłanek uzasadniających, wskazujących z jednej strony na istnienie zagrożeń dla interesu bezpieczeństwa narodowego, a za drugiej na możliwość zapobieżenia lub wykrycia poważnego przestępstwa lub na konieczność ochrony bezpieczeństwa ekonomicznego Zjednoczonego Królestwa.

Analizując system nadzoru nad stosowaniem podsłuchu w Wielkiej Brytanii, warto podkreślić znaczenie jeszcze innych instytucji w tym zakresie – urzędu Komisarza ds. Przechwytywania Komunikacji oraz Trybunału ds. Kontroli Komunikowania się.

Komisarz ds. Przechwytywania Komunikacji, powoływany przez premiera, zajmuje się sprawowaniem kontroli nad działalnością urzędu sekretarza stanu. Trybunał ds. Kontroli Komunikowania się jest natomiast organem niezależnym od władzy wykonawczej i składa się z sędziów oraz osób z wykształceniem prawniczym o odpowiednim stażu i doświadczeniu.

Kodeks postępowania w sprawach o przechwytywanie informacji, na podstawie z przepisu § 2 pkt 9, przewiduje również możliwość odwoływania się przez operatorów telekomunikacyjnych od decyzji o zastosowaniu nakazu wydanego przez sekretarza stanu w przypadku niemożności sprostania wymogom technicznym związanym z realizacją tego nakazu. Zgodnie z wymienioną procedurą odwołanie w celu zasięgnięcia opinii kierowane jest do Ławy Doradztwa Technicznego (*Technical Advisory Board* – TAB).

W Belgii natomiast obowiązuje dualny system nadzoru nad stosowaniem podsłuchu. W przypadku wniosków pochodzących od służb bezpieczeństwa kontrola sprawowana jest przez Komisję administracyjną ds. nadzoru nad realizacją podsłuchu. Komisja ta jest organem administracyjnym składającym się z sześciu osób powoływanych dekretem królewskim na wniosek Rady Ministrów na okres pięciu lat. Członkowie komisji, w ramach swoich uprawnień, mają prawo do zapoznania się z materiałami uzasadniającymi wniosek o podsłuch. Stosowanie wymienionego środka przez policję belgijską poddawane jest nadzorowi sądowemu, sprawowanemu przez sędziów śled-

czych (przepisy art. 90 ust. od 3 do 10 kodeksu postępowania karnego Królestwa Belgii z dnia 30 czerwca 1994 r.).

Na Węgrzech system nadzoru nad stosowaniem podsłuchu regulowany jest ustawą z dnia 19 grudnia 1995 r. o służbach bezpieczeństwa narodowego oraz szeregiem innych ustaw i przepisów wykonawczych regulujących tę problematykę[43]. Zgodnie z § 58 pkt 1 w związku z § 5 pkt pkt b, d i h - j oraz z § 7 pkt pkt b, d, i - k cytowanej ustawy sędzia wyznaczony przez przewodniczącego sądu metropolitalnego w Budapeszcie (odpowiednik sądu okręgowego w przypadku procedur realizowanych zgodnie z ustawami policyjnymi w naszym kraju) jest właściwy w zakresie nadzoru nad stosowaniem podsłuchu w sprawach o przestępstwa dotyczące m.in. porządku konstytucyjnego, bezpieczeństwa ekonomicznego, handlu narkotykami, bronią, przestępstw granicznych, przestępstw na tle rasowym, etnicznym oraz naruszania przepisów o tajemnicy państwowej. Warto przy tym podkreślić, że wystawienie wniosków o zastosowanie podsłuchu dotyczące ujętej wyżej właściwości rzeczowej, pozostaje w sferze zadań Urzędu Bezpieczeństwa Narodowego oraz Urzędu Bezpieczeństwa Wojskowego. W pozostałych sprawach związanych z właściwością tak powyższych organów, jak i Urzędu Wywiadu oraz Urzędu Wywiadu Wojskowego, zwłaszcza odnoszących się do działalności obcych służb specjalnych, szpiegostwa, wywiadu, kontrwywiadu, nieproliferacji, obrotu towarami podwójnego zastosowania, nadzór nad stosowaniem podsłuchów, zgodnie z przepisem § 58 pkt 2 ustawy o służbach bezpieczeństwa narodowego, sprawuje minister sprawiedliwości.

Przyjmując za punkt odniesienia regulacje obowiązujące w innych systemach prawnych, należy jednoznacznie stwierdzić, że przyjęty w naszym kraju model sądowego nadzoru nad stosowaniem podsłuchu jest w dalszym ciągu jednym z nielicznych w Europie, który poddaje podsłuch *ex ante* całkowitej kontroli ze strony niezależnego organu, jakim jest sąd. Pod tym względem jest to jedno z najbardziej rygorystycznych rozwiązań, co przeczy pojawiającym się często opiniom sugerującym nazbyt liberalne formy kontroli nad tą instytucją w Polsce. Warto jednak mieć również świadomość tego, że pomimo formalnego nadzoru sądowego, najważniejszą rolę w przyjętym w naszym kraju modelu odgrywa w dalszym ciągu prokuratura.

Wątpliwości związane z *ratio legis* ustawodawcy może budzić zawarte we wszystkich ustawach policyjnych rozwiązanie pozbawiające służby uprawnione do stosowania podsłuchu możliwości odwoływania się od negatywnej decyzji prokuratury w sprawie zastosowania tego środka. Skutkuje to tym, że sąd pełni funkcję kontrolną jedynie wobec tych wniosków , które zostaną zaakceptowane przez prokuratora i przekazane do dalszego procedowania przez sąd. Intencja, jaką w zakresie wymienionego rozwiązania mógł kierować się ustawodawca staje się niezrozumiała, gdy skonfrontujemy ją z zapisami zawartymi we wszystkich ustawach policyjnych[44], przyznających służbom operacyjnym prawo zaskarżania odmownych decyzji sądu dotyczących wykorzystywania podsłuchu.

---

[43] *Ustawa XXXV z 2001 r. o podpisie elektronicznym*; *Ustawa C z 2003 r. o komunikacji elektronicznej*, *Dekret 22/2002 Szefa Kancelarii Premiera z 2002 r. o obowiązku dostarczania danych przez podmioty świadczące usługi telekomunikacyjne, zarządzaniu danymi i rejestrze prowadzonym przez władze telekomunikacyjne.*

[44] Przepis art. 27 ust. 11a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu wskazuje w tym zakresie expressis verbis, iż *na postanowienia Sądu, o których mowa w ust. 1, 3, 8, 9, Szefowi ABW przysługuje zażalenie. Do zażalenia stosuje się odpowiednio przepisy „Kodeksu postępowania karnego”.* Analogiczne w treści zapisy, określające prawo zaskarżenia przez służby odmownych decyzji czy postanowień sądu dotyczących podsłuchów, przyjęto we wszystkich pozostałych ustawach policyjnych.

Konsekwencją powyższego jest to, iż instancją odwoławczą od decyzji sądu okręgowego w wymienionym zakresie jest sąd apelacyjny. Organ ten mógłby być również instancją właściwą do rozpatrywania odwołań poszczególnych służb policyjnych od negatywnych decyzji prokuratura w tej sprawie.

Odrębną kwestią jest natomiast szereg zastrzeżeń, jakie można wysuwać wobec braku jednoznacznych rozwiązań lub niewystarczająco precyzyjnych przepisów odnośnie do obszarów posługiwania się omawianym środkiem. W niniejszym artykule zawarto wiele przykładów świadczących o powyższym. Zasadnicze znaczenie dla oceny istniejącego w tym względzie stanu rzeczy ma kwestia konsekwencji, jakie przedmiotowa sytuacja powoduje w praktyce. Niejasne, nieostre znaczeniowo i funkcjonalnie przepisy powodują, iż organy stosujące je w codzienej pracy (tj. służby policyjne, prokuratura i sąd) często zmuszone są nie tyle do ich stosowania, co do doszukiwania się intencji (*ratio legis*) ustawodawcy.

Abstrahując od negatywnej oceny wskazanej wyżej sytuacji, należy podkreślić, że jest ona zdecydowanie niepożądana również z punktu widzenia zasad działania służb policyjnych. We właściwie funkcjonujących systemach prawnych służby posługujące się technikami operacyjnymi, zwłaszcza tak wrażliwymi, jak podsłuch czy prowokacja, nie mają tak dalece idących dylematów. Służby te winny działać w tym obszarze zgodnie z jasno określonymi regułami prawnymi. Precyzyjnie określone normy są jednocześnie skutecznym narzędziem kontrolnym.

W chwili obecnej mamy zaś do czynienia z sytuacją, w której szereg przepisów dotyczących nie tylko podsłuchu, ale i innych środków i technik pracy operacyjne, ważnych z punktu widzenia reguł prawa, przestrzegania norm i przepisów obywatelskich, takich jak granice prowokowania do popełnienia przestępstwa oraz posługiwanie się tajnym agentem, charakteryzuje nadmierna ogólnikowość lub wręcz unikanie przez ustawodawcę próby sformułowania jakichkolwiek zasad, zgodnie z którymi narzędzia te mogłyby być stosowane. Porównując szereg regulacji występujących w Polsce i w systemach prawnych innych krajów można odnieść wrażenie, że ustawodawca, unikając podejmowania trudnych zagadnień, pozostaje w błędnym w przekonaniu, że problemy rozwiążą się same, bez jego ingerencji.

W niniejszej publikacji nie poruszono istotnej kwestii związanej z wątpliwościami i problemami, jakie nasuwa stosowanie instytucji tzw. zgody następczej, procedury konwalidującej w obszarze funkcjonowania podsłuchu. Z instytucją tą mamy do czynienia wtedy, gdy podczas stosowania podsłuchu uzyskuje się dowody popełnienia przestępstwa, w którego sprawie można zarządzić kontrolę operacyjną. Przestępstwo to popełniane jest przez osobę, wobec której była już stosowana kontrola operacyjna, ale jest to już inne przestępstwo lub jest popełnione przez inną osobę, która wcześniej nie była objęta kontrolą.

Na przestrzeni ostatnich lat o zasadach dotyczących zgody następczej wypowiadał się m.in. Sąd Najwyższy. W przywoływanej już wielokrotnie nowelizacji kodeksu postępowania karnego i niektórych innych ustaw z dnia 10 marca 2011 r. również podjęto to zagadnienie. Konieczność przeprowadzenia głębszych rozważań nad tą problematyką stanowi o zasadności jej podjęcia w kolejnych numerach „Przeglądu Bezpieczeństwa Wewnętrznego".

Streszczenie

Spośród wszystkich metod operacyjnych stosowanych przez służby policyjne najwięcej kontrowersji wśród polskiego społeczeństwa budzi wykorzystywanie podsłuchu. Uzasadnienie tego stanu rzeczy zawiera się z pewnością w ingerencji podsłuchu w podstawowe prawa obywatelskie, m.in. w prawo do poszanowania prywatności. Wpływ na pejoratywny odbiór tej instytucji ma również jej dyskrecjonalny charakter, charakteryzujący się dalece posuniętą niejawnością jej stosowania.

Niniejsza publikacja, czyniąc z jednej strony zadość niezbędnym, uzasadnionym rygorom dyskrecjonalności, stanowi jednocześnie próbę prezentacji podstawowych cech charakteryzujących instytucję podsłuchu oraz dylematów towarzyszących jej stosowaniu.

Przyjmując pewne uproszczenie w zakresie nazewnictwa należy przyjąć, iż tzw. prawo podsłuchowe w naszym kraju jest zbiorem niedoskonałych rozwiązań i regulacji, budzących wiele wątpliwości, co w niniejszej publikacji wykazywano wielokrotnie. Szczególnie istotna i wymagająca podkreślenia jest w tym zakresie postawa ustawodawcy, który unika podejmowania jednoznacznych rozstrzygnięć w tych kwestiach, które w innych krajach są przedmiotem zainteresowania i ustawowych regulacji.

Za bezsporną należy uznać również krytyczną ocenę nadmiernej reglamentacji uprawnienia do stosowania podsłuchu w naszym kraju. Zbyt wielu (w ocenie autora artykułu) służbom i instytucjom w Polsce przyznano to uprawnienie, co wpłynęło na formułowanie opinii o nadmiernym upolicyjnieniu struktur państwa zajmujących się zagadnieniem bezpieczeństwa, ładu konstytucyjnego i porządku publicznego.

Faktem pozytywnym jest pojawienie się w naszym kraju części rozwiązań ustawowych, takich jak sądowa kontrola nad stosowaniem podsłuchu, z pewnymi zastrzeżeniami dotyczącymi braku możliwości zaskarżenia przez służby policyjne odmownej decyzji prokuratora w sprawie zastosowania tej instytucji. Sąd, w ramach gwarancji niezawisłości i bezstronności, decyduje o zasadności i legalności ingerowania przez państwo (tu reprezentowane przez służby policyjne) w sferę szczególnie wrażliwego obszaru, jakim jest prawo człowieka do prywatności.

Warto mieć świadomość, że obowiązujący w Polsce system nadzoru nad stosowaniem podsłuchów jest jednym z bardziej rygorystycznych rozwiązań obowiązujących w Europie, co przeczy występującym często w dyskursie publicznym opiniom sugerującym zupełnie inny stan rzeczy.

ABSTRACT

Wiretapping is the most controversial of all operational methods utilized by law enforcement institutions in the perception of both the society and the media. One of the reasons for such situation derives from the fact that through wiretapping law enforcement institutions interfere with the guarantee of the civil rights among others the right to privacy. The Negative impact on the perception of that phenomenon is also caused by the confidentiality of rules and principles of its application.

This article is an attempt to present the basic features of wiretapping, including the dilemmas surrounding the use of this institution in the daily practice connected with the aspect of its confidentiality.

Briefly referring to the subject matter and the used nomenclature, it has to be assumed that so called ‘law on wiretapping’ in Poland is a collection of imperfect so-

lutions and regulations, raising doubts and ambiguities, as demonstrated repeatedly in this article. Particularly important is the attitude of the legislator, who avoids making unambiguous decisions, relating to the law and other regulations, which in other countries are of interest.

Critics have negative opinion about the excessive powers to the regulation of the use of wiretaps in Poland. In the author's opinion, too many institutions in Poland have been granted permission to wiretapping. This is the basis for the opinion of the police-oriented (dealing with issues of national security, constitutional order and public policy) structures of the state.

Undisputable fact, having a positive impact on the subject matter, is the adoption in Poland of the regulations on the supervision of the system in the form of judicial supervision with caveats on the impossibility of appeal by special services against a negative decision of the prosecutor concerning wiretapping. The court decides on the validity and legality of the interference by the state police services in the sphere of privacy of other sensitive areas.

It is worth highlighting that Poland has one of the most rigorous systems of supervision over the use of wiretapping in Europe. The fact contradicts common public opinions on legal regulations

Kazimierz Mordaszewski

Retencja danych objętych tajemnicą telekomunikacyjną w świetle prawa europejskiego i polskiego

I

Pojęcie r e t e n c j a wymaga etymologicznej interpretacji i wyjaśnienia jego dokładnego znaczenia. Pochodzi ono od łacińskiego słowa *retentio* i oznacza „zatrzymanie", „powstrzymywanie", „bycie zatrzymanym"[1]. Słowo to weszło do powszechnego użycia, podobnie bowiem brzmi w językach roboczych UE, tj. w języku francuskim (*rétention*) i angielskim (*retention*)[2] i w obu przypadkach ma takie samo znaczenie. R e t e n c j a w geologii oznacza zdolność do magazynowania (*retention)* wody opadowej w gruncie, jeziorach i rzekach lub zbiornikach retencyjnych[3]. Określenie to w terminologii prawnej oznacza (w ujęciu potocznym) prawo do zatrzymania należących do dłużnika przedmiotów w wypadku roszczenia o zwrot nakładów. Mogą to być rzeczy stanowiące przedmiot zastawu, jeśli zostały oznaczone w sposób, który je indywidualizuje[4]. Instytucją prawną, od dawna stosowaną w obrocie prawnym, jest zastaw jako ograniczone prawo rzeczowe stanowiące formę zabezpieczenia wierzytelności na rzeczach ruchomych i niektórych prawach. Może powstać na podstawie czynności prawnej i *ex lege*, czyli jako zastaw ustawowy.

Retencja danych w telekomunikacji oznacza gromadzenie, przechowywanie i archiwizowanie lub usuwanie zapisów dotyczących komunikacji, np. o połączeniach telefonicznych czy danych o ruchu w sieciach telekomunikacyjnych dla potrzeb organów ścigania i służb specjalnych. Pojecie to może także obejmować dane przesyłane poprzez system teleinformatyczny drogą elektroniczną umożliwiającą porozumiewanie się za pomocą środków komunikacji elektronicznej, w szczególności poczty elektronicznej.

Retencja danych ma służyć zapobieganiu przestępczości, a szczególnie terroryzmowi, poprzez docieranie do wszelkich możliwych elektronicznych danych, które mogą okazać się naprowadzeniami na dowody popełnionego przestępstwa. Dowodami tymi mogą być dane o ruchu w sieci, generowane podczas prowadzenia zwykłej działalności przedsiebiorców telekomunikacyjnych lub przez dostawców dostępu do internetu. Przepisy dotyczące retencji danych obligują operatorów telekomunikacyjnych i dostawców usług internetowych do rutynowego zatrzymywania na czas określony danych ruchowych przechodzących w ich serwerach.

---

[1] *Słownik wyrazów obcych*, Warszawa 1980, PWN, s. 646.

[2] Por. *Webster Third New International Dictionary,* Springfield, Mass., 2000, s. 1938; *Słownik prawniczy polsko-angielski*, PAN, Ossolineum 1986, s. 202.

[3] *Słownik języka polskiego*, tom 3, Warszawa 1980, PWN, s. 51.

[4] *Kodeks cywilny z komentarzem*, J. Winiarz (red.), t. 1, Warszawa 1989, Wydawnictwo Prawnicze, s. 249.

II

W społeczeństwach demokratycznych obywatele wykorzystują różne środki oddziaływania, żeby zwrócić uwagę ustawodawcy i wpływać na kształt przepisów. Mogą to być otwarte dyskusje, wysyłanie listów, tworzenie grup obywatelskich, prezentowanie stanowisk poprzez organizacje pozarządowe itd[5].

Od pewnego czasu w środowiskach naukowych, organizacjach pozarządowych i środkach masowego przekazu toczy się dyskusja o wykorzystywaniu bilingów przez służby policyjne. Często jest to dyskusja z tezą przyjętą z góry, że służby te, strzegąc porządku publicznego i bezpieczeństwa państwa, niezasadnie ograniczają prawa i wolności obywatelskie. Można chociażby przywołać interesującą dyskusję, która toczyła się na konferencji zorganizowanej w dniu 17 grudnia 2010 r. przez Uniwersytet Kardynała Stefana Wyszyńskiego w Warszawie, Generalnego Inspektora Ochrony Danych Osobowych oraz Naukowe Centrum Prawno-Informatyczne. Dyskusja ta, zdaniem GIODO, „wbiła kij w mrowisko", czyli była punktem wyjścia do prac nad tzw. dużą nowelizacją ustawy o ochronie danych osobowych. Spotkanie moderowała prof. Irena Lipowicz – Rzecznik Praw Obywatelskich, wypowiadając się na temat stanu prawnego w zakresie retencji danych w świetle zasad konstytucyjnych i wywodząc w konkluzji, że stan ten jest niezgodny z Konstytucją RP. Poza tym głos zabrał m.in.: Wojciech Wiewiórowski (GIODO), który wygłosił referat pt. *Privacy by Design jako paradygmat ochrony prywatności* i podkreślił wagę ochrony danych osobowych, łącznie z tzw. prawem zapomnienia. Z punktu widzenia tematyki niniejszego artykułu istotne było wystąpienie prof. Andrzeja Adamskiego (UMK), które dotyczyło retencji danych telekomunikacyjnych w kontekście zasady proporcjonalności. Z przywołanych przez niego badań wynika, że prokuratorzy w 70% spraw występują o obszerne dane pochodzące z bilingów również w niezbyt istotnych sprawach. Dane te są powszechnie wykorzystywane w postępowaniach w sprawach narkotykowych, nawet dotyczących drobnych dilerów. Wystarczy, że osoba nie związana ze sprawą występuje w bilingu, a wzywana jest do prokuratury w celu złożenia stosownych wyjaśnień. W niewielkich środowiskach tego typu sytuacja komentowana jest w sposób nieprzychylny dla takiego przypadkowego uczestnika postępowania karnego. Dotyczy to na przykład nauczycieli. Zdaniem A. Adamskiego, prawo telekomunikacyjne i ustawa o Policji w zakresie korzystania z danych bilingowych naruszają zasady konstytucyjne.

W niektórych artykułach prasowych tytuły brzmią alarmująco, przestrzegając przed naruszaniem przez służby swobód obywatelskich. Kazimierz Olejnik – były zastępca Prokuratora Generalnego – w wywiadzie dla „Gazety Wyborczej"[6] stwierdził, że sprawdzanie bilingów dziennikarzy to działanie sprzeczne z prawem, za które Polska będzie płacić odszkodowania na skutek zaskarżania tego typu czynności do Trybunału w Strasburgu. Z artykułu red. E. Siedleckiej natomiast wynika, że w Polsce ponad milion zapytań służb o bilingi czyni nas absolutnym liderem w UE[7]. W komentarzu autorka wskazuje, *że rząd zamiast uregulować inwigilację na europejskim poziomie, rozsądnie godząc ochronę bezpieczeństwa z poszanowaniem prywatności, poddaje się temu szantażowi* (w domyśle służb, które szantażują zagrożeniem).

[5] Por. B. D. Fisher, *Law for business*, New York 1991, West Publishing Company, s. 111.
[6] A. Kublik, *Służby wciskają ciemnotę*, „Gazeta Wyborcza" z dnia 22 października 2010 r.
[7] E. Siedlecka, *Służby zaglądają nam w telefon*, „Gazeta Wyborcza" z dnia 9 listopada 2010 r.

W artykule pt. *Bilingi tylko za zgodą sądu*[8] mec. mec. Jacek Kondracki i Krzysztof Stępiński, polemizując z Prokuratorem Dariuszem Barskim, stwierdzają, że dostęp służb do bilingów dziennikarzy jest możliwy tylko za zgodą sądu. Były Prokurator Krajowy D. Barski prezentuje odmienny pogląd. Twierdzi, *iż prawa i wolności obywatelskie ulegają jednak ograniczeniom określonym w przepisach prawa w imię racji uznanych przez ustawodawcę za nadrzędną w stosunku do tych praw i wolności*[9].

Zatem w toczącej się w naszym kraju dyskusji publicznej o wykorzystywaniu bilingów przez służby, w środkach masowego przekazu przeważa stanowisko prezentowane przez organizacje pozarządowe, aczkolwiek inne poglądy dotyczące tego problemu także są dostrzegalne.

III

Wspomiana wyżej dyskusja dotyczy ostatecznie kwestii fundamentalnych, jakimi z jednaej strony są prawna ochrona prywatności oraz prawa i wolności osobiste, a z drugiej – ograniczenia tajemnicy komunikowania się. Debata toczy się na poziomie zarówno krajowym, jak i europejskim.

Akceptowany obecnie w Europie standard gwarancji praw człowieka wyznacza przyjęta w ramach Rady Europy *Konwencja o ochronie praw człowieka i podstawowych wolności*. Państwa członkowie Rady Europy uznały, że jednym z celów Rady jest ochrona oraz rozwój praw człowieka i podstawowych wolności, i odwołując się do *Powszechnej Deklaracji Praw Człowieka* uchwalonej 10 grudnia 1948 r. przez Zgromadzenie Ogólne Narodów Zjednoczonych, przyjęli w listopadzie 1950 r. Konwencję. Konwencja ta, zwana popularnie Europejską Konwencją Praw Człowieka, weszła w życie 3 września 1953 r., a Polska ratyfikowała ją 15 grudnia 1992 r.[10]. Z art. 8 ust. 1 tego dokumentu wynika, że każdy ma prawo do poszanowania swojej korespondencji, co dotyczy także technicznych form przekazywania wiadomości. Zgodnie z art. 8 ust. 2 natomiast niedopuszczalna jest ingerencja władzy publicznej w prawo do poszanowania korespondencji, z wyjątkiem przypadków koniecznych w demokratycznym społeczeństwie, związanych m.in. z zagrożeniem dla bezpieczeństwa państwa, bezpieczeństwa publicznego lub dobrobytu gospodarczego kraju i z zapobieganiem przestępstwom.

Należy podkreślić, że w celu zapewnienia przestrzegania zobowiązań z *Konwencji* i jej protokołów utworzony został Europejski Trybunał Praw Człowieka z siedzibą w Strasburgu. Każdy obywatel państwa członkowskiego, organizacja pozarządowa lub grupa jednostek, która uważa, że stała się ofiarą naruszenia przez państwo członkowskie praw zawartych w Konwencji lub w jej protokołach, może złożyć skargę do tego Trybunału.

Zgodnie z postanowieniami Konwencji[11] Trybunał może zacząć rozpatrywać sprawę dopiero po wyczerpaniu wszystkich środków odwoławczych przewidzianych prawem wewnętrznym, na podstawie powszechnie uznanych zasad prawa międzynarodowego, oraz jeśli sprawa została wniesiona w ciągu sześciu miesięcy od daty podję-

[8] J. Kondracki, K. Stępinski, *Bilingi tylko za zgodą sądu*, „Rzeczpospolita" z dnia 19 października 2010 r.
[9] D. Barski, *Tajemnica dziennikarska nie chroni bilingów*, „Rzeczpospolita" z dnia 15 października 2010 r.
[10] Dz.U. z 1993 r., Nr 61, poz. 284.
[11] Por. art. 35 *Konwencji o ochronie praw człowieka i podstawowych wolności.*

cia ostatecznej decyzji. Jest to istotny element funkcjonowania europejskiego systemu ochrony praw człowieka, którego brak powodował, że mimo ratyfikacji traktatów, takich jak Międzynarodowy Pakt Praw Obywatelskich i Politycznych, nie było radykalnego podwyższenia standardów ochrony praw człowieka w praktyce wielu krajów[12]. Większy wpływ niż zobowiązania traktatowe wywierają często czynniki pozaprawne. Gwałtowny rozwój nowych technologii w ostatnich trzydziestu latach wpływa na poziom życia codziennego, prowadzenie biznesu, a także na kwestie praw człowieka. Po raz pierwszy wszystkie rodzaje informacji – liczby, tekst, dźwięk, video – mogą być zapisywane w formie cyfrowej na komputerach, przetwarzane i przesyłane dalej[13]. Właśnie rozwój telewizji i internetu powoduje, że naruszanie praw człowieka staje się coraz bardziej widoczne. Państwa zawsze były skłonne płacić (choć nie za dużo), żeby usunąć dostrzegalne naruszanie praw człowieka w innych państwach, niezależnie od wymogów międzynarodowych[14]. Przykładem może być sytuacja w wielu krajach Afryki i Ameryki Południowej, gdzie naruszanie praw człowieka bywało drastyczne. Państwa demokratyczne i organizacje międzynarodowe podejmowały interwencje humanitarne dopiero wtedy, gdy dochodziło do zbrodni ludobójstwa. Dopiero ex post została powołana Międzynarodowa Komisja Śledcza do spraw sytuacji w Darfurze oraz Międzynarodowy Trybunał Karny dla Rwandy. W Europie mieliśmy do czynienia z taką sytuacją w latach 90. XX wieku na Bałkanach, gdy interwencja NATO w byłej Jugosławii powstrzymała dalsze zbrodnie przeciwko ludzkości w Bośni i Hercegowinie. Ostatecznie został powołany Międzynarodowy Trybunał Karny dla byłej Jugosławii[15]. Obecne ruchy wolnościowe i zmiany systemów w państwach arabskich zmierzajace ku demokratyzacji rozpoczęły się w dużym stopniu również pod wpływem informacji przekazywanych za pośrednictwem telewizji informacyjnych oraz domen społecznościowych w internecie.

Zdaniem dr. Wolfganga Zellnera, zastępcy dyrektora Instytutu Badań nad Pokojem i Polityką Bezpieczeństwa na Uniwersytecie w Hamburgu i szefa centrum badań OBWE[16], zagrożenia, które mogą się pojawić na terenie OBWE, nie będą miały charakteru międzypaństwowego, tylko transgraniczny. Ich źródłem może być niewydolność państw w zapewnieniu prawidłowego funkcjonowania demokratycznych instytucji[17].

Polska jest krajem, w którym podstawowe prawa człowieka są przestrzegane. Prawa te w Rzeczypospolitej – demokratycznym państwie prawa – są chronione dzięki zapisom w Konstytucji (m.in. w art. art. 47 i 49). Wolności i tajemnicy komunikowania się dotyczy w szczególności prawo telekomunikacyjne oraz prawo prasowe.

Zgodnie z Konstytucją RP ograniczenia w zakresie korzystania z wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne dla porządku

[12] J. Goldsmith, *The limits of international law*, New York 2005, Oxford University Press, s. 120 - 121.

[13] B. Gates, *Business and the speed of thought, using a digital nervous system*, A time Warner Company, New York 1999, s. 15.

[14] J. Goldsmith, *The limits of* ..., s. 123.

[15] Por. *The UN Genocide Convention, a Commentary*, P. Gaeta (red.), Oxford 2009, Oxford University Press.

[16] OSCE, *Ministerial Council*, Maastricht 2003, 2 December 2003, OSCE *Strategy to Address Threats to Security and Stability in the Twenty-First Century*, http://www.osce.org/documents/mcs/2003/12/4175_en.pdf.

[17] Po. W. Zellner, „Security and Human Rights" 2008, nr 4.

publicznego lub zapewnienia bezpieczeństwa demokratycznego państwa (art. 31 ust. 3 *Konstytucji RP*). Ograniczenia prywatności w zakresie komunikowania się poprzez udostępnianie danych bilingowych dla celów ścigania przestępstw organom odpowiedzialnym za egzekwowanie prawa regulowane są w tzw. ustawach pragmatycznych, tj. w ustawie o Policji, Straży Granicznej, Żandarmerii Wojskowej, wywiadzie skarbowym oraz w ustawach dotyczących poszczególnych służb specjalnych: ABW, AW, CBA oraz SKW i SWW.

IV

W prawie unijnym powyższe zagadnienie reguluje *Dyrektywa 2006/24/WE Parlamentu Europejskiego i Rady z 15.03.2006 r. w sprawie zatrzymywania generowanych lub przetwarzanych danych w związku ze świadczeniem ogólnie dostępnych usług łączności elektronicznej lub udostępnianiem publicznych sieci łączności*. Dyrektywa ta określa cel, jakim jest ułatwienie wykrywania, zapobiegania i ścigania poważnych przestępstw podkreślając, że istotne jest, aby państwa członkowskie przyjęły środki legislacyjne zapewniające udostępnianie danych zatrzymywanych na jej mocy jedynie właściwym organom krajowym, zgodnie z ustawodawstwem krajowym, przy pełnym poszanowaniu podstawowych praw osób zainteresowanych. *Dyrektywa* nie definiuje jednak pojęcia p o w a ż n e p r z e s t ę p s t w a[18], zostawiając tę kwestię do uregulowania państwom członkowskim.

Proponowane regulacje budziły żywe dyskusje oraz sprzeciw organizacji pozarządowych. Podczas uchwalania wyżej wymienionej dyrektywy nie doszło jednak do poważnej różnicy zdań w UE. Propozycje Komisji przeszły w Parlamencie przy poparciu chrześcijańskich demokratów (EPP) oraz socjalistów (PSE). Z kolei w Radzie nową dyrektywę popierała Wielka Brytania sprawująca wówczas prezydencję. *Głosowanie w parlamencie Europejskim stanowi wyraźny sygnał, że Europa jest zjednoczona przeciw terroryzmowi i zorganizowanej przestępczości* – komentował w grudniu 2005 r. Charles Clarke, minister spraw wewnętrznych Wielkiej Brytanii.

V

W krajach członkowskich UE dyrektywa nie obowiązuje wprost; winna być implementowana do krajowego porządku prawnego. Taką implementację wyżej wymienionej dyrektywy do prawa polskiego stanowią art. art. 180a i 180c *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*. Na podstawie art. 180a operator publicznej sieci telekomunikacyjnej oraz dostawca usług telekomunikacyjnych są obowiązani zatrzymywać, chronić i udostępniać dane wskazane w art. 180c (potocznie nazywane „bilingowymi”[19]) uprawnionym podmiotom (służbom) oraz sądowi i prokuratorowi, w trybie określonym w odrębnych przepisach. Dane muszą być chronione zgodnie z przestrze-

[18] Por. w wersji angielskiej – *for the purpose of the investigation, detection and prosecution of serious crime, as defined by each Member State in its national law.*

[19] Dane niezbędne do ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego, użytkownika końcowego inicjującego połączenie lub do którego kierowane jest połączenie, a także do określenia: daty i godziny połączenia, czasu jego trwania oraz rodzaju połączenia i lokalizacji telekomunikacyjnego urządzenia końcowego.

ganiem zasady tajemnicy telekomunikacyjnej. Tajemnicę telekomunikacyjną, która w szczególności obejmuje dane dotyczące użytkownika oraz dane transmisyjne, definiuje art. 159 prawa telekomunikacyjnego. Przepis art. 159 ust. 2 przewiduje silniejszą ochronę danych niż przepis art. 23 ust. 1 *Ustawy o ochronie danych osobowych* i dlatego to on znajduje zastosowanie jako podstawa legalizująca przetwarzanie danych objętych tajemnicą telekomunikacyjną[20].

Podczas prac prowadzonych od 2006 r. nad nowelizacją prawa telekomunikacyjnego w Polsce dochodziło do poważnej różnicy zdań. Niektórzy posłowie proponowali nawet 15-letni okres obowiązkowego przechowywania danych bilingowych. Rządy natomiast stały na stanowisku, że nie powinien on być krótszy niż 5 lat. Uchwalony ostatecznie przez sejm w 2009 r. przepis art. 180a *Prawa telekomunikacyjnego* nałożył na operatora publicznej sieci telekomunikacyjnej oraz dostawcę publicznie dostępnych usług telekomunikacyjnych obowiązek przechowywania danych przez maksymalny okres 2 lat. Wprowadzenie maksymalnego okresu dopuszczalnego przez dyrektywę argumentowano tym, że nasz kraj może być wykorzystywany jako zaplecze dla ugrupowań terrorystycznych. *Ratio legis* przepisu stanowi ułatwienie wykrywania przestępstw skierowanych przeciwko obronności i bezpieczeństwu państwa oraz jego porządkowi publicznemu.

Porównując przepisy prawa polskiego do zapisów zawartych w dyrektywie retencyjnej, można mieć wątpliwości co do ich pełnej zgodności. Nawet tak istotne normy, jak zawarte w art. 218 § 1 kpk, nie są tożsame z analogicznymi zapismi wyżej wymienionej dyrektywy, gdyż nie wprowadza ona wymogu zaistnienia poważnych przestępstw, analogicznie do tych, które zostały wprowadzone w artykule 237 § 2 kpk. Artykuł 237 kpk bowiem, regulujący kwestię kontroli procesowej, zawiera ograniczenie do enumeratywnie wyliczonych przestępstw. Brak takiego ograniczenia w art. 218 § 1 kpk może powodować wątpliwości co do jego zgodności z dyrektywą. Nie budzi natomiast wątpliwości przepis art. 218a kpk, stanowiący o „zabezpieczeniu danych", który jest uznawany za wyraz kompromisu pomiędzy interesem wymiaru sprawiedliwości a prawami obywatelskimi.

W konfrontacji ustawy o Policji z postanowieniami dyrektywy retencyjnej wątpliwości mogą dotyczyć braku wykazu poważnych przestępstw, analogicznego do tego, który zawarty jest w art. 19 ust. 1 tej ustawy. Zgodnie bowiem z art. 20c ust. 1 dane bilingowe mogą być ujawnione Policji wyłącznie w celu zapobieżenia przestępstwom lub wykrycia ich[21]. Podobna uwaga nasuwać się może przy analizie norm ustawy o Straży Granicznej oraz o Żandarmerii Wojskowej. Wątpliwości pojawiają się także w zakresie rozwiązań przyjętych w ustawie o Centralnym Biurze Antykorupcyjnym. Artykuł 18 tej ustawy, który upoważnia CBA do pozyskiwania danych bilingowych, odsyła do art. 2, zawierającego katalog poważnych przestępstw. W zakresie postępowań kontrolnych przepisy te mogą jednak budzić wątpliwości jeśli chodzi o zasadę proporcjonalności w świetle dyrektywy retencyjnej w sytuacji, gdy postępowanie kontrolne nie przechodzi do etapu postępowania przygotowawczego.

Z kolei analizując normę art. 28 ustawy o ABW oraz AW upoważniającą ABW do uzyskiwania danych bilingowych, należy stwierdzić, iż przepis wprowadza warunek,

[20] Por. wyrok NSA z dnia 26.01.2009 r., I OSK 174/08, LEX nr 478301.

[21] Dotyczy zatem także czynów nieumyślnych lub podejrzenia kradzieży na kwotę 251 zł; przy wykroczeniu na kwotę 249 zł zaś żądanie bilingów byłoby niezasadne.

że dane te muszą być niezbędne do rozpoznawania, zapobiegania i wykrywania poważnych przestępstw. Gdy skonfrontujemy przepis art. 5 tej ustawy z postanowieniami dyrektywy retencyjnej, to wątpliwości dotyczące zasady proporcjonalności nie wydają się uzasadnione. Podnoszony z kolei zarzut, że przepis art. 28 odsyła także do art. 5 ust. 1 pkt 1 odnoszącego się do rozpoznawania zagrożeń godzących w porządek konstytucyjny jest nieuprawniony w związku z tym, że rozpoznawanie tych zagrożeń polega na ustaleniu, czy nie są wypełnione znamiona przestępstw z rozdziału XVII kk (przestępstwa przeciwko RP). Podnoszony w mediach zarzut braku uprzedniej zgody sądu na udostępnienie danych bilingowych także nie wydaje się zasadny. Dyrektywa stanowi bowiem, że proces oraz warunki uzyskiwania dostępu do zatrzymanych danych, w przypadkach, gdy został spełniony wymóg konieczności oraz proporcjonalności, określone są w prawie krajowym każdego państwa członkowskiego. Należy podkreślić, iż dyrektywa nie wprowadza warunku uzyskania uprzedniej zgody sądu. W praktyce stosowania przepisu istnieją zabezpieczenia uniemożliwiające osobie nieuprawnionej dostęp do tych danych. W sytuacji zdobycia informacji spoza zakresu określonego w katalogu zawartym w art. 5 ustawy o ABW oraz AW mogłoby dojść do wypełnienia znamion czynu zabronionego z art. 231 kk. Przestępstwo to jest ścigane z oskarżenia publicznego. W przypadku postanowienia prokuratora o odmowie wszczęcia śledztwa, osobie pokrzywdzonej przysługuje zażalenie do sądu. Otwiera się zatem droga kontroli sądowej nie uprzedniej, ale następczej, co wydaje się być regulacją prawidłową.

Dyskusyjne byłoby w świetle dyrektywy korzystanie z bilingów dla celów postępowań sprawdzających przeprowadzanych na podstawie ustawy o ochronie informacji niejawnych. Tutaj jednak służby nie działają „z urzędu", a prowadzą postępowanie na wniosek zainteresowanego. W razie skargi osoby ubiegającej się o certyfikat bezpieczeństwa skierowanej do sądu, całość zebranych akt podlega kontroli sądowej, konkretnie wojewódzkiego sądu administracyjnego. Dlatego niesłuszny jest zarzut, że służby działają tu poza kontrolą zewnętrzną.

Nie ma w zakresie wykorzystania retencji danych orzeczeń Trybunału Konstytucyjnego ani Sądu Najwyższego. SN zajmował się kwestią bilingów jedynie w sprawie I KZP 45/02 w 2003 r., dotyczącej rozliczania kosztów połączeń.

Jak już wspomniano, w porządku prawnym UE, którego Polska jako jej członek zobowiązana jest przestrzegać, wszystkie państwa członkowskie winny implementować przyjęte dyrektywy do porządku krajowego, pod rygorem ewentualnego zaskarżenia do Europejskiego Trybunału Sprawiedliwości.

W związku z implementacją dyrektyw odnośnie do sieci i usług łączności elektronicznej, m.in. *Dyrektywy 2002/21/WE*, Polska była już zaskarżona przez Komisję Europejską do Europejskiego Trybunału Sprawiedliwości o uchybienie zobowiązaniom państwa członkowskiego co do określenia pojęcia a b o n e n t .

Wyrok Trybunału (piąta izba) z dnia 22 stycznia 2009 r. w sprawie C 492/07 brzmiał:

1) *Nie dokonując prawidłowo transpozycji dyrektywy 2002/21/WE Parlamentu Europejskiego i Rady z dnia 7 marca 2002 r. w sprawie wspólnych ram regulacyjnych sieci i usług łączności elektronicznej (dyrektywy ramowej, a w szczególności jej art. 2 lit. k) dotyczącej pojęcia „abonent", Rzeczpospolita Polska uchybiła zobowiązaniom, które na niej ciążą na mocy tej dyrektywy.*
2) *Rzeczpospolita Polska zostaje obciążona kosztami postępowania.*

Zatem Europejski Trybunał Sprawiedliwości orzekł, że Polska nie dokonała właściwie transpozycji do polskich przepisów definicji pojęcia a b o n e n t usług te-

lekomunikacyjnych. Polskie pojęcie abonent ograniczało się do osoby, która zawarła umowę pisemną. To pozbawiało abonentów, takich jak użytkownicy telefonów na kartę, wielu praw, w tym prawa do umieszczenia swoich danych w ogólnie dostępnej książce telefonicznej, prawa do otrzymywania rachunków zbiorczych oraz niektórych praw dotyczących wyświetlania identyfikacji rozmów przychodzących lub możliwości zablokowania automatycznego przekazywania połączeń. Komisja Europejska jako „strażnik traktatów" posiada uprawnienia do zapewniania przestrzegania prawa wspólnotowego przez państwa członkowskie[22].

Za brak implementacji dyrektywy retencyjnej do Europejskiego Trybunału Sprawiedliwości została zaskarżona również Szwecja. Należy przypomnieć, że Polska dotychczas nie dokonała na przykład pełnej transpozycji dyrektywy retencyjnej w zakresie danych internetowych.

VI

Zakończył się pierwszy etap prac nad ewaluacją stosowania dyrektywy retencyjnej na poziomie europejskim. Komisja Europejska nie stwierdziła niezgodności polskich regulacji z jej postanowieniami. Ustaliła natomiast, że zatrzymywane dane dotyczące połączeń odgrywają ważną rolę w ochronie społeczeństwa przed szkodami wynikającymi z poważnych przestępstw. Takie dane stanowią materiał dowodowy nie tylko do skazywania osób winnych popełnienia poważnych przestępstw i aktów terroryzmu, lecz także do oczyszczania z zarzutów osób niewinnych[23].

Dyskusja prowadzona w kraju, ale także i w Brukseli, może zaowocować rozwiązaniami bardziej harmonizującymi ze szczegółowymi rozwiązaniami dotyczącymi zasady bezpieczeństwa oraz ochrony praw obywatelskich. Komisarz ds. wewnętrznych UE podkreśliła, iż zatrzymywane dane odnośnie do połączeń dostarczają głównych dowodów niezbędnych do wykrywania sprawców przestępstw oraz wymierzania sprawiedliwości. Transpozycja dyrektywy nie przebiega jednak równomiernie, a różnice w implementacji będą pomocne w ocenie, na ile potrzebna będzie modyfikacja dyrektywy 2006/24/WE. Ewaluacji podlegają także dane statystyczne dotyczące wykorzystywania danych bilingowych. Podawana w mediach liczba ponad miliona bilingów rocznie, które w Polsce były wykorzystywane przez prokuraturę, sądy oraz służby policyjne w związku z przepisami o retencji danych, może być niemiarodajna, ponieważ obejmuje zapytania o abonentów, którzy nie zastrzegli numeru telefonicznego (czyli w zasadzie jest to przeglądanie książki telefonicznej oraz kilkakrotne zliczanie tych samych zapytań, kierowanych do różnych operatorów).

Zdaniem Komisji dyrektywa sama w sobie nie gwarantuje, że dane będą przechowywane, pozyskiwane i wykorzystywane w pełnej zgodności z prawem do ochrony danych osobowych. Doprowadza to do unieważnienia przepisów dotyczących jej transpozycji przez sądy w niektórych państwach członkowskich. Aby udoskonalić istniejące przepisy prawne, Komisja ma dokonać przeglądu obowiązujących zasad dotyczących zatrzymywania danych po skonsultowaniu się ze służbami policyjnymi i sądowniczy-

[22] Por. także: *Prawo Wspólnot Europejskich. Orzecznictwo*, W. Czapliński i in. (wyb. i red.), Warszawa 2005, Scholar, s. 40.

[23] Por. *Report From The Commission To The Council And The European Parlament, Evaluation report on the Data Retention Directive* (Directive 2006/24/EC), www.europa.ue.

mi, z przedstawicielami branży telekomunikacyjnej, organów ds. ochrony danych oraz społeczeństwa obywatelskiego[24].

Z kolei na szczeblu krajowym trwają prace tzw. roboczego zespołu bilingowego, powołanego przez premiera w ramach Kolegium do Spraw Służb Specjalnych, którego zadaniem jest wypracowanie stanowiska w sprawie zakresu zmian legislacyjnych odnośnie do pozyskiwania przez uprawnione organy informacji objętych tajemnicą telekomunikacyjną oraz przygotowanie propozycji tych zmian.

VII

W podsumowaniu należy stwierdzić, że niektóre przepisy implementujące przedmiotową dyrektywę wymagają doprecyzowania. Niewątpliwie niezgodne z nią jest uzyskiwanie od operatorów danych bilingowych dla celów spraw rozwodowych w trybie art. 248 § 1 kpc. Jednocześnie korzystanie z regulowanych dyrektywą retencyjną danych przez służby państwowe i wymiar sprawiedliwości stanowi ważny i skuteczny instrument ułatwiający zwalczanie poważnej przestępczości, w tym terroryzmu. Instrumentu tego nie należy jednak nadużywać.

Przykład Wielkiej Brytanii pokazuje, że na kilkaset tysięcy bilingów wykorzystanych przez policję i służby specjalne, skarg do specjalnego Trybunału (*Investigatory Powers Tribunal*) jest kilkanaście rocznie, a za słuszne uznawanych jest kilka. Retencję danych uzyskiwanych w wyniku komunikacji implementowano w Wielkiej Brytanii, traktując dyrektywę retencyjną jako istotną inicjatywę instytucji unijnych.

Artykuł 8 ust. 2 Europejskiej Konwencji Praw Człowieka umożliwia ingerencję w prawa jednostki do prywatności, jeśli jest to konieczne z punktu widzenia bezpieczeństwa narodowego oraz zapobiegania i wykrywania niektórych rodzajów przestępstw.

W Polsce natomiast na ponad milion spraw, w których wykorzystywano dane bilingowe, tylko kilka przypadków zostało nagłośnionych jako dopuszczenie się nadużyć.

Na zakończenie niniejszego artykułu nasuwa się wniosek, że nie należy eliminować tak skutecznego i niezbędnego narzędzia zwalczania przestępczości, jakim jest możliwość wykorzystywania bilingów, powołując się na pojawiające się jedynie sporadycznie nadużycia.

[24] Por. Oświadczenie Cecilii Malmström, Komisarza do spraw wewnętrznych UE z dnia 18 kwietnia 2011 r. www.europa.ue.

Streszczenie

Artykuł przedstawia analizę prawną oraz stanowisko autora w toczącej się aktualnie debacie dotyczącej wykorzystywania przez uprawnione podmioty (m.in. służby specjalne) tzw. danych retencyjnych, czyli gromadzonych przez operatorów lub dostawców usług telekomunikacyjnych, związanych z sieciowym ruchem ich usługobiorców. Stanowiąc próbę całościowego ujęcia tematu, artykuł przybliża znaczenie, tak potoczne, jak i normatywne, pojęcia r e t e n c j i d a n y c h, opisuje zagadnienia retencji na tle rozwiazań normatywnych Unii Europejskiej oraz krajowych, a także dokonuje zwięzłej oceny implementacji przepisów *Dyrektywy 2006/24/WE w sprawie zatrzymywania generowanych lub przetwarzanych danych* (...) do polskiego porządku prawnego. Dla poszerzenia perspektywy ocena ta podejmowana jest przez autora przy uwzględnieniu tak wymagń zapewnienia należytej ochrony praw obywateli, jak i ciążącego na państwach obowiązku skutecznego zwalczania przestępczości. W niniejszej publikacji wskazano na głosy krytyczne wobec rozwiązań prawnych przyjętych w zakresie retencji danych oraz przywołano pozytywne oceny, w tym także wyrażane na arenie międzynarodowej.

Abstract

The paper introduces legal analysis and author's opinion relating to the currently ongoing debate concerning the use of the so called data retention by competent national authorities (i.a. law enforcement agencies), that is data gathered by operators or providers of telecommunication services, concerning network traffic of their services users. Being an attempt to address the topic integrally, the paper brings closer the meaning, both colloquial and legal, of the term 'data retention', analyzes retention based on legal regulations stipulated in the European Union and national laws, and also presents a brief evaluation of implementation of Directive 2006/24/EC on the retention of data [...] into Polish law. To extend the perspective, this evaluation is done with having in mind both the requirements of ensuring the protection of civil rights as well as duty of national authorities to effectively fight crimes. In this thesis, is author points both to criticism on regulations concerning retention of data and to positive opinions, including those presented on international level.

Alfred Staszak

Prawne podstawy dopuszczalności żądania bilingów

W ostatnim okresie w mediach i w piśmiennictwie fachowym rozgorzała dyskusja na temat prawnej dopuszczalności pozyskiwania, a następnie przetwarzania i gromadzenia przez organy ścigania danych dotyczących połączeń telefonicznych, uzyskanych od operatorów usług telefonicznych[1]. Szczególną uwagę należy przy tej dyskusji zwrócić na pytania podnoszone przez przedstawicieli środków masowego przekazu dotyczące prawnej dopuszczalności pozyskiwania wykazów połączeń telefonów należących do dziennikarzy, w sytuacji gdy są oni „chronieni" przed takim żądaniem tajemnicą dziennikarską.

I. Wzorce Europejskiego Trybunału Praw Człowieka i norm konstytucyjnych

Punktem wyjścia wszelkich rozważań dotyczących prawnej dopuszczalności pozyskiwania, a następnie przetwarzania i gromadzenia przez organy ścigania uzyskanych od operatorów usług telefonicznych danych dotyczących połączeń telefonicznych, wśród których mogą znaleźć się wykazy połączeń należące do dziennikarzy, w demokratycznym państwie prawa musi być zawsze powszechnie akceptowany standard gwarancji praw człowieka i podstawowych swobód obywatelskich. W krajach europejskich takim punktem odniesienia jest *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* (dalej: *Konwencja*) oraz orzecznictwo Europejskiego Trybunału Praw Człowieka (dalej: ETPCz).

Artykuł 5 wyżej przytoczonej *Konwencji* stwierdza, że każdy ma prawo do wolności i bezpieczeństwa osobistego. Artykuł 8 natomiast odnosi się do konieczności poszanowania życia prywatnego i rodzinnego, mieszkania i korespondencji. Ten sam artykuł stanowi, że: *Niedopuszczalna jest ingerencja władzy publicznej w korzystanie z tego prawa, z wyjątkiem przypadków przewidzianych przez ustawę i koniecznych w demokratycznym społeczeństwie z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób*[2]. W ten sposób wyżej wymieniona *Konwencja* z jednej strony wskazuje podstawowe prawa obywatelskie, a z drugiej przewiduje możliwość – po spełnieniu określonych przesłanek – ingerencji organów władzy państwowej, a w tym i organów ścigania,

[1] Zob.: rs, amk/fac [podpis autora pod przytoczonym dalej artykułem – przyp. red.], *Oświadczenie przewodniczącego speckomisji. Kontrola dziennikarzy „zgodna z prawem", ale „niedopuszczalna"*, www.tvn24.pl/12690,1677636,0,1,kontrola-dziennikarzy-zgodna-z-prawem--ale-niedopuszczalna,wiadomosc.html [dostęp: 18.05.2011]; W. Czuchnowski, *Wpadka speckomisji*, „Gazeta Wyborcza" z 14.10.2010; D. Barski, *Tajemnica dziennikarska nie chroni bilingów*, „Rzeczpospolita" z 15.10.2010; J. Kondracki, K. Stępiński, *Bilingi pod osłoną tajemnicy dziennikarskiej*, „Rzeczpospolita" z 11.10.2010; es [podpis autora pod przytoczonym dalej artykułem – przyp. red.], *Jak śledzić podsłuchy*, http://wyborcza.pl/1,75478,8758667,Jak_sledzic_podsluchy.html.

[2] *Konwencja o Ochronie Praw Człowieka i Podstawowych Wolności* sporządzona w Rzymie dnia 4 listopada 1950 r., Dz.U. z 1993 r., Nr 61, poz. 284.

w te prawa. Uznaje także, że istnieje możliwość interwencji państwa, jeżeli tylko organy władzy będą działały:
– na podstawie ustaw i w ich granicach,
– w sytuacjach koniecznych *z uwagi na bezpieczeństwo państwowe, bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób.*

Konwencja zawiera także normę, choć nie wyrażoną wprost, odnoszącą się do działalności dziennikarskiej poprzez zagwarantowanie obywatelom prawa do wolności wyrażania opinii, która obejmuje *wolność posiadania poglądów oraz otrzymywania i przekazywania informacji i idei*[3].

Podobne uregulowania znajdujemy w *Konstytucji Rzeczypospolitej Polskiej z 2 kwietnia 1997 roku* (dalej: *Konstytucja*). Art. 49 tej ustawy zasadniczej gwarantuje *wolność i ochronę tajemnicy komunikowania się*, jednak następne zdanie tego artykułu stwierdza, że ograniczenie tych praw jest możliwe *w przypadkach określonych w ustawie i w sposób w niej określony*. Podobnie art. 31 zawiera zapis, że: *Ograniczenia w zakresie korzystania z konstytucyjnych wolności i praw mogą być ustanawiane tylko w ustawie i tylko wtedy, gdy są konieczne w demokratycznym państwie dla jego bezpieczeństwa lub porządku publicznego, bądź dla ochrony środowiska, zdrowia i moralności publicznej, albo wolności i praw innych osób.*

Stwierdzić zatem należy, że zarówno *Konwencja*, jak i *Konstytucja*, wyraźnie wskazują na to, że wolność komunikowania się i swobodnego przepływu informacji należy do fundamentalnych praw obywatelskich w państwach demokratycznych. Prawa te podlegają ochronie przewidzianej dla tajemnicy komunikowania się, a ingerencja organów władzy państwowej w to prawo jest możliwa jedynie wtedy, gdy te organy będą działały w granicach ustawowego umocowania i w sytuacjach koniecznych dla zapewnienia bezpieczeństwa lub porządku publicznego.

II. Zakres pojęć: kontrola korespondencji, kontrola operacyjna i wykaz połączeń

Aktualnie obowiązujące przepisy rozróżniają takie pojęcia jak: korespondencja i przesyłka, kontrola i utrwalanie treści rozmów telefonicznych, kontrola operacyjna, wykaz połączeń. Z każdym z tych pojęć związana jest różna regulacja prawna dotyczącą możliwości zapoznania się przez organy władzy państwowej z treścią informacji przekazywanej w jeden ze wskazanych sposobów komunikowania się. Tylko część tej regulacji zawarta jest w *Kodeksie postępowania karnego*, zdecydowana większość zaś – w przepisach innych ustaw.

Zawartość semantyczna pojęcia korespondencja i przesyłka wynika z definicji legalnej zawartej w *Prawie pocztowym*, zgodnie z którą przesyłka to *rzeczy opatrzone adresem, przedłożone do przyjęcia lub przyjęte przez operatora w celu przemieszczenia i doręczenia adresatowi*[4].

Pojęcie kontroli i utrwalania treści rozmów telefonicznych jest tożsame, w myśl art. 237 kpk, z pojęciem podsłuch, które w tym przypadku

[3] Art. 10 *Konwencji*.
[4] *Ustawa z dnia 12 czerwca 2003 r. Prawo pocztowe* (Dz.U. z 2003 r., Nr 130, poz. 1188 z późn. zm.).

jest pojęciem procesowym. Przepis tego artykułu nie może, i faktycznie nie stanowi, prawnej podstawy do stosowania podsłuchu pozaprocesowego[5]. Procesowa kontrola oraz utrwalanie przy użyciu środków technicznych treści innych rozmów lub przekazów informacji, w tym korespondencji przesyłanej pocztą elektroniczną, uregulowana została w art. 241 kpk. Warto przy tym zauważyć, że Sąd Najwyższy w uchwale z 21 marca 2001 r. uznał, że określenie t r e ś c i p r z e k a z ó w i n n y c h n i ż r o z m o w y t e l e f o n i c z n e oznacza *nie mające charakteru rozmowy telefonicznej przesyłanie informacji za pośrednictwem sieci telekomunikacyjnej, tj. przez przewody, systemy radiowe, optyczne lub jakiekolwiek inne urządzenia wykorzystujące energię elektromagnetyczną*[6].

Kontrola operacyjna, rozumiana także jako podsłuchiwanie treści rozmów i przekazów utrwalanych na odpowiednich nośnikach, została unormowana – zgodnie z wymogami konstytucyjnymi – w ustawach regulujących funkcjonowanie odpowiedniej służby stosującej ten sposób pozyskiwania informacji. W poszczególnych ustawach wskazane zostały prawne przesłanki dopuszczalności stosowania podsłuchu, przy czym zawsze muszą się one mieścić w zakresie kompetencyjnym danej służby, a nadto spełniać zasadę subsydiarności wyrażającą się w stwierdzeniu, że inne formy pracy operacyjnej są lub mogą być bezskuteczne.

Każda ze służb uprawnionych do stosowania podsłuchów (tj. Policja, Straż Graniczna, Agencja Bezpieczeństwa Wewnętrznego, Centralne Biuro Antykorupcyjne, Kontrola Skarbowa, Służba Kontrwywiadu Wojskowego, Żandarmeria Wojskowa) ma inny katalog przestępstw, w których ściganiu dopuszczalne jest stosowanie kontroli operacyjnej[7].

Wspólną dla wszystkich służb stosujących podsłuch formą pracy operacyjnej jest, podobnie jak w przypadku podsłuchu procesowego, sądowa kontrola podejmowanych działań, która wyraża się w wydaniu stosownego postanowienia przez sąd okręgowy, po uprzednim uzyskaniu zgody właściwego prokuratora[8].

---

[5] Zob. Komentarz do art. 237 kpk (Dz.U. z 1997 r., Nr 89, poz. 555), w: J. Grajewski, L. K. Paprzycki, S. Steinborn, *Kodeks postępowania karnego. Komentarz*, tom I (art. 1 - 424), LEX 2010, wyd. II.

[6] Uchwała SN z 21 marca 2001 r. o sygn. I KZP 60/99, OSNKW 2000, nr 3 - 4, poz. 26.

[7] Obecnie dochodzi do sytuacji wręcz paradoksalnych w tym zakresie. Przykładowo można wskazać postanowienie Sądu Apelacyjnego w Warszawie z 18.05.2007 r., II AKz 288/07, które dotyczy korzystania w postępowaniu karnym z dowodów zebranych przez CBA podczas stosowania kontroli operacyjnej. Służba ta ujawniła okoliczności popełnienia zbrodni zabójstwa, którego to przestępstwa nie ma w katalogu przestępstw ściganych przez tę służbę. Sąd Apelacyjny w orzeczeniu stwierdził wprost: *Uzyskane w trybie niejawnym przez CBA materiały nie mogą stanowić dowodu w sprawie o zabójstwo. Ustawa o CBA wprowadza prawo korzystania z dowodów uzyskanych przez Centralne Biuro Antykorupcyjne w trybie art. 17 ust. 1 ustawy w sprawach wskazanych w zamkniętym katalogu przestępstw wymienionych w art. 17 ust. 1 pkt pkt 1 i 2 tej ustawy. Przepisy te nie wymieniają zbrodni zabójstwa, ani nieumyślnego spowodowania śmierci. Sprawia to, że uzyskane w tym trybie dowody nie mogą być podstawą ustaleń, jako zgromadzone w sposób sprzeczny z prawem, a tym samym nielegalne.*

[8] Na temat prawnych podstaw dopuszczalności stosowania kontroli operacyjnej szerzej zobacz m.in. w: L. Paprzycki, Z. Rau (red.), *Praktyczne elementy zwalczania przestępczości zorganizowanej i terroryzmu,* A. Biernaczyk*, Zarys problematyki czynności operacyjnych realizowanych w trybie art. 19, 19a i 19b ustawy z dnia 6 kwietnia 1990 r. o Policji;* J. Kudła*, Wybrana problematyka czynności operacyjnych na tle uwag de lege ferenda projektu ustawy o czynnościach operacyjno-rozpoznawczych,* K. Olejnik*, Zakres stosowania czynności operacyjnych (...);* A. Taracha*, Czynności operacyjno-rozpoznawcze – aspekty kryminalistyczne i prawno-porównawcze,* czy inne publikacje, szczególnie Jacka Kudły.

Ani w *Kodeksie postępowania karnego*, ani w ustawach regulujących funkcjonowanie służb uprawnionych do prowadzenia pracy operacyjnej nie ma zdefiniowanego pojęcia bilingu, które potocznie rozumiane jest jako wykaz połączeń. Legalnej definicji tego terminu nie można również znaleźć w *Prawie telekomunikacyjnym*[9].

W próbie zdefiniowania terminu b i l i n g pomocny może być jedynie tzw. słowniczek zawarty w art. 2 *Prawa telekomunikacyjnego*. Artykuł ten definiuje m.in. dwa interesujące z tego punktu widzenia podobne pojęcia, tj. p o ł ą c z e n i e i p o ł ą c z e n i e t e l e f o n i c z n e. Pierwszy z tych terminów (połączenie) definiowane jest jako: *fizyczne lub logiczne połączenie telekomunikacyjnych urządzeń końcowych pozwalające na przesłanie przekazów telekomunikacyjnych*, drugie zaś (połączenie telefoniczne) jako *połączenie ustanowione za pomocą publicznie dostępnej usługi telefonicznej, pozwalające na dwukierunkową łączność w czasie rzeczywistym*.

Ważna z tego punktu widzenia jest także treść art. 80 wyżej wymienionej ustawy, gdyż zgodnie z ust. 1 tego artykułu: *Dostawca publicznie dostępnych usług telekomunikacyjnych dostarcza abonentowi nieodpłatnie z każdą fakturą podstawowy wykaz wykonanych usług telekomunikacyjnych zawierający informację o zrealizowanych płatnych połączeniach z podaniem, dla każdego typu połączeń, liczby jednostek rozliczeniowych odpowiadającej wartości zrealizowanych przez abonenta połączeń*.

Z cytowanych przepisów wynika zatem, że pojęcie b i l i n g musi być rozumiane jako wykaz wykonanych połączeń telefonicznych. Na operatorów sieci telefonicznych został przez ustawodawcę nałożony szereg obowiązków istotnych z punktu widzenia obronności i szeroko rozumianego bezpieczeństwa państwa. Obowiązki te wynikają wprost z treści ustawowych przepisów. W tym miejscu można jedynie zaznaczyć, że operator został zobowiązany przez *Prawo telekomunikacyjne* (na własny koszt) między innymi do:

– niezwłocznego blokowania na żądanie uprawnionych podmiotów połączeń telekomunikacyjnych lub przekazów informacji, jeżeli połączenia te mogą zagrażać obronności, bezpieczeństwu państwa oraz bezpieczeństwu i porządkowi publicznemu,
– przechowywania przez okres 24 miesięcy danych generowanych w sieci telekomunikacyjnej lub przez nich przetwarzanych, licząc od dnia połączenia lub nieudanej próby połączenia,
– udostępniania danych uprawnionym podmiotom, a także sądowi i prokuratorowi, na zasadach i w trybie określonym w odrębnych przepisach.

Zgodnie z ustawą obowiązkiem gromadzenia i przechowywania objęte są dane niezbędne do:

1) ustalenia zakończenia sieci, telekomunikacyjnego urządzenia końcowego i użytkownika końcowego:
   a) inicjującego połączenie,
   b) do którego kierowane jest połączenie;
2) określenia:
   a) daty i godziny połączenia oraz czasu jego trwania,
   b) rodzaju połączenia,
   c) lokalizacji telekomunikacyjnego urządzenia końcowego.

Korzystając z przyznanej w art. 180c ust. 2 ustawy *Prawo telekomunikacyjne* delegacji ustawowej, minister infrastruktury wydał *Rozporządzenie z dnia 28 grudnia 2009 r. w sprawie szczegółowego wykazu danych oraz rodzajów operatorów publicznej*

[9] *Ustawa z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne*, Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.

sieci telekomunikacyjnej lub dostawców publicznie dostępnych usług telekomunikacyjnych obowiązanych do ich zatrzymywania i przechowywania[10]. W rozporządzeniu tym przyjęto między innymi[11], że danymi niezbędnymi do ustalenia w ruchomej publicznej sieci telekomunikacyjnej, a więc w sieciach telefonii komórkowej, są dane dotyczące:

– numeru MSISDN użytkownika końcowego, inicjującego połączenie i do którego połączenie jest kierowane,
– imienia i nazwiska albo nazwy oraz adresu użytkowników końcowych,
– numerów IMSI użytkowników końcowych,
– pierwszych 14 cyfr numeru IMEI albo numeru ESN telekomunikacyjnego urządzenia końcowego,
– daty i godziny pierwszego zalogowania telekomunikacyjnego urządzenia końcowego do ruchomej publicznej sieci telefonicznej, zgodnie z czasem lokalnym, oraz współrzędnych geograficznych lokalizacji stacji BTS,
– daty i godziny połączenia (lub jego próby) oraz czasu jego trwania z dokładnością do 1 sekundy,
– lokalizacji telekomunikacyjnego urządzenia końcowego poprzez identyfikator anteny stacji BTS.

W przypadku stacji bazowych dane identyfikujące anteny stacji BTS obejmować muszą, zgodnie z tym rozporządzeniem, nie tylko współrzędne geograficzne tej stacji, ale także azymut, wiązkę i zasięg roboczy tego typu anteny. W konsekwencji dane te pozwalają na bardzo dużą dokładność ustalenia miejsca pobytu użytkownika telefonu komórkowego zarówno wykonującego, jak i odbierającego połączenie telefoniczne.

Wynikające z omawianych przepisów obowiązki wskazane zostały również w postanowieniu Sądu Najwyższego z dnia 25 marca 2010 r., w sprawie o sygn. I KZP 37/09. W postanowieniu tym Sąd stwierdził, że: *Przepis art. 180a ust. 1 pkt 2 ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r., Nr 171, poz. 1800 ze zm.) nakłada na operatorów publicznej sieci telekomunikacyjnej oraz dostawców ogólnie dostępnych usług telekomunikacyjnych obowiązek udostępniania, to jest wyszukiwania, tworzenia stosownych zestawień i przesyłania za pomocą sieci telekomunikacyjnej uprawnionym podmiotom, w tym sądowi i prokuratorowi danych, o których mowa w art. 180c ust. 1 ustawy. Tak rozumiane koszty udostępniania tych danych obciążają operatora lub dostawcę* (…)[12].

W świetle obowiązującej i przedstawionej regulacji prawnej, a w szczególności jednoznacznej treści znowelizowanego art. 218 kpk, nie jest konieczne uzyskanie postanowienia sądu na otrzymanie od operatora na potrzeby toczącego się postępowania przygotowawczego wykazu połączeń telefonicznych, czyli tzw. bilingu. W myśl tego przepisu bowiem: *Urzędy, instytucje i podmioty prowadzące działalność w dziedzinie poczty lub działalność telekomunikacyjną, urzędy celne oraz instytucje i przedsiębiorstwa transportowe obowiązane są wydać sądowi lub prokuratorowi, na żądanie zawarte w postanowieniu, korespondencję i przesyłki oraz dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.)*, jeżeli mają znaczenie dla toczącego się postępowania. Tylko sąd lub prokurator mają prawo je otwierać lub zarządzić ich otwarcie.* Warun-

[10] Dz.U. z 2009 r., Nr 226, poz. 1828.
[11] Zob. załącznik nr 2 do przedmiotowego rozporządzenia.
[12] Zob. System Informacji Prawnej Lex - 564521.

kiem koniecznym otrzymania tych danych jest zatem jedynie wydanie postanowienia przez prokuratora na etapie postępowania przygotowawczego, a przez sąd na etapie postępowania sądowego.

III. Dopuszczalność uzyskiwania, analizowania i gromadzenia wykazu połączeń dla potrzeb pracy operacyjnej

Nadal otwarta pozostaje jednak kwestia, czy dopuszczalne jest uzyskiwanie, analizowanie i gromadzenie bilingów w ramach pracy operacyjnej wykonywanej przez uprawnione do tego służby. Jako punkt wyjścia do dalszych rozważań należy przyjąć, że każdy z uprawnionych podmiotów prowadzących tego typu pracę będzie działał w ramach swoich zadań i ustawowych kompetencji.

1. Ustawa o Policji

Kwestia uzyskiwania bilingów na potrzeby Policji została uregulowana z dniem 6 lipca 2009 r. w art. 20c *Ustawy o Policji* w brzemieniu, co jest ważne, nadanym mu ustawą z dnia 24 kwietnia 2009 r. *o zmianie ustawy – Prawo telekomunikacyjne oraz niektórych innych ustaw* (Dz.U. z 2009 r., Nr 85, poz. 716). Przepis ten wskazuje, że: *W celu zapobiegania lub wykrywania przestępstw Policja może mieć udostępniane dane, o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.), zwane dalej „danymi telekomunikacyjnymi", oraz może je przetwarzać*[13].

Udostępnienie żądanych przez policję danych telekomunikacyjnych następuje nieodpłatnie. Przekazuje się je policjantowi wskazanemu w pisemnym wniosku skierowanym do operatora przez Komendanta Głównego Policji lub komendanta wojewódzkiego Policji albo osobie przez nich upoważnionej.

Przepis ten bardzo ogólnie wskazuje, że udostępnienie bilingów może nastąpić jedynie w celu zapobieżenia lub wykrycia przestępstw, ale już w żaden sposób ich nie wartościuje (nie kataloguje, jak w przypadku kontroli operacyjnej). Możliwe jest zatem żądanie bilingu zarówno w sprawie dotyczącej zabójstwa, jak i kradzieży lub przywłaszczenia mienia ruchomego o wartości nie większej niż 250 złotych. Policja nie ma jedynie możliwości występowania z tego typu żądaniem w sprawach o wykroczenia.

Ważne jest przy tym, że materiały uzyskane od operatora w postaci bilingów i ich analiza (jako forma ich przetworzenia), w sytuacji gdy zawierają informacje mające znaczenie dla postępowania karnego, przekazywane są właściwemu miejscowo i rzeczowo prokuratorowi do prowadzonego postępowania karnego. Nie ma zatem potrzeby ponownego zwracania się o nie w trybie art. 218 § 1 kpk, co jednak w praktyce bardzo często się zdarza.

Ustawa reguluje również sytuację, gdy uzyskane w ten sposób materiały nie zawierają informacji mających znaczenie dla postępowania karnego. Podlegają one wówczas niezwłocznemu zniszczeniu komisyjnemu i protokolarnemu, przy czym w ustawie brak definicji tego terminu i określenia, jak należy go rozumieć. Nie można nawet w sposób wiążący w tym przypadku powołać się, stosując analogię, na dwumiesięczny termin z art. 19 ust. 17, to jest na sytuację, gdy w wyniku stosowania kontroli operacyjnej nie uzyskano materiału pozwalającego na wszczęcie postępowa-

[13] *Ustawa z dnia 6 kwietnia 1990 r. o Policji*; tekst jednolity – Dz.U. z 2007 r., Nr 43, poz. 277 z późn. zm.

nia karnego, gdyż termin tam określony, jak i cały ten przepis, odnosi się jedynie do tej kontroli[14].

2. Ustawy o: Straży Granicznej, Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Centralnym Biurze Antykorupcyjnym i Kontroli Skarbowej

Regulacja prawna, bardzo podobna do tej obowiązującej w przypadku Policji, została nadana nowelizacją *Prawa telekomunikacyjnego* z 2009 r. ustawie o Straży Granicznej, o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu i o Kontroli Skarbowej[15]. Rozwiązanie przyjęte w ustawie powołującej w 2006 r. Centralne Biuro Antykorupcyjne przeniesione zostało w 2009 r. do *Ustawy o ABW oraz AW.*

Pozyskiwanie bilingów, danych BTS, danych personalnych użytkowników inicjujących połączenie i je odbierających zostało uregulowane w:
- art. 10b *Ustawy z dnia 12 października 1990 r. o Straży Granicznej* (tekst jednolity Dz.U.05.234.1997 z późn. zm.),
- art. 28. *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (tekst jednolity Dz.U.10.29.154),
- art. 18 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* (Dz.U.06.104.708 z późn. zm.),
- art. 36b *Ustawy z dnia 28 września 1991 r. o kontroli skarbowej* (tekst jednolity Dz.U.04.8.65 z późn. zm.).

Tożsama regulacja dotycząca uzyskiwania danych od operatora telefonicznego zawarta w Ustawie o Policji, o Straży Granicznej i o Kontroli Skarbowej nieznacznie różni się od regulacji zawartej w ustawach o ABW oraz AW i o CBA. W obu ostatnich ustawach bowiem w sposób nie budzący żadnych wątpliwości wskazano, że: *Obowiązek uzyskania zgody sądu*, o której mowa w art. 27 ust. 1 *Ustawy o ABW oraz AW* i w art. 17 *Ustawy o CBA* (to jest koniecznej dla kontroli operacyjnej), *nie dotyczy informacji niezbędnych do realizacji ich zadań (...) w postaci danych:*
1) *o których mowa w art. 180c i 180d ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne (Dz.U. z 2004 r., Nr 171, poz. 1800 z późn. zm.),*
2) *identyfikujących podmiot korzystający z usług pocztowych oraz dotyczących faktu, okoliczności świadczenia usług pocztowych lub korzystania z tych usług.*

IV. Tajemnice prawnie chronione

M. i R. Taradejna w książce pt. *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego*[16] wskazują na istnienie w polskim systemie ponad 120 różnego rodzaju prawnie (ustawowo) uregulowanych tajemnic. Ich waga dla bezpieczeństwa państwa zależy oczywiście nie od zakresu i obszerności ustawowego uregulowania, ale od tre-

[14] Nie oznacza to oczywiście, że termin dwóch miesięcy nie może być jakimś odnośnikiem realizacji ustawowego obowiązku *niezwłocznego zniszczenia*, które jednak powinno nastąpić wcześniej.

[15] W analizie celowo pominięto *Ustawę z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych*, a także *Ustawę z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego*, gdyż regulacja jest podobna, a praktycznie niespotykana w powszechnych jednostkach prokuratury.

[16] M. i R. Taradejna, *Dostęp do informacji publicznej, a prawna ochrona informacji dotyczących działalności gospodarczej, społecznej i zawodowej oraz życia prywatnego,* Toruń 2003, Adam Marszałek.

ści informacji niejawnych objętych tą tajemnicą. Przykładowo, jako mające największe znaczenie dla pracy operacyjnej organów ścigania, a jednocześnie uregulowane np. w *Ustawie o Policji* (a więc w ustawie regulującej funkcjonowanie tej służby) traktowane są dane objęte tajemnicą pocztową, ubezpieczeniową i bankową. Tajemnica pocztowa uregulowana jest w art. 39 ustawy z dnia 12 czerwca 2003 r. – *Prawo pocztowe* (Dz.U. z 2003 r., Nr 130, poz. 1188 z późn. zm.). Obejmuje ona *informacje przekazywane w przesyłkach, informacje dotyczące realizacji przekazów pocztowych, dane dotyczące podmiotów korzystających z usług pocztowych oraz dane dotyczące faktu i okoliczności świadczenia usług pocztowych lub korzystania z tych usług*[17]. Do zachowania tajemnicy pocztowej zobowiązany jest nie tylko operator pocztowy, czyli podmiot prowadzący działalność gospodarczą polegającą na dostarczaniu przesyłek, ale także każda inna osoba, która z racji wykonywanej działalności uzyskała dostęp do tajemnicy pocztowej.

Ustawa wskazuje także na sytuacje stanowiące naruszenie obowiązku zachowania tajemnicy pocztowej, wymieniając w szczególności jako jej przykłady: ujawnianie lub przetwarzanie informacji albo danych objętych tajemnicą pocztową i otwieranie zamkniętych przesyłek lub zapoznawanie się z ich treścią czy umożliwianie osobom nieuprawnionym działań mających na celu wykonywanie którejkolwiek z tych czynności[18].

Ustawa o Policji w art. 20d reguluje sytuacje legalnego dostępu do danych objętych tajemnicą pocztową. Wskazuje ona, podobnie jak w przypadku danych telekomunikacyjnych, że informacje dotyczące osób korzystających z usług pocztowych oraz dotyczące faktu i okoliczności świadczenia lub korzystania z tych usług mogą być ujawnione Policji i przez nią przetwarzane wyłącznie w celu zapobiegania lub wykrywania przestępstw oraz ich sprawców. Także i w tym przypadku ujawnienie tych danych na potrzeby operacyjne odbywa się na pisemny wniosek skierowany do operatora usług pocztowych przez Komendanta Głównego Policji lub Komendanta Wojewódzkiego lub na żądanie policjanta posiadającego pisemne upoważnienie tych osób.

Policja, a także inne służby, posiadają uprawnienia do niejawnego (ale legalnego) pozyskiwania określonych danych chronionych tajemnicą ubezpieczeniową i bankową, oczywiście po spełnieniu wszystkich ustawowych przesłanek takiej dopuszczalności[19].

Regulacja prawna dotycząca pozyskiwania na potrzeby pracy operacyjnej przez policję (podobnie jak i przez CBA i Straż Graniczną) danych objętych tajemnicą ubezpieczeniową i bankową jest szczególnie ważna z punktu widzenia potrzeby pozyskiwania ewentualnej zgody sądu, gdyż wprost do tej zgody się odnosi[20].

Omawiana ustawa wyraźnie wskazuje, że: *Jeżeli jest to konieczne dla skutecznego zapobieżenia przestępstwom określonym w art. 19 ust. 1 lub ich wykrycia albo ustalenia sprawców i uzyskania dowodów, Policja może korzystać z informacji dotyczących*

[17] Art. 39 ust. 1 *Ustawy z dnia 12 czerwca 2003 r. – Prawo pocztowe* (Dz.U. z 2003 r., Nr 130, poz. 1188 z późn. zm.).

[18] Tamże, ust. 2.

[19] Przesłanki dopuszczalności pozyskiwania informacji objętych tajemnicą ubezpieczeniową i bankową zawarte zostały także w:
– art. 10c *Ustawy o Straży Granicznej*,
– art. 23 *Ustawy o Centralnym Biurze Antykorupcyjnym*.

[20] Szerzej zob.: J. Kudła, A. Staszak, *Praktyczne aspekty tajemnicy bankowej. Przetwarzanie i wykorzystanie informacji zgromadzonych na etapie czynności operacyjno-rozpoznawczych,* w: „Policja" 2010, nr 1 lub strona internetowa Prokuratury Okręgowej w Zielonej Górze: *http://www.zielona-gora.po.gov.pl/esi-admin/upload/lektury_elektroniczne/2-praktyczne-aspekty-tajemnicy-bankowej.pdf.*

umów ubezpieczenia, a w szczególności z przetwarzanych przez zakłady ubezpieczeń danych podmiotów, w tym osób, które zawarły umowę ubezpieczenia, a także przetwarzanych przez banki informacji stanowiących tajemnicę bankową[21].

Informacje te na podstawie postanowienia wydanego na pisemny wniosek Komendanta Głównego Policji albo Komendanta Wojewódzkiego Policji udostępnia sąd okręgowy właściwy miejscowo ze względu na siedzibę organu wnioskującego. Po rozpatrzeniu wniosku sąd, w drodze postanowienia, wyraża zgodę na przekazanie informacji i danych wskazanego podmiotu, określając ich rodzaj i zakres oraz podmiot (konkretnego ubezpieczyciela lub bank) zobowiązany do ich udostępnienia.

Charakter gwarancyjny w zakresie przestrzegania praw i wolności obywatelskich ma przepis art. 20 ust. 10 *Ustawy o Policji*, zgodnie z którym w terminie do 90 dni od dnia przekazania danych objętych tajemnicą ubezpieczeniową i bankową podmiot, którego te dane dotyczyły – a więc konkretny człowiek lub konkretny podmiot gospodarczy – jest informowany przez policję o treści postanowienia sądu, wyrażającego zgodę na udostępnienie tych danych.

Pozornie trudniejsza sytuacja prawna może dotyczyć tajemnic wskazanych w art. 180 kpk, który odnosi się do osób zobowiązanych do zachowania tajemnicy notarialnej, adwokackiej, radcy prawnego, doradcy podatkowego, lekarskiej lub dziennikarskiej. Takie osoby mogą być przesłuchiwane co do faktów objętych tą tajemnicą tylko wtedy, gdy jest to niezbędne dla dobra wymiaru sprawiedliwości, a okoliczność (na jaką mają być przesłuchane te osoby) nie może być ustalona na podstawie innego dowodu. Wówczas w trakcie postępowania przygotowawczego konieczna jest decyzja sądu zezwalająca na przesłuchanie i określająca jego przedmiot. Warunkiem procesowego zwolnienia tych osób z tajemnicy jest konieczność przeprowadzenia tego przesłuchania dla dobra wymiaru sprawiedliwości i to pod warunkiem wyczerpania wszelkich innych środków dowodowych odnoszących się do okoliczności mających być ujawnionymi w trakcie przesłuchania[22].

W przypadku tajemnicy dziennikarskiej *zwolnienie dziennikarza od obowiązku zachowania tajemnicy nie może dotyczyć danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie powyższych danych*[23].

Pojęcie t a j e m n i c y d z i e n n i k a r s k i e j zostało jednak sformułowane nie w przepisach kpk, ale w *Ustawie z dnia 26 stycznia 1984 r. – Prawo prasowe*[24], a dokładnie w art. 15 tej ustawy. Tajemnica ta dotyczy danych umożliwiających identyfikację:

1. Autora materiału prasowego,
2. Listu do redakcji lub innego materiału o tym charakterze,
3. Innych osób udzielających informacji opublikowanych albo przekazanych do opublikowania,

---

[21] Art. 20c ust. 3 *Ustawy o Policji.*

[22] J. Grajewski, L. Paprzycki, S. Steinborn, *Komentarz do art.180 kodeksu postępowania karnego* (Dz.U. z 1997 r., Nr 89, poz. 555), w: J. Grajewski, L. K. Paprzycki, S. Steinborn, *Kodeks postępowania karnego. Komentarz,* tom I (art. 1 - 424), wyd. II, LEX 2010.

[23] Art. 180 § 3 kpk.

[24] Dz.U. z 1984 r., Nr 5, poz. 24 z późn. zm.

4. Wszelkich informacji, których ujawnienie mogłoby naruszać chronione prawem interesy osób trzecich.

Anonimizacja autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, a także osób udzielających informacji opublikowanych albo przekazanych do opublikowania może nastąpić tylko wtedy, gdy osoby te zastrzegły nieujawnianie powyższych danych. Jest to zatem warunek sine qua non objęcia danych personalnych tych osób ochroną.

Obowiązek przestrzegania tajemnicy dziennikarskiej dotyczy wszystkich osób zatrudnionych w redakcjach, wydawnictwach prasowych i innych prasowych jednostkach organizacyjnych, które z racji wykonywanej pracy zapoznały się z treścią podlegających tej ochronie danych[25]. Punktem wyjścia do określenia zakresu tajemnicy dziennikarskiej jest jednak treść art. 15 *Prawa prasowego* w kontekście art. 7 tejże ustawy. Wymaga to szczególnego podkreślenia, gdyż art. 15 stwierdza, że dziennikarzowi przysługuje prawo zobowiązujące do zachowania tajemnicy dziennikarskiej tylko jako *autorowi materiału prasowego*, a nie w związku z wykonywanym zawodem. W art. 7 zaś zawarta jest definicja legalna materiału prasowego. Przepis ten stwierdza, że: *Materiałem prasowym jest każdy opublikowany lub przekazany do opublikowania w prasie tekst albo obraz o charakterze informacyjnym, publicystycznym, dokumentalnym lub innym, niezależnie od środków przekazu, rodzaju, formy, przeznaczenia czy autorstwa*[26].

W konsekwencji można powiedzieć, że art. 7 *Prawa prasowego* w sposób istotny zawęża przedmiot i zakres tajemnicy dziennikarskiej. Obecnie jednak próbuje się nadać tej tajemnicy bardziej pojemny charakter, szczególnie w środowiskach reprezentujących dziennikarzy, a więc żywotnie zainteresowanych maksymalnym rozszerzeniem jej stosowania. Warto jednak zwrócić uwagę na to, że definiowanie pojęcia t a j e m n i c a d z i e n n i k a r s k a jedynie przez pryzmat art. 15, w oderwaniu od kontekstu innych przepisów (choćby tylko tej jednej ustawy) powoduje, że mamy do czynienia z zakresem wręcz wykraczającym poza dopuszczalne ramy prawne. O znaczeniu praktycznym tego zawężonego zakresu pojęcia t a j e m n i c y d z i e n n i k a r s k i e j może świadczyć to, że również dziennikarze dopuszczają się popełniania przestępstw, nawet bardzo poważnych. Ograniczenie możliwości dowodowych w zakresie analizy bilingów z tego powodu, że sprawcą poważnego przestępstwa jest dziennikarz, prowadzi do wypaczenia powagi wymiaru sprawiedliwości, czyniąc określoną grupę zawodową niemal bezkarną.

Prawo prasowe nie zawiera norm pozwalających na uchylenie tajemnicy dziennikarskiej. Zawiera je natomiast przepis art. 180 § 3 kpk, który *stanowi lex specialis w stosunku do art. 15 ust. 2 ustawy z 26 stycznia 1984 r. - Prawo prasowe, Dz. U. Nr 5, poz. 24 z późn. zm. (SN I KZP 15/94, OSNKW 1995, nr 1 - 2, poz. 1* [27] i daje częściowo taką możliwość.

W uzasadnieniu tego orzeczenia SN wskazał, iż *generalny charakter regulacji zawartej w art. 15 prawa prasowego. wynika z ustanowienia w nim zarówno przedmiotu, jak i zakresu tajemnicy zawodowej obejmującej wszystkich dziennikarzy.* (...) *Natomiast*

[25] Zob. E. Ferenc-Szydełko, *Komentarz do art. 15 ustawy z dnia 26 stycznia 1984 r. Prawo prasowe*, (Dz.U. z 1984 r., Nr 5, poz. 24), Oficyna 2010, LEX, wyd. III.

[26] Art. 7 ust. 2 pkt 4 *Prawa prasowego.*

[27] J. Grajewski, L. Paprzycki, S. Steinborn, *Komentarz do art. 180...*, s. 448; podobnie J. Sobczak, *Komentarz do art.15 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe* (Dz.U. z 1984 r., Nr 5, poz. 24), LEX 2008.

regulacja art. 163 d. kpk dotyczy jedynie sytuacji wycinkowej obejmującej kwestię składania zeznań w procesie karnym i uwarunkowanej ponadto zwolnieniem przez określony organ od obowiązku zachowania tajemnicy. Stanowisko Sądu Najwyższego spotkało się zarówno z krytyką (Z. Gostyński), jak i z pełną aprobatą glosujących to orzeczenie (E. Łętowska i J. Łętowski oraz M. Filar)[28].

Orzeczenie to jest o tyle ważne, że wskazuje na to, iż zakaz dowodowy sformułowany w dyspozycji art. 180 § 2 kpk w zw. z art. 15 *Prawa prasowego* nie ma charakteru bezwzględnego, a nadto możliwa jest interpretacja tych przepisów według ogólnie przyjętych zasad wykładni. Warto wspomnieć również, że zgodnie z art. 12 tegoż *Prawa* dziennikarz obowiązany jest zachować szczególną staranność i rzetelność przy zbieraniu i wykorzystywaniu materiałów prasowych. Powinien w szczególności sprawdzić zgodność z prawdą uzyskanych wiadomości lub podać ich źródło, chronić dobra osobiste, a ponadto interesy działających w dobrej wierze informatorów i innych osób, które okazują mu zaufanie. Od obowiązku zachowania tajemnicy notarialnej, adwokackiej, radcowskiej, lekarskiej i dziennikarskiej może bowiem zwolnić jedynie sąd, po spełnieniu odpowiednich przesłanek.

W literaturze przedmiotu można znaleźć informację, że co najmniej od 2004 r. żywy był w doktrynie spór o to, czy istnieje bezwzględny zakaz stosowania podsłuchu rozmów telefonicznych i kontroli przekazów e-mailowych dziennikarzy i innych osób wymienionych w art. 180 § 2 kpk. Tak zdefiniowany problem może być kontrowersyjny nadal.

Przeciwko możliwości stosowania podsłuchu (procesowego lub w formie kontroli operacyjnej), a także samej możliwości żądania bilingów dziennikarza wypowiedzieli się W. Gontarski i J. Sobczak. Gontarski stwierdził nawet, że *prokurator nie ma prawa żądać bilingu rozmów dziennikarza ani od niego, ani od operatora, gdyż postępowanie takie stanowi przestępstwo nadużycia władzy prokuratorskiej. Wyjątkowo z takim żądaniem mógłby wystąpić dopiero po zwolnieniu dziennikarza z obowiązku zachowania tajemnicy przez sąd, ale jedynie w przypadku, gdy chodzi o informacje, których przedmiotem są najcięższe przestępstwa* (zob. W. Gontarski, *Prokurator nadużywa władzy*, „Rzeczpospolita" z dnia 13 grudnia 2004 r.)[29].

Zdaniem A. Bajończyka, R. Stefańskiego i G. Musialik natomiast istnieje prawna możliwość żądania bilingów, a nawet stosowania podsłuchu, gdyż nigdy nie można z całą pewnością przewidzieć, jakie informacje zostaną uzyskane dzięki uruchomieniu kontroli rozmów telefonicznych dziennikarza, a tym bardziej, czy będą one objęte tajemnicą dziennikarską, która w dużej mierze zależna jest od woli osoby udzielającej informacji lub od autora listu do redakcji. Bajończyk dowodzi dalej, iż w zasadzie na żądanie prokuratora czy sądu operator musi wydać biling, jeżeli ma on znaczenie dla toczącego się postępowania, ponieważ art. 218 § 1 kpk nie przewiduje żadnych ograniczeń w tym zakresie[30].

Podobne stanowisko prezentuje J. A. Śliwa, który uważa, że *wykaz rozmów prowadzonych z telefonu używanego przez dziennikarza nie jest objęty tajemnicą dziennikarską* (…). *W związku z tym wykaz nie może być wystarczającym dowodem na przeka-*

[28] J. Sobczak, *Komentarz do art.15 ustawy z dnia 26 stycznia 1984 r. – Prawo prasowe* (Dz.U. z 1984 r., Nr 5, poz. 24), LEX 2008.
[29] Tamże.
[30] Tamże.

zanie określonych informacji, chroniony jest natomiast tajemnicą telekomunikacyjną, podobnie jak relacja między organem procesowym a operatorem[31].

Stanowisku wskazującemu na dopuszczalność żądania i analizowania bilingów osób, co do których potencjalnie konieczne jest uzyskanie zwolnienia z zachowania tajemnicy i zgoda sądu, nie przeczy często przywoływane orzeczenie Sądu Najwyższego z 22 listopada 2002 r. W uchwale tej SN stwierdził, że: *Sformułowany w art. 180 § 3 k.p.k. zakaz zwalniania dziennikarza od obowiązku zachowania w tajemnicy danych umożliwiających identyfikację autora materiału prasowego, listu do redakcji lub innego materiału o tym charakterze, jak również identyfikację osób udzielających informacji opublikowanych lub przekazanych do opublikowania, jeżeli osoby te zastrzegły nieujawnianie tych danych - konkretyzuje treść tajemnicy dziennikarskiej określonej w art. 15 ustawy z 26 stycznia 1984 r. – Prawo prasowe. Zakaz ten ma charakter bezwzględny i nie może być naruszany poprzez zastosowanie art. 2 § 1 pkt 1 k.p.k. i art. 9 k.p.k.*[32]. Zakaz ten bowiem odnosi się do poprawnie zdefiniowanej tajemnicy dziennikarskiej, a nie do osoby wykonującej zawód dziennikarza.

V. Analiza aktualnego stanu prawnego

Jako wystarczającą podstawę do żądania bilingu na etapie postępowania przygotowawczego (przez prokuratora) należy wskazać treść art. 218 kpk.

W przypadku uzyskiwania, gromadzenia i przetwarzania (a więc i analizowania) danych telekomunikacyjnych oraz pozyskiwania tych danych w ramach niejawnej pracy operacyjnej danej służby taką samoistną podstawę prawną stanowić będą, jako *lex specialis,* przepisy art. 10b *Ustawy z dnia 12 października 1990 r. o Straży Granicznej*, art. 28 *Ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu*, art. 18 *Ustawy z dnia 9 czerwca 2006 r. o Centralnym Biurze Antykorupcyjnym* czy art. 36b *Ustawy z dnia 28 września 1991 r. o kontroli skarbowej.*

Ogólne zasady wykładni, a w szczególności zasada *lex posterior derogat legi priori,* a więc, że pierwszeństwo należy zawsze przypisać prawu ustanowionemu później, jednoznacznie wskazują na to, że prym musi wieść prawo ustanowione później dla zwalczania zjawisk patologicznych. Chodzi więc o to, że, przepisy dotyczące możliwości gromadzenia danych telekomunikacyjnych w zakresie pracy operacyjnej zostały wprowadzone w 2009 r., a więc później niż te wprowadzone w okresie, z którego wywodzi się nie tylko prawna definicja tajemnicy dziennikarskiej, ale także chroniąca ją norma art. 180 § 2 i 3 kpk. Przy czym należy wskazać, że przepisy dotyczące prawnej dopuszczalności uzyskiwania danych objętych tajemnicą telekomunikacyjną zostały wprowadzone w celu realizacji fundamentalnego prawa obywateli do bezpiecznego życia[33], wolnego od przemocy. Racjonalny ustawodawca, wprowadzając przepisy pozwalające przykładowo policji żądać danych objętych tajemnicą ubezpieczeniową czy bankową na podstawie postanowienia sądu, mógł, gdyby widział taką potrzebę, objąć kontrolą sądową również dane telekomunikacyjne.

Oczywiste jest też, że ingerencja władzy publicznej w korzystanie z tego prawa nastąpiła na podstawie ustawy i jest konieczna *z uwagi na bezpieczeństwo państwowe,*

[31] Tamże.

[32] Uchwała SN o sygn. I KZP 26/02 z 22 listopada 2002 r. OSNKW 2003/1 - 2/6.

[33] Art. 5 *Konwencji o Ochronie Praw Człowieka i Podstawowych Wolności.*

bezpieczeństwo publiczne lub dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności lub ochronę praw i wolności innych osób[34].

VI. Postulaty *de lege ferenda*

Z orzecznictwa ETPCz dotyczącego prawnej dopuszczalności działań państwa i jego służb policyjnych czy specjalnych wynika, że systemy niejawnej inwigilacji muszą zawierać proceduralne gwarancje skutecznej kontroli działań tych służb, która to powinna być sprawowana przez organy zewnętrzne wobec nich. Jednocześnie zawarte jest tu stwierdzenie o charakterze postulatywnym, że kontrola sądowa jest najlepszą gwarancją niezależności, bezstronności i stosowania właściwych procedur.

Niezależnie od tego, czy działania służb państwowych o charakterze policyjnym, które żądały bilingów dziennikarzy, o ile oczywiście takie sytuacje występowały, były w świetle obowiązujących przepisów dopuszczalne, należy wskazać, że powinny one ulec zmianie. Potrzebna jest bowiem większa niż dotychczas ochrona podstawowych praw i swobód obywatelskich.

Podstawy prowadzenia czynności operacyjnych oraz standardy sądowej kontroli ich zasadności i legalności powinny odnosić się do wszystkich działań operacyjnych i procesowych naruszających prawa obywatelskie, a nie tylko do podsłuchu procesowego czy operacyjnego, jak ma to miejsce w tej chwili. Dokonana właśnie przez sejm zmiana przepisów nie zapewnia jednak sądowej kontroli działań operacyjnych innych niż podsłuch, w tym także jedynie sądowej podstawy żądania bilingów co jak się wydaje, powinno być standardem w demokratycznym państwie.

Streszczenie

Niniejszy artykuł podejmuje aktualną obecnie i żywo dyskutowaną w środkach masowego przekazu kwestię prawnych podstaw żądania bilingów przez organy ścigania, zarówno do celów operacyjnych, jak i procesowych. Jako punkt wyjścia rozważań obrano powszechnie akceptowany standard gwarancji praw człowieka i podstawowych swobód obywatelskich wyrażony w *Konwencji o Ochronie Praw Człowieka i Podstawowych wolności*, orzecznictwie Europejskiego Trybunału Praw Człowieka oraz w normach konstytucyjnych.

Opierając się na wymienionych wyżej przepisach, autor stwierdza, że ingerencja organów władzy państwowej w te prawa jest możliwa tylko wtedy, gdy będą one działały:

– na podstawie ustaw i w ich granicach,
– w sytuacjach koniecznych z uwagi na bezpieczeństwo państwa, bezpieczeństwo publiczne, dobrobyt gospodarczy kraju, ochronę porządku i zapobieganie przestępstwom, ochronę zdrowia i moralności oraz ochronę praw i wolności innych osób.

Dalej autor definiuje pojęcia: k o n t r o l a k o r e s p o n d e n c j i, k o n t r o l a o p e r a c y j n a i w y k a z p o ł ą c z e ń z uwagi na to, że w ustawach regulujących

[34] Art. 8 Konwencji.

funkcjonowanie odpowiedniej służby stosującej niejawny sposób pozyskiwania informacji, wskazane zostały prawne przesłanki dopuszczalności stosowania niejawnych form pracy operacyjnej. Jednocześnie zwraca uwagę, że przesłanki te muszą mieścić w zakresie kompetencyjnym danej służby oraz spełniać zasadę subsydiarności wyrażającą się w stwierdzeniu, że inne formy pracy operacyjnej są lub mogą być bezskuteczne.

Kolejną kwestią podnoszoną w artykule było zdefiniowanie pojecia b i l i n g, które potocznie rozumiane jest jako wykaz połączeń telefonicznych, a tym samym nie może być utożsamiane z kontrolą operacyjną i posłuchem procesowym. Autor artykułu zauważa, że w świetle obowiązujących przepisów, a w szczególności jednoznacznej treści art. 218 § 1 kpk, nie jest konieczne uzyskanie postanowienia sądu w celu otrzymania od operatora na potrzeby toczącego się postępowania przygotowawczego wykazu połączeń telefonicznych.

Podobnie kwestia uzyskiwania bilingów przez Policję, Agencję Bezpieczeństwa Wewnętrznego, Agencję Wywiadu, Straż Graniczną czy Centralne Biuro Antykorupcyjne została uregulowana między innymi w przepisach znowelizowanej w lipcu 2009 r. ustawy *Prawo telekomunikacyjne*. Udostępnienie żądanych przez te instytucje danych telekomunikacyjnych następuje nieodpłatnie, bez potrzeby uzyskiwania postanowienia sądu, ale jedynie w celu zapobiegania przestępstwom lub wykrywania ich.

Dalej autor analizuje treść i zakres tajemnicy dziennikarskiej przez pryzmat brzmienia art. 15 *Prawa prasowego* w kontekście art. 7 tej ustawy. Artykuł 15 przytoczonej ustawy stwierdza bowiem, że dziennikarzowi przysługuje prawo związane z zachowaniem tajemnicy dziennikarskiej tylko jako *autorowi materiału prasowego*, a nie w związku z wykonywanym zawodem. Artykuł 7 natomiast w sposób istotny zawęża znaczenie i zakres tajemnicy dziennikarskiej tylko do materiału opublikowanego lub przekazanego do publikacji.

W konsekwencji autor niniejszej publikacji stoi na stanowisku, że wykaz rozmów prowadzonych z telefonu używanego przez dziennikarza nie jest objęty tajemnicą dziennikarską. Postuluje jednak (*de lege ferenda*), aby systemy niejawnej inwigilacji podlegały kontroli organów zewnętrznych. Obecnie zaś najlepszą gwarancją niezależności, bezstronności i stosowania właściwych procedur jest kontrola sądowa.

Abstract

The article refers to the widely discussed mater of legal basis for the right to claim telephone billings by law enforcement institutions for both operational purposes and prosecution. The starting point for considerations was the publicly accepted standard for guarantees of human rights and fundamental freedoms expressed in the Convention for the Protection of Human Rights and Fundamental Freedoms, the European Court of Human Rights and constitutional norms.

The interference of state authorities in these rights is possible only if the authorities will act:

- accordingly to and strictly within legal regulations and Acts;
- according to the interests of national security, public safety or national prosperity, protection and prevention, health or morals or the protection of the rights and freedoms of others.

Further on, the author defines the concept: *control of correspondence, operational control, the list of telephone connections*. The laws governing the operation of the

appropriate service using a clandestine method of obtaining information are defined in the legal conditions for admissibility of clandestine forms of operational activity. These conditions have to be included within the statutory competences of the service, and fulfill the subsidiary rule that other forms of operational activity are or may be considered as ineffective.

Another issue raised in the article was to define the term *telephone billing*, which is understood to be a form of a list of phone calls, therefore cannot be identified with the operational control and wiretapping.

The existing legislation, in particular the wording of Article 218 § 1 of the Code of Criminal Procedure, it is not necessary to obtain a court order to request for billing from the operator company within the preparatory proceedings.

The issue of obtaining billings by the Police, the Internal Security Agency, the Foreign Intelligence Agency, the Border Guard or the Central Anticorruption Bureau is regulated, inter alia, by the provisions of the amended in July 2009, the Telecommunications Act. Making available telecommunication data is provided free of charge, without the necessity to obtain a court order, but only if used to prevent or detect crime.

Additionally, the author analyzes the content and scope of journalistic confidentiality contained in the articles of the Press Law. Art 15 states that a journalist has the right associated with the confidentiality of journalism only as the 'author of a press release' not in relation to the profession. Article 7 of the Press Law in fact significantly narrows down the scope and range of confidentiality of journalistic materials only to published or communicated for publication.

Consequently, the author presents the view that a list of phone conversations of a journalist cannot be treated as a part of the journalist confidentiality.

The author suggests (de lege ferenda) that classified surveillance systems should fall under the supervision of external institutions. Judicial control is the best guarantee of independence, impartiality and the use of appropriate procedures.

Katarzyna Wojtaszyn

Stosowanie instytucji tymczasowego zajęcia mienia ruchomego w postępowaniu przygotowawczym – aspekty praktyczne

Jednym z najważniejszych narzędzi w walce z przestępczością jest stosowanie mechanizmów prawnych pozwalających na skuteczne pozbawianie sprawców przychodów z popełnianych przestępstw. W literaturze przedmiotu wielokrotnie podkreśla się, że pozbawienie sprawców „owoców" popełnionego przestępstwa jest najdotkliwszą karą i stanowi efektywny sposób zwalczania zorganizowanej przestępczości[1]. Działanie to ma na celu także pozbawienie ich możliwości prowadzenia dalszej działalności przestępczej, które wiąże się z ponoszeniem dużych nakładów finansowych. Majątek, głównie ten nielegalnie uzyskany, zwykle przenoszony jest na rzecz zaufanych osób trzecich, bądź transferowany za granicę. Działania te mają uniemożliwić przeprowadzenie zabezpieczenia majątkowego[2].

Wzrost zainteresowania problematyką postępowania zabezpieczającego w polskim procesie karnym ma związek z przystąpieniem Polski do Unii Europejskiej, a tym samym z koniecznością stosowania systemu prawnego tej organizacji w wewnątrzkrajowym obrocie prawnym, w tym także w relacjach z innymi państwami członkowskimi. W zakresie zabezpieczenia majątkowego niezwykle istotne znaczenie mają przepisy ramowej decyzji Rady UE nr 2003/577/WSiSW z dnia 22.07.2003 r. w sprawie wykonywania w Unii Europejskiej postanowień o zabezpieczeniu mienia i środków dowodowych, na podstawie których m.in. ustalono zasady stosowania przez państwa członkowskie postanowień o zabezpieczeniu majatkowym, wydanych przez organ sądowy innego państwa członkowskiego w ramach postępowania karnego[3].

Instytucja stosowania zabezpieczenia majątkowego, na gruncie przepisów polskiego kodeksu karnego i kodeksu postępowania karnego, została zastrzeżona wyłącznie dla prokuratora i sądu. Niemniej jednak, podkreślenia wymaga fakt, że niezwykle istotny wpływ na przebieg postępowania zabezpieczającego mają działania organów innych niż prokurator, którym powierzono prowadzenie postępowania przygotowawczego, jak np. Agencji Bezpieczeństwa Wewnętrznego, Policji czy Straży Granicznej. Rola tych organów sprowadza się m.in. do zajęcia mienia ruchomego poprzez dokonanie tymczasowego zajęcia i wskazania prokuratorowi składników mienia podejrzanego, podlegających zabezpieczeniu[4]. Organy te, z racji przyznanych kompetencji ustawowych, poza czynnościami procesowymi mają również prawo do prowadzenia działań o charakterze operacyjno-rozpoznawczym.

---

[1] Zob. np. W. Filipkowski, *Zwalczanie przestępczości zorganizowanej w aspekcie finansowym*, Kraków 2004, Zakamycze, s. 344; K. Liszewski, D. Najmoła, K. Wiciak, *Śledztwo finansowe*, Szczytno 2006, WSPOL, s. 11; M. Prengel, *Środki zwalczania prania pieniędzy w ujęciu prawnoporównawczym*, Toruń 2003, Dom Organizatora, s. 376 i nast.; B. Kurzępa, *Przesłanki stosowania zabezpieczenia majątkowego oraz tymczasowego zajęcia mienia w postępowaniu przygotowawczym*, „Prokurator" 2005, nr 4, s. 7.

[2] B. Kurzępa, *Przesłanki stosowania zabezpieczenia*..., s. 7 - 8; D. Bunikowski, *Przepadek korzyści majątkowych pochodzących z popełnienia przestępstwa jako środek karny*, „Prokuratura i Prawo" 2008, nr 5, s. 68 - 69.

[3] Dz.Urz. UE L196/45 z 2.08.2003.

[4] K. Liszewski, D. Najmoła, K. Wiciak, *Śledztwo finansowe*, s. 9 - 10.

W niniejszym artykule zostanie omówiona głównie problematyka dotycząca stosowania instytucji tymczasowego zajęcia mienia ruchomego w postępowaniu przygotowawczym. Dla pełnego zaprezentowania podjętej tematyki niezbędne jest uwzględnienie przesłanek prawnych, jednak zasadnicze treści przedstawionego tekstu koncentrują się na aspektach proceduralnych związanych z przeprowadzaniem tymczasowego zajęcia tego typu mienia. Zagadnienia praktyczne nie znajdują się bowiem w kręgu zainteresowania badaczy zajmujących się tym problemem.

Problematyka zabezpieczenia majątkowego ściśle związana jest – obok instytucji tymczasowego zajęcia mienia ruchomego – również z procesem ustalenia składników majątkowych osób podejrzanych. Ze względu na zakres i charakter artykułu zagadnienie to zostało jedynie zasygnalizowane i poddane ogólnej charakterystyce.

Zabezpieczenie majątkowe jest środkiem przymusu stosowanym wobec podejrzanego, a jego celem jest zagwarantowanie realizacji rozstrzygnięcia co do odpowiedzialności karnej. Zgodnie art. 291 kpk i następnymi w razie popełnienia przestępstwa, za które można orzec grzywnę, przepadek, nawiązkę lub świadczenie pieniężne albo nałożyć obowiązek naprawienia szkody lub zadośćuczynienia za doznaną krzywdę, może z urzędu nastąpić zabezpieczenie wykonania orzeczenia na mieniu oskarżonego, a także zabezpieczenie roszczeń o naprawienie szkody w razie popełnienia przestępstwa przeciwko mieniu lub wyrządzenia przestępstwem szkody w mieniu. Postanowienie o zabezpieczeniu majątkowym w postępowaniu przygotowawczym wydaje prokurator, w postępowaniu sądowym zaś – sąd.

Skuteczne wykonanie kar i zastosowanie środków karnych niejednokrotnie byłoby niemożliwe lub nieskuteczne, gdyby na etapie prowadzonego postępowania przygotowawczego nie dokonano zabezpieczenia majątkowego. *Dostatecznie wczesne i sprawne zabezpieczenie może być warunkiem właściwej i całkowitej realizacji wyroku skazującego dla oskarżonego na kary i środki karne o charakterze majątkowym oraz zasądzającego roszczenia odszkodowawcze*[5].

W rozdziale 32 *Kodeks postępowania karnego* przewiduje instytucję tymczasowego zajęcia mienia ruchomego, którą poprzedza zabezpieczenie majątkowe. Tymczasowe zajęcie mienia ruchomego jako środek przymusu procesowego jest instrumentem prawnym, który może przyczynić się do skutecznego przebiegu postępowania zabezpieczającego. Zaniechanie dokonania tej czynności może niejednokrotnie mieć wpływ na niemożność wykonania przyszłego orzeczenia sądu. Z drugiej jednak strony należy pamiętać, że jej nieprawidłowe wykonanie może skutkować naruszeniem prawa do poszanowania mienia[6]. Mimo, że przepisy odnoszące się do stosowania tymczasowego zajęcia mienia ruchomego wydają się jasne, praktyka pokazuje, że ich interpretacja nastręcza wiele trudności. Jednym z problemów związanych z prawidłowym przeprowadzeniem tej czynności jest np. kwestia prawidłowego sporządzenia dokumentacji.

Stosowanie instytucji tymczasowego zajęcia mienia ruchomego – co podkreśla się w literaturze przedmiotu – możliwe jest nie tylko na etapie postępowania przygoto-

[5] Tamże, s. 14.

[6] P. Starzyński, *Postępowanie zabezpieczające w polskim procesie karnym*, Warszawa 2007, C.H. Beck, s. 265.

wawczego, ale i sądowego[7]. Zagadnienia poruszone w tej publikacji koncentrować się będą właśnie na kwestiach związanych z postępowaniem przygotowawczym. Tymczasowe zajęcie mienia może być przeprowadzone nie tylko po wszczęciu postępowania przygotowawczego, lecz także w trybie czynności, o jakich mowa w treści art. 308 kpk, w niezbędnym zakresie.

Przesłanki tymczasowego zajęcia mienia

Czytając treść art. 295 § 1 kpk, można wyodrębnić przesłanki, których łączne występowanie warunkuje prawne przeprowadzenie tej czynności. Zgodnie z jego treścią *w razie popełnienia przestępstwa, o którym mowa w art. 291 KPK, Policja może dokonać tymczasowego zajęcia mienia ruchomego osoby podejrzanej, jeżeli zachodzi obawa usunięcia tego mienia*[8]. Uprawnienia te, stosownie do art. 312 kpk przysługują także jednostkom Agencji Bezpieczeństwa Wewnętrznego, Straży Granicznej, Służby Celnej, Centralnego Biura Antykorupcyjnego oraz, na podstawie przepisów szczególnych, innym organom, np. Państwowej Inspekcji Handlowej.

Przestępstwa określone w art. 291 kpk

Tymczasowego zajęcia mienia ruchomego można dokonać tylko w razie popełnienia przestępstwa, za które orzeczone mogą być:
– grzywna,
– przepadek,
– nawiązka,
– świadczenie pieniężne,
– obowiązek naprawienia szkody lub zadośćuczynienia za doznaną krzywdę,
– zabezpieczenie roszczeń o naprawienie szkody w sprawach o przestępstwo przeciwko mieniu, lub gdy przestępstwem wyrządzono szkodę w mieniu.

Podmiot, wobec którego można stosować tymczasowe zajęcie mienia ruchomego

Tymczasowe zajęcie mienia ruchomego może być dokonane wyłącznie na mieniu osoby podejrzanej lub podejrzanego. Kodeks postępowania karnego, w art. 71, definiuje wyłącznie pojęcie p o d e j r z a n e g o, brak natomiast ustawowej definicji pojęcia o s o b y p o d e j r z a n e j. *Podejrzanym jest osoba, co do której wydano postanowienie o przedstawieniu zarzutów albo której bez wydania takiego postanowienia postawiono zarzut w związku z przystąpieniem do przesłuchania w charakterze podejrzanego*[9]. Za o s o b ę p o d e j r z a n ą uznaje się zaś osobę, którą podejrzewa się o popełnienie prze-

[7] Tymczasowe zajęcie mienia ruchomego może być dokonane na etapie postępowania sądowego, a więc po wniesieniu aktu oskarżenia, jednakże organy uprawnione do jego przeprowadzenia, m.in. ABW i Policja, nie mogą *ex officio* dokonać tego zajęcia w przypadku uzyskania informacji o podejmowaniu przez oskarżonego działań mających na celu usunięcie składników majątkowych. Tymczasowe zajęcie mienia może natomiast zostać dokonane na podstawie postanowienia o przeszukaniu/żądaniu wydania rzeczy wydanego przez sąd.

[8] Dz.U. z 1997 r., Nr 89, poz. 555 ze zm.

[9] *Ustawa z dnia 6.06.1997 r., Kodeks postępowania karnego*, Dz.U. z 1997, Nr 89, poz. 555 ze zm. (art. 71 kpk).

stępstwa, przypuszcza się, że je popełniła, ale której nie przedstawiono jeszcze zarzutu jego popełnienia i której bez wydania takiego postanowienia nie postawiono zarzutu w związku z przystąpieniem do przesłuchania w charakterze podejrzanego[10].

W praktyce przesłanka ta jest często błędnie interpretowana (szczególnie przez niedoświadczonych funkcjonariuszy), wskutek czego wywodzą oni przekonanie, że mienie ruchome można zająć tylko od podejrzanego albo od osoby podejrzanej. Z punktu widzenia prawnego nie ma natomiast znaczenia, czy mienie podlegające tymczasowemu zajęciu znajduje się (jest przechowywane) w miejscu zamieszkania podejrzanego albo osoby podejrzanej. Ważne jest jedynie, aby mienie to było własnością tej osoby. Wiele prowadzonych spraw pokazuje, że mienie należące do podejrzanego (osoby podejrzanej) nie jest przechowywane w miejscu jej zamieszkania bądź też jest użytkowane przez osoby trzecie. Innym aspektem tego zagadnienia jest kwestia mienia, które widnieje jako własność osób trzecich, jednak z ustaleń wynika że stanowi własność podejrzanego (osoby podejrzanej) i zostało przeniesione na osobę trzecią w celu m.in. zapobieżenia zajęciu.

Rodzaj mienia podlegającego zajęciu

Kolejną przesłanką stosowania instytucji tymczasowego zajęcia mienia jest rodzaj mienia, które może zostać zajęte. Artykuł 295 § 1 kpk wskazuje jednoznacznie, że może to być wyłącznie mienie ruchome. Należy pamiętać, że o ile przepisy cywilistyczne nie mają zastosowania do tymczasowego zajęcia mienia, to jednak może ono dotyczyć rzeczy ruchomych w rozumieniu prawa cywilnego, co do których może być skierowana egzekucja[11].

Przedmiotami wchodzącymi w zakres mienia ruchomego podlegającego tymczasowemu zajęciu mogą być także dokumenty, które uprawniają do otrzymania sumy pieniężnej, np. los loteryjny, weksel, bony premiowe, książeczki oszczędnościowe, obligacje, akcje, listy zastawne, polisy ubezpieczeniowe bądź dokumenty zawierające obowiązek wypłaty odsetek, kapitału, udziału w zyskach albo stwierdzenie uczestnictwa w spółce[12]. Tymczasowemu zajęciu podlegają także pieniądze polskie i zagraniczne, monety będące numizmatami, złoto, platyna oraz inne rzeczy przedstawiające wartość historyczną lub artystyczną (obrazy, fotografie itp.).

---

[10] T. Grzegorczyk, J. Tylman, *Polskie postępowanie karne*, Warszawa 1999, Wydawnictwo Prawnicze PWN, s. 290.

[11] Mienie podlegające zabezpieczeniu zgodnie z art. 291 kpk rozumiane jest w ujęciu cywilistycznym: „Przy interpretowaniu pojęcia mienia ruchomego, w kontekście stosowania środka przymusu procesowego, należy przede wszystkim kierować się charakterem prawnym tej instytucji, jej celem. Mienie ruchome jest pojęciem normatywnym, którym posługują się przepisy procesu karnego. Nie ulega wątpliwości, że mienie ruchome przyjmuje postać rzeczy w rozumieniu cywilistycznym, skoro przedmiotem zabezpieczenia jest mienie w ujęciu cywilistycznym, a wykonanie tymczasowego zajęcia następuje stosownie do przepisów art. 217 - 235 kpk, w których właśnie jest mowa o rzeczach podlegających zajęciu. Wobec tego należy uznać, że zajęciu podlegają rzeczy ruchome, lecz nie w rozumieniu prawa karnego, tylko prawa cywilnego". Tamże, s. 45.

[12] *Zarządzenie nr 1426 Komendanta Głównego Policji w sprawie metodyki wykonywania czynności dochodzeniowo-śledczych przez służby policyjne wyznaczone do wykrywania przestępstw i ścigania ich sprawców*, Dz.Urz. KGP z 2005, Nr 1, poz. 1; P. Starzyński podkreśla w tym kontekście: *skoro wykonanie zabezpieczenia praw majątkowych związanych z takimi dokumentami polega na ich zajęciu, to właśnie charakter tymczasowego zajęcia mienia ruchomego, jego cel, jakim jest uniemożliwienie wyzbycia się mienia, stanowi o dopuszczalności zajmowania tego typu dokumentów w trybie art. 295 kpk*, P. Starzyński, *Postępowanie zabezpieczające*, s. 48.

Zgodnie z art. 295 kpk, tymczasowemu zajęciu podlega mienie ruchome, którego podejrzany lub osoba podejrzana jest faktycznym właścicielem. Podlega mu również mienie wchodzące w skład majątku wspólnego małżonków, mienie ruchome, na zakup którego zaciągnięto kredyt lub pożyczkę, a w szczególności którego spłata jest zaawansowana w stopniu pozwalającym na zaspokojenie wierzytelności banku i uzyskanie kwot na poczet zabezpieczenia majątkowego, a także mienie ruchome, którego współwłaścicielem oprócz podejrzanego lub osoby podejrzanej jest kilka innych osób. Tymczasowe zajęcie mienia ruchomego nie może jednak nastąpić na majątku stanowiącym wspólność majątkową, jeżeli pokrzywdzonym jest małżonek podejrzanego lub osoby podejrzanej.

Dokonując tymczasowego zajęcia mienia ruchomego należy pamiętać, iż spod zajęcia wyłączone są przedmioty wskazane w treści art. 829 kpc[13].

Tymczasowemu zajęciu mienia nie podlegają także przedmioty wskazane w treści *Rozporządzenia Ministra Sprawiedliwości z 16 maja 1996 r. w sprawie przedmiotów należących do rolnika prowadzącego gospodarstwo, które nie podlegają egzekucji sądowej*[14], np. ciągnik wraz z maszynami i sprzętem współpracującym niezbędnym do uprawy, pielęgnacji, zbioru i transportu ziemiopłodów.

Zajęciu nie podlega ponadto mienie ruchome stanowiące własność:

– *spółek prawa handlowego, innych osób prawnych, w których podejrzany lub osoba podejrzana posiada udziały lub zajmuje stanowiska;*
– *banków, firm leasingowych lub innych osób prawnych, a oddanych do użytkowania podejrzanemu lub osobie podejrzanej na podstawie odpowiedniej umowy*[15].

Obawa usunięcia mienia

Kolejnym warunkiem stosowania tymczasowego zajęcia mienia ruchomego jest obawa jego usunięcia. Musi ona dotyczyć konkretnego mienia ruchomego, które jest przedmiotem tymczasowego zajęcia[16]. Wspomniana obawa może być wynikiem ustaleń poczynionych przez organ procesowy, wskazujących, że osoba podejrzana lub inna,

[13] *Ustawa z dnia 17.11.1964 r. Kodeks postępowania cywilnego*, Dz.U. z 1964 r., Nr 43, poz. 296 z późn. zm., art. 829 kpc: „przedmioty urządzenia domowego, pościel, bielizna i ubranie codzienne niezbędne dla dłużnika i będących na jego utrzymaniu członków jego rodziny, a także ubranie niezbędne do pełnienia służby lub wykonywania zawodu, zapasy żywności i opału niezbędne dla dłużnika i będących na jego utrzymaniu członków rodziny na okres jednego miesiąca, jedna krowa lub dwie kozy albo trzy owce potrzebne do wyżywienia dłużnika i będących na jego utrzymaniu członków jego rodziny wraz z zapasem paszy i ściółki do najbliższych zbiorów, narzędzie i inne przedmioty niezbędne do osobistej pracy zarobkowej dłużnika oraz surowce niezbędne dla niego do produkcji na okres jednego tygodnia, z wyłączeniem jednak pojazdów mechanicznych, u dłużnika pobierającego periodyczną stałą pracę – pieniądze w kwocie, która odpowiada nie podlegającej egzekucji części płacy za czas do najbliższego terminu wypłaty, a u dłużnika nie otrzymującego stałej płacy – pieniądze niezbędne dla niego i jego rodziny na utrzymanie przez dwa tygodnie, przedmioty niezbędne do nauki, papiery osobiste, odznaczenia i przedmioty służące do wykonywania praktyk religijnych oraz przedmioty codziennego użytku, które mogą być sprzedane tylko znacznie poniżej ich wartości, a dla dłużnika mają znaczną wartość użytkową".

[14] Dz.U. z 1996 r., Nr 63, poz. 300.

[15] *Zarządzenie nr 1426 Komendanta Głównego Policji z 23 grudnia 2004* (zob. przyp. 13).

[16] P. Starzyński, *Postępowanie zabezpieczające*, s. 274 i nast.; w literaturze przedmiotu przesłankę tę interpretuje się jako realne niebezpieczeństwo, że mienie zostanie zbyte, ukryte, oddane na przechowanie lub darowane innej osobie. Zob. też: B. Kolasiński (red.), R. Gawinek, T. Kulikowski, J. Masierowski, W. Palejko, D. Wiśniewski, *Metodyka postępowania w zakresie zabezpieczenia majątkowego*, „Prokuratura i Prawo" 2006, nr 4, s. 103.

mając świadomość możliwości zajęcia tego mienia, podejmuje działania zmierzające do wyzbycia się go lub ukrycia[17]. O jej istnieniu świadczyć mogą wypowiedzi lub zachowanie osoby podejrzanej (podejrzanego) – anonsy prasowe o sprzedaży samochodu[18] lub też wypowiedzi innych osób, np. zeznania świadków. Ponieważ większość przestępstw popełnianych jest w celu osiągnięcia korzyści majątkowej można przyjąć, że z niebezpieczeństwem usunięcia mienia mamy do czynienia niemal w każdym przypadku[19].

Obawa może wystąpić nie tylko w momencie ujawnienia przestępstwa i osoby podejrzanej, ale także później, na etapie postępowania przygotowawczego prowadzonego w fazie *in pesonam*. Każda taka okoliczność powinna być udokumentowana w ustaleniach operacyjnych lub procesowych[20]. W przepisach kpk nie został jednak wskazany sposób dokumentowania informacji wskazujących na obawę usunięcia tego typu mienia. W praktyce najczęściej stosowaną formą dokumentacji tego rodzaju wiedzy w toku postępowania przygotowawczego jest notatka urzędowa. Należy jednak podkreślić, że forma dokumentowania takich informacji uzależniona jest od ich źródła, dlatego też wiedza o zamiarze wyzbycia się mienia może zostać udokumentowana w protokole przesłuchania świadka, protokole przesłuchania podejrzanego itp. Zbieranie tego typu wiadomości należy do zadań organów prowadzących postępowanie przygotowawcze. W tym kontekście ogromne znaczenie mają działania o charakterze operacyjno-rozpoznawczym, które niejednokrotnie stanowią jedyne źródło informacji na ten temat.

W literaturze przedmiotu wymienia się jeszcze jedną przesłankę, której wystąpienie dowodzi słuszności dokonania tymczasowego zajęcia mienia ruchomego, mimo że nie wynika ona z przepisów kpk, a tym samym nie ma charakteru obligatoryjnego – tj. istotną szkodę majątkową wyrządzoną przestępstwem[21].

Procedura przeprowadzania tymczasowego zajęcia mienia ruchomego

Tymczasowe zajęcie mienia ruchomego może być – jak wspomniano – stosowane na etapie prowadzonego postępowania przygotowawczego, a także w trakcie postępowania w niezbędnym zakresie (art. 308 kpk). Zgodnie z treścią art. 295 § 2 kpk w zakresie tymczasowego zajęcia mienia przepisy art. art. 217 - 235 stosuje się odpowiednio. Oznacza to, że organy uprawnione do prowadzenia postępowań przygotowawczych dokonują zajęcia podczas czynności zatrzymania rzeczy lub przeszukania[22].

---

[17] P. Starzyński, *Postępowanie zabezpieczające*, s. 274; K. Liszewski, D. Najmoła, K. Wiciak, *Śledztwo finansowe*, s. 15.

[18] P. Starzyński, *Postępowanie zabezpieczające*, s. 275.

[19] Tamże; M. Kulesza, *Zabezpieczenie roszczeń na majątku podejrzanego*, „Służba MO" 1960, nr 2, s. 189.

[20] Zob. J. Kudrelek, *Uwagi dotyczące tymczasowego zajęcia mienia ruchomego w świetle „Kodeksu postępowania karnego" z 6 czerwca 1997 r.*, „Przegląd Policyjny" 1998, nr 2, s. 106; B. Kolasiński (red.), R. Gawinek, T. Kulikowski, J. Masierowski, W. Palejko, D. Wiśniewski, *Metodyka postępowania w zakresie postępowania*..., s. 103.

[21] J. Kudrelek, *Uwagi dotyczące tymczasowego zajęcia mienia*..., s. 106; J. Kudrelek, M. Lisiecki, *Zabezpieczenie majątkowe w postępowaniu karnym*, Szczytno 2004, WSPOL, s. 29.

[22] K. Liszewski, D. Najmoła, P. Wiciak, *Śledztwo finansowe*, s. 16; P. Starzyński, *Postępowanie zabezpieczające*, s. 286 - 294; według innych interpretacji zatrzymanie rzeczy lub przeszukanie przeprowadza się wyłącznie w razie potrzeby – gdy osoba podejrzana lub podejrzany nie wydaje mienia podlegającego zajęciu lub utrudnia swoim zachowaniem jego zajęcie. Zob. także: J. Kudrelek, R. Kwasiński, *Pisma procesowe*, Szczytno 2010, WSPOL, s. 385; B. Kolasiński (red.), R. Gawinek, T. Kulikowski, J. Masierowski, W. Palejko, D. Wiśniewski, *Metodyka postępowania w zakresie postępowania*..., s. 104.

Rzeczy mogące stanowić dowód w sprawie lub podlegające zajęciu w celu zabezpieczenia kar majątkowych, środków karnych o charakterze majątkowym albo roszczeń o naprawienie szkody należy wydać na żądanie sądu lub prokuratora, a w wypadkach niecierpiących zwłoki, także na żądanie Policji lub innego uprawnionego organu[23], np. ABW. Osobę, w której dyspozycji taka rzecz się znajduje, wzywa się do jej dobrowolnego wydania. W wypadkach niecierpiących zwłoki, gdy wcześniejsze uzyskanie postanowienia prokuratora nie było możliwe – należy pouczyć osobę, która rzecz wydała, że ma prawo do niezwłocznego złożenia wniosku o sporządzenie i doręczenie jej postanowienia prokuratora o zatwierdzeniu zatrzymania. Doręczenie postanowienia o zatwierdzeniu czynności powinno nastąpić w terminie 14 dni od momentu zatrzymania rzeczy.

Przeszukanie pomieszczeń i innych miejsc jest prawnie dopuszczalne w przypadku zamiaru wykrycia lub zatrzymania albo przymusowego doprowadzenia osoby podejrzanej, a także w celu znalezienia rzeczy mogących stanowić dowód w sprawie lub podlegających zajęciu w postępowaniu karnym, jeżeli istnieją uzasadnione podstawy do przypuszczenia, że osoba podejrzana lub wymienione powyżej rzeczy tam się znajdują[24]. Na tej samej podstawie dopuszczalne jest także przeprowadzenie przeszukania osoby, jej odzieży i podręcznych przedmiotów. Przeszukanie w toku prowadzonego postępowania przygotowawczego przeprowadzane jest na podstawie postanowienia prokuratora, w wypadkach niecierpiących zwłoki zaś, gdy wydanie postanowienia przez prokuratora nie jest możliwe, na podstawie nakazu kierownika jednostki organu przeprowadzającego tę czynność lub na podstawie legitymacji służbowej. Organ przeprowadzający daną czynność musi niezwłocznie wystąpić do prokuratora o zatwierdzenie jej przeprowadzenia, nawet jeżeli osoba, u której przeprowadzono przeszukanie, pouczona o tym prawie nie żąda doręczenia postanowienia.

Stosując tymczasowe zajęcie mienia ruchomego, należy pamiętać także, że zgodnie z art. 218 kpk można żądać od urzędów, instytucji i podmiotów prowadzących działalność pocztową lub telekomunikacyjną, urzędów celnych oraz instytucji i przedsiębiorstw transportowych wydania m.in. korespondencji i przesyłek. Wydanie tych rzeczy może nastąpić jednak tylko i wyłącznie na podstawie postanowienia sądu lub prokuratora.

Przeprowadzenie przeszukania lub zatrzymania rzeczy musi być udokumentowane w formie protokołu, na co wskazuje wymóg art. 143 § 1 pkt 6 kpk, konieczność sporządzenia protokołu z tymczasowego zajęcia mienia ruchomego wynika natomiast z art. 143 § 2 kpk[25].

Sposób prawidłowego sporządzania dokumentacji z czynności zatrzymania rzeczy lub przeszukania, podczas których dokonano tymczasowego zajęcia mienia, rodzi wiele pytań. Zgodnie z dyspozycją art. 148 § 1 kpk protokół powinien zawierać:
- oznaczenie czynności, czasu i miejsca jej dokonania oraz wykaz osób w niej uczestniczących,
- przebieg czynności oraz oświadczenia i wnioski jej uczestników,
- wydane w toku czynności postanowienia i zarządzenia, a jeżeli postanowienie lub zarządzenie sporządzono osobno – wzmiankę o jego wydaniu,

[23] Dz.U. z 1997 r., Nr 89, poz. 555 ze zm. (art. 217 kpk).
[24] Tamże, art. 219 kpk.
[25] Tamże. Zob. P. Starzyński, *Postępowanie zabezpieczające*, s. 289; K. Liszewski, D. Najmoła, K. Wiciak, *Śledztwo finansowe*, s. 16; J. Kudrelek, R. Kwasiński, *Pisma procesowe*, s. 385 i nast.

– w miarę potrzeby stwierdzenie innych okoliczności dotyczących przebiegu czynności.

Jednocześnie, jak wskazuje art. 148 § 2 kpk, oświadczenia i wnioski oraz stwierdzenia określonych okoliczności przez organ prowadzący postępowanie zamieszcza się w protokole z możliwą dokładnością, osoby biorące udział w czynności zaś mają prawo żądać zamieszczenia w protokole z pełną dokładnością wszystkiego, co dotyczy ich praw i interesów. Zgodnie z dyspozycją art. 229 kpk protokół zatrzymania rzeczy lub przeszukania, poza wymogami wskazanymi w art. 148 kpk powinien zawierać dodatkowo oznaczenie sprawy, z którą ma ono związek, dane na temat godziny rozpoczęcia i zakończenia czynności, dokładnej listy zatrzymanych rzeczy (w miarę potrzeby ich opis), a także wskazanie polecenia prokuratora lub sądu. Gdy czynność jest przeprowadzana w wypadku niecierpiącym zwłoki natomiast – wzmianki o poinformowaniu osoby, u której czynność jest przeprowadzana, że (na jej wniosek) otrzyma postanowienie o zatwierdzeniu czynności[26]. Protokół powinien odzwierciedlać ponadto – co podkreśla Z. Uniszewski – *wszystkie istotne szczegóły biegu wypadków na miejscu prowadzonych czynności; w przypadku przeszukania czasem byłoby trudno wskazać okoliczność bardziej doniosłą niż to, kiedy, kto konkretnie, w jakiej sytuacji i z jakiego miejsca wydostał przedmiot objęty poszukiwaniem*[27].

Mając na uwadze fakt, że tymczasowe zajęcie mienia ruchomego realizowane jest podczas czynności zatrzymania rzeczy lub przeszukania[28], każdorazowo należy sporządzić protokół z przeprowadzenia tych czynności, tj. protokół zatrzymania rzeczy lub przeszukania i tymczasowego zajęcia mienia ruchomego[29].

We wzorach pism procesowych[30] wskazuje się, że w protokole przeszukania lub zatrzymania rzeczy, w części zatytułowanej *Spis i opis rzeczy,* należy wpisać wszystkie przedmioty, które zatrzymano lub odnaleziono w toku przeszukania, niezależnie od dokładnego ich opisu w protokole tymczasowego zajęcia. W praktyce tak sporządzone protokoły mogą być nieczytelne dla referentów sprawy, którzy nie brali udziału w czynnościach, zwłaszcza gdy ze względu na okoliczności sprawy przeprowadzenie przeszukania (zatrzymania) rzeczy wiązało się z koniecznością zatrzymania wielu potencjalnych dowodów w sprawie i rzeczy podlegających tymczasowemu zajęciu mienia ruchomego.

Osobom zainteresowanym należy, zgodnie z art. 228 § 3 kpk, natychmiast wręczyć pokwitowanie stwierdzające, jakie przedmioty i przez kogo zostały zatrzymane. Wydaje się, że nie będzie stanowiło błędu wpisanie w protokole przeszukania lub zatrzymania rzeczy w pierwszej kolejności wszystkich zatrzymanych rzeczy mogących stanowić dowód w sprawie, a następnie dodanie wzmianki, iż podczas przeszukania zatrzymane zostały także przedmioty spisane i opisane w protokole tymczasowego zajęcia mienia ruchomego, z podaniem daty sporządzenia tego protokołu i wskazaniem osoby podejrzanej lub podejrzanego, którego mienie ruchome zajęto. Jednocześnie w protokole przeszukania lub zatrzymania rzeczy należy wpisać, które z pozycji wy-

[26] Dz.U. z 1997 r., Nr 89, poz. 555 ze zm.
[27] Z. Uniszewski, *Przeszukanie. Problematyka kryminalistyczna*, Warszawa 2000, Neriton, s. 150.
[28] K. Liszewski, D. Najmoła, K. Wiciak, *Śledztwo finansowe*, s. 16.
[29] W praktyce funkcjonariusze albo postępują zgodnie z powyższymi wskazaniami, albo ograniczają się wyłącznie do sporządzenia protokołu tymczasowego zajęcia mienia ruchomego.
[30] J. Kudrelek, R. Kwasiński, *Pisma procesowe*, s. 385 i nast.

mienionych w protokole tymczasowego zajęcia mienia zostały wydane dobrowolnie, a które ujawniono w drodze przeprowadzonego przeszukania. Wpisywanie do protokołu wszystkich rzeczy zatrzymywanych, bez względu na ich przydatność dla prowadzonego śledztwa, może sprawić, że protokół taki będzie nieczytelny, przez co utrudniona może być szybka realizacja dalszych procedur związanych z zatrzymaniem rzeczy mogących stanowić dowód w sprawie, jak sporządzenie wykazu rzeczy zatrzymanych czy dowodów w sprawie itp.

Najważniejszym elementem protokołu tymczasowego zajęcia mienia ruchomego jest właściwe opisanie zajmowanego mienia. Opis powinien pozwolić na identyfikację przedmiotów. Dokonując spisu i opisu rzeczy podczas czynności przeszukania lub zatrzymania rzeczy lub tymczasowego zajęcia mienia ruchomego, zawsze należy kierować się charakterem prowadzonej czynności, tj. dowodowym lub zabezpieczającym.

Przy zatrzymaniu pieniędzy (banknotów) w sprawie dotyczącej fałszowania środków płatniczych funkcjonariusz musi spisać każdy banknot oddzielnie, podając m.in. jego serię i numer, wartość itp. W przypadku zaś zajmowania pieniędzy w związku z tymczasowym zajęciem mienia wystarczy wpisanie łącznej sumy i wyszczególnienie ilości poszczególnych banknotów składających się na tę kwotę, np. 50 tys. zł w banknotach o nominale 200 zł – 150 sztuk, o nominale 100 zł – 200 sztuk.

Sporządzając opis zajmowanego mienia, należy (w miarę potrzeby) wzorować się na opisach stosowanych w toku oględzin śledczych i w ten sposób, w zależności od rodzaju zajmowanej rzeczy, uwzględnić w opisie takie cechy, jak: rodzaj przedmiotu, rodzaj materiału, z którego przedmiot jest wykonany, stan i rodzaj zużycia bądź uszkodzenia przedmiotu, właściwości jego budowy (zestawienie części), przeznaczenie i pochodzenie, kształt, wymiary liniowe – możliwa do ustalenia powierzchnia lub objętość, ilość lub liczba sztuk rzeczy policzalnych, barwa, ciężar, konsystencja, przeźroczystość, elastyczność, zapach, temperatura, numer, monogramy i inne cechy szczególne lub indywidualne oraz miejsce położenia w momencie ujawnienia[31].

Najwięcej trudności sprawia fachowe opisanie przedmiotów przedstawiających wartość artystyczną i historyczną. Owa trudność niejednokrotnie polega nie tylko na ustaleniu wartości, ale także na potwierdzeniu autentyczności czy też wskazaniu cech pozwalających na indywidualną identyfikację takich rzeczy. W tym zakresie prowadzący czynność, o ile zajdzie taka potrzeba, może do udziału w czynności powołać biegłego. Szczegółowy opis zajmowanych rzeczy musi pozwolić na taką identyfikację przedmiotu, aby w przypadku konieczności jego zwrotu nie został on zakwestionowany.

W przypadku dokonywania tymczasowego zajęcia mienia oprócz opisu rzeczy należy podać także jej wartość szacunkową, uwzględniając stan jej zużycia i uszkodzenia. Ustalając wartość szacunkową, można posiłkować się ogólnie dostępnymi informacjami zamieszczonymi np. w internecie, na portalach, za których pośrednictwem następuje sprzedaż różnego rodzaju rzeczy itp.

Po sporządzeniu wymaganych protokołów prowadzący czynność musi podjąć decyzję co do dalszego postępowania z zajętymi przedmiotami. Zgodnie z dyspozycją art. 228 § 1 kpk przedmioty wydane lub znalezione w toku przeszukania po dokonaniu oględzin, sporządzeniu spisu i opisu należy skonfiskować albo oddać na przechowanie osobie godnej zaufania z zaznaczeniem obowiązku przedstawienia ich na każde żą-

[31] Z. Uniszewski, *Przeszukanie. Problematyka*..., s. 195.

danie organu prowadzącego postępowanie. Zgodnie z § 215 rozporządzenia ministra sprawiedliwości z dnia 24 marca 2010 r. dotyczącego regulaminu wewnętrznego urzędowania powszechnych jednostek organizacyjnych prokuratury[32] zajęte ruchomości, a w szczególności pojazdy samochodowe, maszyny i urządzenia techniczne wymagające niezbędnej konserwacji, z wyjątkiem kosztowności, książeczek oszczędnościowych, kart płatniczych, pieniędzy i papierów wartościowych, można pozostawić u podejrzanego lub członka jego rodziny albo oddać na przechowanie osobie godnej zaufania. W przypadku podjęcia decyzji o pozostawieniu niektórych zajętych ruchomości u wyżej wymienionych osób, należy sporządzić protokół oddania rzeczy na przechowanie. Pomimo, iż przepisy prawne dają możliwość pozostawienia rzeczy u podejrzanego czy członków jego rodziny, podjęcie tej decyzji wymaga dużej rozwagi. Skoro mienie to zostało zabezpieczone, to istniała obawa jego usunięcia. Nie można zatem mieć gwarancji, że podejrzany (osoba podejrzana) nie zainicjują działań mających na celu np. upozorowanie kradzieży, i tym samym uniemożliwienie wykonania zabezpieczenia majątkowego.

Należy pamiętać, że osobie, u której dokonano tymczasowego zajęcia mienia ruchomego, należy pozostawić jeden egzemplarz protokołu, który stanowi pokwitowanie zajętych rzeczy. W przypadku zaś pozostawienia tymczasowo zajętego mienia u podejrzanego, członka jego rodziny lub osoby godnej zaufania, należy pozostawić jeden egzemplarz protokołu oddania rzeczy na przechowanie, który także stanowi pokwitowanie.

Zgodnie z § 4 art. 295 kpk tymczasowe zajęcie mienia ruchomego upada, jeżeli w ciągu 7 dni od daty jego dokonania nie zostanie wydane postanowienie o zabezpieczeniu majątkowym. Dlatego po przeprowadzeniu czynności tymczasowego zajęcia mienia ruchomego należy niezwłocznie wystąpić do prokuratora nadzorującego postępowanie przygotowawcze z wnioskiem o wydanie postanowienia o zabezpieczeniu majątkowym tak, aby we wskazanym powyżej terminie prokurator mógł to postanowienie wydać. Wniosek, o którym mowa powyżej, powinien zawierać m.in. informacje o rodzaju mienia ruchomego i miejscu, w którym się ono znajduje. Wraz z wnioskiem należy przekazać zajęte kosztowności, obiegowe pieniądze polskie i zagraniczne, inne środki płatnicze (np. karty płatnicze) oraz papiery wartościowe. Jeżeli tymczasowe zajęcie mienia ruchomego nastąpiło w trybie, o którym mowa w art. art. 217 § 4 lub 220 § 3 kpk wraz z wnioskiem o wydanie postanowienia o zabezpieczeniu majątkowym należy skierować wniosek o zatwierdzenie czynności przeszukania lub zatrzymania rzeczy[33].

O fakcie odstąpienia od wydania postanowienia o zabezpieczeniu majątkowym należy zawiadomić podejrzanego oraz osobę, u której pozostawiono zajęte ruchomości i niezwłocznie zwrócić (za pokwitowaniem) tymczasowo zajęte mienie osobie uprawnionej. Jeżeli prokurator nie powiadomi wyżej wymienionych osób o ich obowiązku, a tym samym nie zwróci mienia, obowiązek ten ciąży na organie prowadzącym postępowanie przygotowawcze.

Omawiając problematykę związaną z postępowaniem zabezpieczającym należy wspomnieć, że nie można dokonać zatrzymania rzeczy lub przeszukania w celu zabezpieczenia kar majątkowych, środków karnych o charakterze majątkowym albo rosz-

[32] Dz.U. z 2010 r., Nr 49, poz. 296.
[33] P. Starzyński, *Postępowanie zabezpieczające*..., s. 290.

czeń o naprawienie szkody, a następnie wydania postanowienia o zabezpieczeniu majątkowym, z pominięciem instytucji tymczasowego zajęcia mienia ruchomego[34]. Takie postępowanie bowiem nie rodzi obowiązku wydania postanowienia o zabezpieczeniu majątkowym w terminie 7 dni, jak ma to miejsce w przypadku tymczasowego zajęcia mienia ruchomego. Ponadto postępowanie takie z jednej strony pozwalałoby na obejście instytucji tymczasowego zajęcia mienia, którego przeprowadzenie uzależnione jest m.in. od wystąpienia obawy usunięcia mienia. Z drugiej zaś strony byłoby naruszeniem konstytucyjnie chronionego prawa własności. P. Starzyński podkreśla także, że nie można stosować zajęcia rzeczy ruchomych, które w sprawie zostały uznane za dowody rzeczowe[35]. Dotyczy to głównie przedmiotów zajmowanych zgodnie z art. 44 kk (przedmioty pochodzące bezpośrednio z przestępstwa, służące lub przeznaczone do popełnienia przestępstwa) na poczet przepadku. *Tego typu postępowania* – jak pisze Starzyński – *pozbawione są racjonalności. Bezcelowe jest stosowanie środka przymusu, mającego na celu zabezpieczenie mienia ruchomego podlegającego przepadkowi, skoro jest ono już de facto i de iure zabezpieczone w postaci dowodów rzeczowych*[36]. Inny jest bowiem cel stosowania tymczasowego zajęcia mienia, a inny zatrzymania rzeczy lub przeszukania, jeśli ma służyć odnalezieniu i zabezpieczeniu dowodów w sprawie.

W przypadku, gdy nie zachodzą przesłanki do przeprowadzenia tymczasowego zajęcia mienia ruchomego organy, którym powierzono przeprowadzenie postępowania przygotowawczego, występują do prokuratora nadzorującego z wnioskiem o wydanie postanowienia o zabezpieczeniu majątkowym. We wniosku należy wskazać wszystkie ujawnione składniki mienia ruchomego i nieruchomego należące do podejrzanego i podlegające zabezpieczeniu zgodnie z art. 291 kpk.

Ogół podejmowanych czynności o charakterze procesowym, operacyjnym i analitycznym ukierunkowanych na ustalenie składników majątkowych, w szczególności pochodzących z korzyści związanych z popełnieniem przestępstwa, potocznie określanych jest jako przeprowadzanie śledztwa finansowego[37]. Na gruncie polskich przepisów prawnych termin ś l e d z t w o f i n a n s o w e odnosi się do działań podejmowanych przez służby skarbowe. Jednak aktualnie zostało ono rozszerzone na czynności prowadzone przez organy prowadzące postępowanie przygotowawcze, które ma doprowadzić do ujawnienia mienia i jego zabezpieczenia na poczet kar i środków karnych. W jego toku podejmowane są różnego rodzaju działania o charakterze procesowym i operacyjnym. Zakres i rodzaj podejmowanych działań uzależniony jest m.in. od charakteru popełnionego przestępstwa. Dlatego w śledztwie finansowym niezwykle ważnym elementem jest nie tylko prawna analiza czynu zabronionego, lecz także analiza powiązań między członkami grupy przestępczej lub innych elementów mogących mieć wpływ na ujawnienie składników podlegających zabezpieczeniu majątkowemu.

Problematyka dotycząca prowadzenia śledztwa finansowego jest dość skomplikowana. Wbrew pozorom, śledztwo finansowe nie sprowadza się wyłącznie do dokonania sprawdzeń w dostępnych bazach. Nakład pracy i zakres podejmowanych czynności

[34] Tamże.
[35] Tamże, s. 292.
[36] Tamże.
[37] K. Liszewski, D. Najmoła, K. Wiciak, *Śledztwo finansowe*, s. 9 - 10.

jest tak samo szeroki, jak przy prowadzonych postępowaniach przygotowawczych czy działaniach o charakterze operacyjnym, ukierunkowanych na zbieranie, zabezpieczanie i utrwalanie dowodów przestępstwa. Kilka lat temu Instytut Kształcenia Służb Państwowych Zwalczających Przestępczość Zorganizowaną i Terroryzm Wyższej Szkoły Policji w Szczytnie przeprowadził wśród funkcjonariuszy Policji badania ankietowe związane ze skutecznością ujawniania i zabezpieczania mienia[38]. Na ich podstawie wykazano m.in. nienależyte wykorzystywanie dostępnych rozwiązań prawnych w tym zakresie, niewiedzę na przedmiotowy temat oraz brak znajomości baz danych i zawartych w nich informacji. Jako przyczynę tego stanu rzeczy wskazywano przede wszystkim brak szkoleń specjalistyczno-warsztatowych. W reakcji na to w 2006 r. Centralne Biuro Śledcze Komendy Głównej Policji powołało koordynatorów do spraw zabezpieczeń majątkowych i rozpoczęło dla nich cykl szkoleń. Tematyka tych szkoleń obejmowała nie tylko aspekty prawne i praktyczne związane z prowadzeniem śledztwa finansowego na gruncie polskich unormowań prawnych: uczestnicy kursu mieli możliwość zapoznania się również z regulacjami prawnymi dotyczącymi postępowania zabezpieczającego obowiązującymi w innych krajach europejskich i zdobycia w ten sposób wiedzy na temat prawnych możliwości uzyskania informacji o składnikach majątkowych zlokalizowanych poza granicami RP. Zajęcia były urozmaicane ćwiczeniami warsztatowymi, które okazały się prawdziwym sprawdzianem z nabytej wcześniej wiedzy.

Omawiając problematykę zabezpieczenia majątkowego, warto także wspomnieć o roli utworzonego w 2009 r. Krajowego Biura do Spraw Odzyskiwania Mienia, zwłaszcza w kontekście prawnych możliwości uzyskiwania informacji o składnikach majątkowych podlegających zabezpieczeniu, a zlokalizowanych poza granicami RP. W dniu 18 grudnia 2007 r. weszła w życie decyzja Rady Unii Europejskiej 2007/845/WSiSW z dnia 6 grudnia 2007 r. dotycząca współpracy pomiędzy biurami ds. odzyskiwania mienia w państwach członkowskich w zakresie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem[39]. Na mocy tej decyzji każde państwo członkowskie zostało zobowiązane (w terminie do 18 grudnia 2008 r.) do utworzenia lub wyznaczenia krajowych biur ds. odzyskiwania mienia. Miało to na celu przede wszystkim ułatwienie wykrywania i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem, które mogą być objęte nakazem zabezpieczenia, zajęcia lub konfiskaty w trakcie postępowania karnego. Zadania Krajowego Biura ds. Odzyskiwania Mienia realizuje utworzony w strukturze Biura Kryminalnego Komendy Głównej Policji Wydział ds. Odzyskiwania Mienia, który m.in.:

– *zapewnia wymianę informacji pomiędzy jednostkami organizacyjnymi Policji i innymi uprawnionymi krajowymi podmiotami oraz odpowiednimi organami państw Unii Europejskiej, dotyczących ujawniania, identyfikowania, zabezpieczania i odzyskiwania mienia pochodzącego z przestępstwa lub mającego związek z przestępstwem,*
– *współdziała z krajowymi podmiotami uprawnionymi do ujawniania, identyfikowania, zabezpieczania i odzyskiwania mienia, w szczególności z podległymi lub nadzorowanymi przez ministra właściwego do spraw wewnętrznych, ministra właściwego do spraw finansów publicznych, Ministra Sprawiedliwości oraz Prokuratora Generalnego,*

[38] Tamże, s. 9.
[39] Dz.Urz. UE L332/103 z 18.12.2007 r.

– *prowadzi „zbiór dobrych praktyk" oraz upowszechnianie rozwiązań sprzyjających ujawnianiu i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem,*
– *opracowuje propozycje zmian w przepisach prawa regulujących problematykę dotyczącą ujawniania, identyfikowania, zabezpieczania i odzyskiwania mienia pochodzącego z przestępstwa lub mającego związek z przestępstwem,*
– *prowadzi współpracę międzynarodową dotyczącą problematyki ujawniania, identyfikacji, zabezpieczania i odzyskiwania mienia pochodzącego z przestępstwa lub mającego związek z przestępstwem, w szczególności z zakresie działalności Międzyagencyjnej Sieci Odzyskiwania Mienia Camden (CARIN)*[40].

W celu ułatwienia wykrycia i identyfikacji korzyści z przestępstwa oraz innego mienia związanego z przestępstwem Biuro ds. Odzyskiwania Mienia w państwie członkowskim Unii Europejskiej może zwrócić się do swojego odpowiednika w innym państwie członkowskim z wnioskiem o przekazanie niezbędnych informacji[41].

W dniu 18 grudnia 2008 r. minister finansów, minister spraw wewnętrznych i administracji oraz minister sprawiedliwości – Prokurator Generalny podpisali deklarację współpracy w sprawie współdziałania przy stosowaniu decyzji Rady Unii Europejskiej z 6 grudnia 2007 r., a następnie zawarli porozumienie w sprawie współpracy w wykrywaniu i identyfikacji korzyści pochodzących z przestępstwa lub innego mienia związanego z przestępstwem w zakresie zadań Krajowego Biura ds. Odzyskiwania Mienia (15 września 2009). Współpraca realizowana jest na poziomie centralnym i terenowym przez następujące podmioty: Prokuratora Krajowego, Komendanta Głównego Policji, Komendanta Głównego Straży Granicznej, Komendanta-Rektora Wyższej Szkoły Policji w Szczytnie oraz komendantów szkół Policji, Dyrektora Departamentu Kontroli Skarbowej w Ministerstwie Finansów, Dyrektora Departamentu Kontroli Celno-Akcyzowej i Kontroli Gier w Ministerstwie Finansów, Dyrektora Departamentu Służby Celnej w Ministerstwie Finansów, Dyrektora Departamentu Wywiadu Skarbowego w Ministerstwie Finansów, Dyrektora Departamentu Administracji Podatkowej w Ministerstwie Finansów, Dyrektora Nadzoru Informacji Finansowej w Ministerstwie Finansów upoważnionego przez Generalnego Inspektora Informacji Finansowej do wykonywania jego zadań ustawowych, komendantów wojewódzkich (Komendanta Stołecznego) Policji, komendantów oddziałów Straży Granicznej, dyrektorów urzędów kontroli skarbowej, dyrektorów izb celnych, dyrektorów izb skarbowych, prokuratorów apelacyjnych i prokuratorów okręgowych.

Realizacja założeń porozumienia polega na wymianie informacji, efektywnej koordynacji i wykonywaniu działań podejmowanych przez wyszczególnione podmioty, opracowywaniu programów szkoleń i doskonalenia zawodowego, udzielaniu sobie wzajemnej pomocy w zakresie realizowanych przez strony czynności służbowych oraz inicjowaniu koniecznych zmian organizacyjnych i legislacyjnych[42]. W uzasadnieniu do zawartego porozumienia podkreślono, że skuteczność w wykrywaniu i identyfikacji nielegalnie uzyskanych korzyści i innego mienia pochodzącego z działalności

[40] www.policja.gov.pl. [dostęp: 15.01.2011].
[41] Dz.Urz. UE L 322/103 z 18.12.2007 r.
[42] www.policja.gov.pl [dostęp: 20.02.2011]. W przypadku, gdy organem prowadzącym postępowanie przygotowawcze jest Agencja Bezpieczeństwa Wewnętrznego, wymiana informacji następuje za pośrednictwem jednostki prokuratury nadzorującej śledztwo lub dochodzenie.

przestępczej może zostać zwiększona m.in. poprzez pełny dostęp do krajowych baz danych oraz rejestrów publicznych, tj. poprzez wymianę informacji uzyskiwanych, przetwarzanych i gromadzonych przez podmioty objęte *Porozumieniem*[43]. W tym celu w Ministerstwie Finansów i Ministerstwie Sprawiedliwości powołano Punkty Współpracy odpowiedzialne za koordynację działań i efektywne współdziałanie z Wydziałem ds. Odzyskiwania Mienia Biura Kryminalnego Komendy Głównej Policji. Zawarte porozumienie przewiduje także opracowanie programów szkoleń i doskonalenia zawodowego, a następnie ich realizację.

W celu wypełnienia postanowień zawartych w Deklaracji współpracy z 18 grudnia 2008 r. powołane zostały ponadto trzy zespoły eksperckie: zespół prawny, zespół ds. wymiany informacji i tworzenia struktur organizacyjnych oraz ds. szkoleń i Elektronicznego Systemu Odzyskiwania Mienia (ESOM). Zespół ds. szkoleń i ESOM wspierał wdrożenie do właściwych jednostek Ministerstwa Spraw Wewnętrznych i Administracji, np. Policji, Ministerstwa Sprawiedliwości i Ministerstwa Finansów, programu ESOM stanowiącego niezwykle przydatne narzędzie w pracy osób zajmujących się prowadzeniem śledztw finansowych.

Postępowanie związane z ujawnianiem składników majątkowych podlegających zabezpieczeniu majątkowemu, a zwłaszcza stanowiących korzyść uzyskaną z popełnienia przestępstwa, a przenoszonych faktycznie lub pod jakimkolwiek tytułem prawnym na osoby fizyczne, prawne i jednostki organizacyjne niemające osobowości prawnej, stanowi niezwykle trudną materię. Powyżej zaledwie zasygnalizowano problem, przy czym przedmiotowe zagadnienie ze względu na skomplikowaną materię wymaga odrębnego omówienia.

Przedstawione powyżej zadania organów, którym powierzono prowadzenie postępowań przygotowawczych w związku z postępowaniem zabezpieczającym, to zaledwie próba zwrócenia uwagi na skomplikowaną materię śledztwa finansowego, a tym samym podkreślenia wagi szkoleń, wymiany doświadczeń i poglądów. Praktyka pokazuje, że wraz z rozwojem przestępczości przestępcy, ukrywając mienie czy to legalnie uzyskane, czy pochodzące z korzyści związanych z popełnieniem przestępstwa, stosują coraz bardziej wyszukane i skomplikowane metody, które niejednokrotnie związane są z dostępem do specjalistycznej wiedzy. Dlatego też stałe podnoszenie przez funkcjonariuszy kwalifikacji i poszerzanie wiedzy z zakresu sposobu prowadzenia śledztwa finansowego, a tym samym profesjonalne podejmowanie i przeprowadzanie czynności w tym zakresie, z jednej strony stanowi jeden z elementów mających wpływ na zagwarantowanie wykonalności przyszłego orzeczenia, z drugiej zaś minimalizuje ryzyko odpowiedzialności Skarbu Państwa za niezgodne z prawem ich działania.

[43] Tamże.

Streszczenie

Pozbawienie sprawców przestępstw przychodów pochodzących z ich popełnienia należy traktować jako ważny i skuteczny element walki z przestępczością zorganizowaną. Działania takie wymagają dobrej znajomości zarówno procedur prawnych, jak i czynności związanych z ujawnianiem składników majątkowych podlegających zabezpieczeniu.

W artykule podjęto próbę przedstawienia praktycznych aspektów stosowania instytucji tymczasowego zajęcia mienia ruchomego. Poza zaprezentowaniem podstaw prawnych omawianej tematyki autorka zajęła się operacjonalizacją istniejących przepisów oraz ich implementacją na grunt praktyczny. Podjęta tematyka dotyczy istotnej kwestii działań organów procesowych prowadzących postępowania przygotowawcze. Wymaga jednak bliższego rozpoznania w celu, z jednej strony, zapewnienia skutecznego mechanizmu w walce z przestępczością, z drugiej zaś – zminimalizowania ryzyka odpowiedzialności Skarbu Państwa za niezgodne z prawem działania funkcjonariuszy.

Abstract

Depriving criminals of income coming from committed crimes should be treated as a significant and effective element of fight against organized crime. These actions require good knowledge of legal proceedings as well as practical aspects connected with revealing of property's components, which are subject to property impound. This article attempts to present the practical aspects of applied provisional seizure of property. Apart from the presentation of legal basis of the discussed subject, the author has touched the ways of making the existing legal regulations operational and their implementation on applied basis. The topic addresses an important issue related to the proceedings of trial authorities conducting preparatory proceedings. Moreover, it requires taking a closer look in order to provide effective mechanism in the fight against crime and to minimize the risk of the State Treasury's responsibility for the officers' unlawful acts.

Fabiana Fetke

Działania skierowane *przeciwko Rzeczypospolitej Polskiej* oraz działania *mogące wyrządzić szkodę Rzeczypospolitej Polskiej* w świetle regulacji art. 130 *Kodeksu karnego*[1]

W grudniu 2010 r. przed Sądem Okręgowym w Warszawie zakończył się proces obywatela Federacji Rosyjskiej Tadeusza J., oskarżonego przez Prokuraturę Apelacyjną w Warszawie o czyn z art. 130 § 1 Kodeksu karnego, tj. o branie udziału w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej. Tadeusz J. został uznany za winnego zarzucanego mu czynu i skazany na karę trzech lat pozbawienia wolności[2]. Mimo niejawnego charakteru śledztwa, jego przebieg oraz zapadły w sprawie wyrok były szeroko komentowane w prasie oraz na licznych portalach internetowych[3]. W wygłoszonej ustnie, jawnej części uzasadnienia wyroku skazującego, przedstawiając okoliczności przemawiające za uznaniem winy Tadeusza J., sędzia Igor Tuleya wskazał, iż szpieg działał na terenie województwa kujawsko-pomorskiego i mazowieckiego, począwszy od 2003 r., aż do zatrzymania przez funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego w lutym 2009 r. Śledztwo wykazało, iż w tym czasie regularnie przesyłał do Centrali GRU (Główny Zarząd Wywiadowczy Sztabu Generalnego Ministerstwa Obrony Federacji Rosyjskiej) w Moskwie zaszyfrowane informacje, wykorzystując wysoko zaawansowane urządzenia kryptograficzne. Tą samą drogą odbierał od swoich mocodawców zaszyfrowane instrukcje. Sąd nie dał wiary tłumaczeniom Tadeusza J., że sprzęt kupił na bazarze, nie wiedząc o jego rzeczywistym przeznaczeniu. Sędzia stwierdził, że oskarżony posiada *wysoką wiedzę kryptograficzną, a sprzętem posługiwał się sprawnie*. Sąd skonstatował ponadto, że J. był *istotnym ogniwem w strukturze wywiadu*. Według sędziego, *fakty z życiorysu oskarżonego* świadczą to tym, że był on tzw. uśpionym agentem, niewykonującym działań, ale pozostającym w stałej gotowości na wykonanie zlecenia[4].

---

[1] Art. 130. § 1. „Kto bierze udział w działalności obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od roku do lat 10.
§ 2. Kto, biorąc udział w obcym wywiadzie albo działając na jego rzecz, udziela temu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności na czas nie krótszy od lat 3.
§ 3. Kto, w celu udzielenia obcemu wywiadowi wiadomości określonych w § 2, gromadzi je lub przechowuje, wchodzi do systemu informatycznego w celu ich uzyskania albo zgłasza gotowość działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej, podlega karze pozbawienia wolności od 6 miesięcy do lat 8.
§ 4. Kto działalność obcego wywiadu organizuje lub nią kieruje, podlega karze pozbawienia wolności na czas nie krótszy od lat 5 albo karze 25 lat pozbawienia wolności".

[2] Orzeczenie jest prawomocne wyrokiem Sądu Apelacyjnego w Warszawie z dnia 19.05.2011 r.

[3] Jako pierwszy sprawę opisał Robert Zieliński w artykule zatytułowanym: *ABW ujęło szpiega*, opublikowanym w „Dzienniku Gazecie Prawnej" z dnia 6 stycznia 2010 r.

[4] Pisemne uzasadnienie wyroku jest niejawne, cytowane fragmenty pochodzą zaś z publikacji internetowych: www.abw.gov.pl; www.tvn24.pl/168704,0,1,rosyjski-szpieg-skazany-na-trzy-lata,wiadomosc.html; www.rp.pl/artykul/582845.html; www.wprost.pl/ar/Rosyjski-szpieg-skazny-na-trzy-lata-wiezienia/; www.wiadomosci.dziennik.pl/wydarzenia/artykul/314635,uspiony–szpieg-gru-skazany-na-trzy-lata-wiezienia.html.

Z punktu widzenia Agencji Bezpieczeństwa Wewnętrznego, służby powołanej do ochrony bezpieczeństwa wewnętrznego państwa polskiego, której jednym z zasadniczych zadań jest neutralizacja aktywności obcych służb wywiadowczych oraz rozpoznawanie, zapobieganie i wykrywanie przestępstwa szpiegostwa, niewątpliwie istotny wydaje się nie tylko sam fakt uznania Tadeusza J. za winnego zarzucanych mu czynów, ale przede wszystkim argumentacja podniesiona przez sąd w uzasadnieniu wyroku. Sąd nie miał wątpliwości, że zostały wypełnione znamiona przestępstwa szpiegostwa w formie brania udziału w działalności obcego wywiadu przeciwko RP, a polskie organa ścigania rozpoznały i udokumentowały dowodowo bezspornie, iż Tadeusz J. przynależał do struktur obcego wywiadu i, operując na terenie naszego kraju w sposób utajniony, pozostawał w gotowości do realizacji zadań na jego rzecz. O wyroku skazującym nie przesądziła natomiast okoliczność, że w wyniku działań prowadzonych przez Tadeusza J. na terenie Polski, w rzeczywistości powstała lub też mogła powstać szkoda dla państwa polskiego. Proces bowiem w istocie nie rozstrzygnął, czy działalność Tadeusza J. na terenie naszego kraju przyniosła lub mogła przynieść państwu polskiemu jakikolwiek uszczerbek. Wyrok skazujący świadczy natomiast o tym, że Sąd nie kwestionował, iż aktywność sprawcy skierowana była przeciwko RP.

Fakt uznania przez sąd Tadeusza J. za winnego szpiegostwa na rzecz Rosji stanowi, jak się wydaje, doskonały punkt wyjścia do rozważań nad wyjaśnieniem oraz interpretacją przywołanych w art. 130 *Kodeksu karnego* trudnych do zdefiniowania pojęć działania skierowane *przeciwko Rzeczypospolitej Polskiej* oraz działania mogące wyrządzić *szkodę Rzeczypospolitej Polskiej*.

W tym miejscu należałoby zauważyć, że terminy te nie są tożsame – i taka też zapewne była intencja twórców brzmienia tego przepisu. W literaturze przedmiotu podnosi się, iż z uwagi na fakt, że działanie sprawcy szpiegostwa z reguły charakteryzuje się dużą złożonością i zmiennością, ujęcie związanych z nim sytuacji w wąskie ramy przepisu ustawy stwarza określone i często niedające się usunąć trudności[5]. Być może dlatego w piśmiennictwie prawniczym trudno również znaleźć bliższe wyjaśnienia czy też interpretacje przywołanych powyżej pojęć. Z uwagi na specyfikę materii, która w dużej mierze opiera się na informacjach niejawnych oraz niewielkiej liczbie orzeczeń sądów w tego typu sprawach, brak jest odniesienia do wymienionej problematyki również w dostępnym, publikowanym orzecznictwie.

Obowiązujący aktualnie *Kodeks karny* z 1997 r.[6] wymienia kilka typów przestępstwa szpiegostwa: podstawowy, penalizujący branie udziału w działalności obcego wywiadu (art. 130 § 1), kwalifikowany, w którym okolicznością kwalifikującą jest udzielanie obcemu wywiadowi wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej (art. 130 § 2), kwalifikowany, w którym surowsza odpowiedzialność związana jest z faktem organizowania lub kierowania działalnością obcego wywiadu (art. 130 § 4), a także uprzywilejowany, polegający na gromadzeniu, przechowywaniu lub wchodzeniu do systemu informatycznego w celu uzyskania informacji, aby następnie udzielić ich obcemu wywiadowi lub też zgłaszaniu gotowości działania na rzecz obcego wywiadu przeciwko Rzeczypospolitej Polskiej (art. 130 § 3). Podej-

[5] S. Hoc, *Przestępstwa przeciwko Rzeczypospolitej Polskiej*, Opole 2003 r., Wydawnictwo Uniwersytetu Opolskiego, s. 44.

[6] *Ustawa z dnia 6 czerwca 1997 r. Kodeks karny* (Dz.U. z 1997 r., Nr 88, poz. 553 ze zm.) weszła w życie z dniem 1 września 1998 r.

mowanie działalności na rzecz obcego wywiadu w innych formach niż wymienione w art. 130 kk nie wypełni zatem znamion typu czynu zabronionego, o którym mowa w tym przepisie. Z tego względu tak istotne dla służb zajmujących się rozpoznawaniem, zapobieganiem i wykrywaniem szpiegostwa jest właściwe i wyczerpujące wskazanie, jak należy interpretować wszystkie znamiona tego przestępstwa.

O ile znamię strony podmiotowej w postaci umyślnego działania sprawcy szpiegostwa nie budzi w praktyce większych wątpliwości, to dotychczasowe doświadczenia ABW współpracującej z polskimi prokuraturami i sądami wskazują, iż problematyczne jest rozumienie tych znamion, które charakteryzują czynność sprawczą. W odniesieniu do przestępstwa szpiegostwa w typie kwalifikowanym (art. 130 § 2) oraz uprzywilejowanym (art. 130 § 3) jednym z tego typu znamion jest możliwość wyrządzenia *szkody Rzeczypospolitej Polskiej*, w przypadku pozostałych typów przestępstw natomiast, określając znamiona charakteryzujące czynność sprawczą, ustawodawca posługuje się pojęciem zachowań skierowanych *przeciwko Rzeczypospolitej Polskiej*.

Podjęcie próby przybliżenia nomenklatury, którą operuje ustawodawca, nie jest możliwe bez szerszego wyjaśnienia terminu o b c y w y w i a d, który wydaje się zasadniczym i wymagającym interpretacji w kontekście wszystkich odmian przestępstwa szpiegostwa – zarówno tam, gdzie dla bytu przestępstwa niezbędne jest prowadzenie przez sprawcę działań *przeciwko Rzeczypospolitej Polskiej*, jak i tam, gdzie jego zachowanie może wyrządzić *szkodę Rzeczypospolitej Polskiej*.

W aktualnie obowiązującym *Kodeksie karnym* termin o b c y w y w i a d nie został bliżej określony. Patrząc historycznie, definicji o b c e g o w y w i a d u nie było także we wcześniej obowiązujących regulacjach prawnych[7]. Podejmując próbę zdefiniowania pojęcia w y w i a d, należy zwrócić uwagę na fakt, iż także w literaturze przedmiotu trudno znaleźć uniwersalne źródło określające jednoznacznie ten termin. W y w i a d definiowany jest np. jako specjalne, zazwyczaj państwowe organy, których zadaniem jest nielegalne zdobywanie niedostępnych innymi sposobami informacji o politycznych, gospodarczych, wojskowych i innych działaniach kraju będącego przedmiotem zainteresowania[8]. Posiłkując się piśmiennictwem o charakterze czysto prawniczym, odnoszącym się do przedmiotowej problematyki, termin w y w i a d przedstawić można w ujęciu szerszym lub węższym. Ujęcie szersze dobrze oddaje definicja, w której w y w i a d rozumiany jest jako całokształt działalności polegającej na zbieraniu i opracowywaniu przez wyspecjalizowane służby wiadomości o innych państwach, w celu wykorzystania ich w interesie własnego państwa. W ujęciu węższym przez w y w i a d rozumie się organizację wyspecjalizowaną w zbieraniu wiadomości o innych państwach oraz opracowywaniu ich w celu wykorzystywania w sferze polityki, ekonomii i obronności na użytek własnego[9]. Różnica sprowadza się zatem do ograniczenia, w ujęciu węższym, zakresu wykorzystywania uzyskanych i opracowanych przez wywiad informacji dotyczących innego państwa jedynie do sfery polityki, obronności lub ekonomii.

---

[7] *Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny* (Dz.U. z 1969 r., Nr 13, poz. 94 ze zm.), *Rozporządzenie Prezydenta RP z dnia 11 lipca 1932 r. Kodeks karny* (Dz.U. z 1932 r., Nr 60, poz. 571), *Rozporządzenie Prezydenta RP z dnia 24 października 1934 r. o niektórych przestępstwach przeciwko bezpieczeństwu Państwa* (Dz.U. z 1934 r., Nr 94, poz. 851).

[8] *Encyklopedia szpiegostwa*, Warszawa 1995, SPAR, s. 281.

[9] W. Kubala, *Sporne zagadnienia szpiegostwa*, Zeszyty Naukowe Akademii Spraw Wewnętrznych z 1975 r., z. 10, s. 83 - 84.

Interpretując pojęcie wywiadu na użytek polskiego prawa karnego, w przeszłości wykorzystywano zazwyczaj ujęcie węższe. Jednak w ocenie autorki artykułu, z uwagi choćby na zmianę zainteresowań wywiadów światowych (do tych zainteresowań zalicza się w chwili obecnej nie tylko sferę polityczną, militarną i gospodarczą w ujęciu tradycyjnym, ale również biznes i naukę, a nawet ekologię i kulturę) ujęcie szersze wydaje się bardziej przystawać do aktualnych realiów. Szersze rozumienie pojęcia w y w i a d ma znaczenie również z tego powodu, że o ile przyjmuje się, iż szpiegostwo polityczne i militarne prowadzi się głównie wobec państw wrogich, to działania dotyczące chęci poznania tajemnic ekonomicznych i technologicznych mogą być, i często są, w rzeczywistości także wymierzone w potencjalnych sojuszników. Szpiegostwo skoncentrowane na nauce i przemyśle uprawiane przez wszystkich i w stosunku do wszystkich obecnie zyskuje na znaczeniu, gdyż rosnące współzawodnictwo ekonomiczne wymaga posiadania informacji zapewniających przewagę technologiczną nad konkurentami. Umożliwia również poznanie tych rozwiązań stosowanych w innych krajach, których wynalezienie lub udoskonalenie nie tylko zabrałoby całe lata, ale również generowałoby olbrzymie koszty finansowe[10]. Jednocześnie warto zwrócić uwagę, iż państwowe agendy wywiadowcze, wspierając rozwój gospodarczy swoich krajów, w rzeczywistości działają również na rzecz prywatnych koncernów, dostarczając im wiedzy o konkurencji zdobytej metodami właściwymi służbom wywiadowczym[11].

Próby wyjaśnienia pojęcia o b c y w y w i a d pojawiły się również w orzecznictwie polskich sądów. Podjął się tego, m.in. Sąd Najwyższy, który przyjął, iż o b c y w y w i a d to służba specjalna obcego państwa, do którego zadań należy zdobywanie wiadomości o innych państwach, a także opracowywanie tych wiadomości dla państwa, dla którego taka służba pracuje. Profesor Stanisław Hoc zaproponował, aby przyjąć, iż o b c y w y w i a d to tajna służba specjalna państwa obcego, realizująca za pomocą swoistych form i metod zadania w zakresie zdobywania wiadomości dotyczących innych państw i opracowywania ich dla organów własnego państwa[12]. Różnica w definicjach sprowadza się nie tylko do uwypuklenia przez profesora Hoca elementu „tajności" działań, ale również do podkreślenia faktu wyposażenia w y w i a d u w specyficzne instrumenty niezbędne do wykonywania przypisanych mu zadań. W literaturze pojawił się też pogląd, że dbałość o suwerenność Rzeczypospolitej Polskiej wymaga, by przez o b c y w y w i a d rozumieć nie tylko zagraniczne organa państwowe nazywane w y w i a d e m, lecz także różnorodne ogniwa i służby ochronne, policyjne, które na rzecz obcego państwa zajmują się zbieraniem danych na polskim terytorium lub na temat Polski i jej mieszkańców albo w celu wykorzystania tych danych na szkodę polskich interesów lub obywateli i osób będących pod opieką państwa polskiego[13].

W związku z tym, do uznania określonej instytucji za organizację wywiadowczą niezbędne są pełnienie przez nią funkcji wywiadowczych oraz wywiadowczy charakter jej działania. Zagadnieniem wtórnym natomiast, nierzutującym w sposób zasadniczy na kwalifikację takiej instytucji, jest jej nazwa, siedziba, struktura organizacyjna, sposób

[10] P. Schweizer, *Szpiedzy wśród przyjaciół. Jak sojusznicy wykradają Amerykanom tajemnice technologiczne*, Warszawa 1997, Książka i Wiedza, s. 20.

[11] Z. Siemiątkowski, *Wywiad a władza. Wywiad cywilny w systemie sprawowania władzy politycznej PRL*, Warszawa 2009, ASPRA-JR, s. 28.

[12] S. Hoc, *Przestępstwa przeciwko…*, s. 60 - 61.

[13] B. Zając, *W masce lub bez*, „Rzeczpospolita" z dnia 21 lutego 2000 r.

podporządkowania czy formalne źródła finansowania prowadzonej działalności. Przyjmuje się, że za obcy wywiad nie mogą być uznane zagraniczne agencje prasowe, radiowe czy telewizyjne, informacyjne służby obcych przedstawicielstw dyplomatycznych i konsularnych oraz instytucje naukowe i badawcze, które zbierają informacje w sposób jawny, wykorzystując powszechnie dostępne źródła. Nie spełniają one bowiem jednego z zasadniczych elementów definicyjnych instytucji wywiadowczej, który sprowadza się do celu, w jakim zbiera ona i opracowuje informacje dotyczące innego państwa[14]. Ta charakterystyka wymienionych wyżej instytucji nie wyklucza jednak możliwości uznania działalności poszczególnych ich pracowników za aktywność wywiadowczą, jeśli działalność ta spełnia kryteria definicyjne przyjęte dla wywiadu. Jak pokazuje praktyka, przypadki działalności wywiadowczej tego typu osób nie są odosobnione i służby kontrwywiadowcze wielokrotnie stykają się z nimi w trakcie swojej pracy.

Na marginesie warto zauważyć, że w literaturze przedmiotu można spotkać się również z poglądem, iż tradycyjne ujęcie prawa karnego w odniesieniu do przestępstwa szpiegostwa traci aktualnie na znaczeniu, nie obejmuje bowiem innych, równie niebezpiecznych, przejawów obcych aktywności charakterystycznych dla działań wywiadowczych. Uwzględniając zachodzące w świecie zmiany, działalnością noszącą wszelkie cechy tajnego wywiadu i wypełniającą podstawowe jego funkcje zajmują się obecnie na przykład organizacje terrorystyczne. Klasyczne środki, techniki i metody tajnego wywiadu stosują w swojej działalności również organizacje przestępcze. Można zaobserwować także, iż przy procederach przynoszących ogromne zyski, jak na przykład pranie brudnych pieniędzy, handel bronią lub narkotykami, wątki ideowe przenikają się z kryminalnymi. Dlatego też niektórzy autorzy postulują, by przy rozpoznawaniu działalności karteli przestępczych posiłkować się również przepisami karnymi odnoszącymi się wprost do przestępstwa szpiegostwa[15].

Jak już wcześniej wspomniano, aktualnie obowiązujące brzmienie art. 130 kk wymaga, aby wszelkie wymienione w nim formy zachowania się sprawcy biorącego udział w działalności obcego wywiadu lub współdziałającego z nim w innej formie, były zwrócone *przeciwko Rzeczypospolitej Polskiej* albo mogły spowodować *szkodę Rzeczypospolitej Polskiej*. Szersza analiza pojęcia działań skierowanych *przeciwko Rzeczypospolitej Polskiej* z powodzeniem może zostać przeprowadzona na postawie przywołanego na wstępie zapisu art. 130 § 1 kk, który ogranicza kryminalizację zachowania polegającego na braniu udziału w działalności obcego wywiadu tylko do takich jego przejawów, które skierowane są przeciwko RP. A zatem sama przynależność organizacyjna do instytucji wywiadowczej, związana choćby z wykonywaniem zadań agenta, rezydenta obcego wywiadu czy jakiejkolwiek innej funkcji w jej strukturach organizacyjnych, nie wypełnia znamion przestępstwa szpiegostwa, jeśli nie wynika z niej, iż skierowana jest przeciwko interesom RP. Powyższa konkluzja jest o tyle istotna, że przez działalność w obcym wywiadzie rozumie się również zachowania osoby dostarczającej lub przygotowującej środki techniczne wykorzystywane przez ten wywiad, a także zbierającej i opracowującej zdobyte informacje, obsługującej tzw. punkty kontaktowe lub przerzutowe oraz zaopatrującej siatkę szpiegowską w materiały i środ-

[14] A. Marek, *Kodeks karny. Komentarz*, Warszawa 2010, Wolters Kluwer Polska, s. 362.
[15] B. Zając, *W masce lub bez*, „Rzeczpospolita" z dnia 21 lutego 2000 r.

ki wykorzystywane do działalności wywiadowczej[16]. Uwzględniając złożoność metod stosowanych przez wywiady, należy stwierdzić, że uczestniczenie w ich działalności to także realizacja poleceń obcego wywiadu przez tzw. agenta wpływu (inspirowanie lub podejmowanie decyzji zgodnych z otrzymanym zadaniem)[17].

W świetle obowiązujących przepisów nie wypełnia znamion przestępstwa opisanego w art. 130 § 1 kk uczestniczenie w strukturach wywiadu państwa sojuszniczego lub neutralnego, którego działalność nie jest skierowana przeciwko państwu polskiemu[18]. W piśmiennictwie przyjmuje się, iż nie stanowi realizacji znamion typu podstawowego szpiegostwa przynależność do struktur organizacyjnych obcego wywiadu, jeśli działalność danej osoby nie jest wymierzona przeciwko RP, lecz jest prowadzona na szkodę innego państwa. Warunkiem jest to, żeby nie było to państwo sojusznicze, które zapewnia Rzeczypospolitej Polskiej wzajemność w zakresie kryminalizacji szpiegostwa polegającego na samym braniu udziału w obcym wywiadzie. W związku z tym, iż powyższa kwestia dotyczy zarówno zagrożenia bezpieczeństwa Polski, jak i ewentualnych kroków prawnych podejmowanych przez nasze organa ścigania i sądy, oficjalne gwarancje ścigania przez odpowiednie organy państw sojuszniczych powinny być dostatecznie jasno promulgowane w naszym kraju, tj. ogłoszone w postaci jawnych i opublikowanych protokołów dodatkowych do istniejących i ratyfikowanych umów. Dopiero wtedy będą mogły mieć zastosowanie przepisy art. 138 § 2 kk[19].

W praktyce nadal pozostaje nierozwiązany problem państw, z którymi Rzeczpospolita Polska nie zawarła sojuszy politycznych lub militarnych. Należy podkreślić, iż istotą suwerennej władzy jest faktyczna kontrola tego, co dzieje się na podległym jej terytorium. Wychodząc z tego założenia, państwo trzecie, niesojusznicze, może mieć wobec RP uzasadnione pretensje, jeśli zdobędzie dowody, że działalność wywiadowcza innego kraju przeciwko jego interesom prowadzona jest na polskim terytorium, albo że jest przez polskie władze tolerowana. Wydaje się, iż państwo takie może mieć rzeczywiste podstawy do uznania stwierdzonego działania (lub zaniechania) naszego kraju jako co najmniej nieprzyjazne – z wszelkimi wypływającymi z tego faktu konsekwencjami. W ocenie autorki artykułu, w analizowanej sytuacji można rozważyć zakwalifikowanie takiej działalności obcego wywiadu na naszym terytorium (nawet jeżeli nie jest ona wprost skierowana przeciwko interesom Rzeczypospolitej Polskiej lub państw sojuszniczych) jako związanej z możliwą utratą prestiżu państwa, a niekiedy i z innymi, dalej idącymi reperkusjami. W związku z powyższym, nie wydaje się nadużyciem traktowanie takiej działalności jako skierowanej również przeciwko Rzeczypospolitej Polskiej.

Uwzględniając wcześniejsze uwagi na temat roli i zadań stawianych obecnie przed służbami wywiadowczymi, w szczególności w odniesieniu do działań podejmowanych wobec państw sojuszniczych, widać wyraźnie, jak niejednoznaczny, a w związku z tym trudny do zdefiniowania, jest w stosunku do potencjalnego sprawcy uczestniczącego

[16] M. Fleming, J. Wojciechowska, *Zbrodnie wojenne. Przestępstwa przeciwko pokojowi, państwu i obronności*, rozdz. XVI, XVII i XVIII *Kodeksu karnego z komentarzem*, Warszawa 1999, C.H. Beck, s. 142.

[17] S. Hoc, *Szpiegostwo w nowym kodeksie karnym*, „Wojskowy Przegląd Prawniczy" 1998, nr 1/2, s. 25.

[18] A. Marek, *Kodeks karny* ..., s. 362.

[19] Art. 138 § 2. *Przepisy art. 127, 128, 130 oraz 131 stosuje się odpowiednio, jeżeli czyn zabroniony popełniono na szkodę państwa sojuszniczego, a państwo to zapewnia wzajemność.*

w działalności obcego wywiadu element tzw. działań skierowanych *przeciwko Rzeczypospolitej Polskiej*.

Równie złożoną kwestią jest określenie znamion opisujących czynność wykonawczą w postaci działań mogących wyrządzić szkodę Rzeczypospolitej Polskiej, o których mowa w art. 130 § 2 i 3 kk, w odniesieniu do czynu polegającego na gromadzeniu wiadomości, których przekazanie może wyrządzić szkodę Rzeczypospolitej Polskiej, lub na ich przechowywaniu albo włączaniu się do systemu informatycznego w celu ich uzyskania. Elementem łączącym wymienione typy przestępstw jest możliwość wyrządzenia szkody państwu polskiemu.

Powszechnie przyjmuje się, że jeśli określony termin nie został zdefiniowany w akcie normatywnym lub gałęzi prawa, należy posługiwać się jego definicją zawartą w innych przepisach regulujących daną instytucję prawną. Tak wypowiedział się Sąd Najwyższy m.in. w uchwale z dnia 29 stycznia 2004 r.[20]: *Definicji legalnej należy szukać w pierwszej kolejności w akcie prawnym zawierającym interpretowane wyrażenie. Jeżeli brak definicji w danym akcie, to należy sprawdzić, czy definicja taka występuje w innej ustawie uznanej za podstawową dla danej dziedziny.* Z uwagi na to, że ani przepisy prawa karnego procesowego, ani prawa karnego materialnego, nie zawierają definicji s z k o d y, pojęcie to na gruncie prawa karnego należy rozumieć tak, jak na gruncie prawa cywilnego. Odstąpienie od definicji s z k o d y funkcjonującej w prawie cywilnym byłoby bowiem dopuszczalne, gdyby ustawodawca w przepisach prawa karnego materialnego bądź procesowego zawarł definicję odmienną od cywilistycznej. Nie budzi zatem wątpliwości okoliczność, że na gruncie prawa karnego materialnego, w przypadkach niektórych kategorii przestępstw (np. przeciwko obrotowi gospodarczemu), s z k o d a jest interpretowana tak, jak na gruncie prawa cywilnego. W tym miejscu należy zaznaczyć, iż wprawdzie *Kodeks cywilny*[21] również nie zawiera wprost definicji s z k o d y, niemniej jednak zagadnienie to doczekało się wielu obszernych komentarzy w orzecznictwie i piśmiennictwie.

W związku z powyższym, pod pojęciem s z k o d y na gruncie prawa karnego – podobnie jak na gruncie prawa cywlinego – należy rozumieć uszczerbek (ubytek, stratę) w sferze prawnie chronionych dóbr (interesów), określany przez porównanie stanu dóbr, jaki już istniał, i jaki w normalnych warunkach mógłby powstać, ze stanem, jaki powstał w granicach normalnych następstw w wyniku zdarzenia wywołującego zmianę w dotychczasowym porządku, z którym prawo łączy odpowiedzialność odszkodowawczą (w odniesieniu do prawa karnego zdarzeniem takim jest przestępstwo). S z k o d a w tym znaczeniu obejmuje zarówno poniesione przez pokrzywdzonego straty (*damnum emergens*), jak i utracone korzyści (*lucrum cessans*). W ślad za prawem cywilnym należy przyjąć, że s z k o d a w rozumieniu prawa karnego może być zarówno szkodą materialną, jak i niematerialną (niemajątkową).

Z punktu widzenia znamienia s z k o d y, zasadnicze – w kontekście zapisów art. 130 kk – jest przede wszystkim zdefiniowanie pojęcia w i a d o m o ś c i, których przekazanie obcemu wywiadowi, albo których gromadzenie i przechowywanie lub włączenie się do sieci komputerowej w celu ich uzyskania, może wyrządzić szkodę Rzeczypospolitej Polskiej. Konstrukcja przywołanych zapisów *Kodeksu karnego* sprawia, iż do zaistnienia opisanych przestępstw nie jest w rzeczywistości konieczne wy-

[20] Uchwała Sądu Najwyższego z dnia 29 stycznia 2004 r. I KZP 39/03, OSNKW 2004, z. 2, poz. 13.
[21] *Ustawa z dnia 23 kwietnia 1964 r. Kodeks cywilny* (Dz.U. z 1964 r., Nr 16, poz. 93 ze zm.).

rządzenie szkody państwu polskiemu. Wystarczy natomiast stwierdzenie, że o ile wiadomości te znajdą się w posiadaniu obcego wywiadu, szkoda może zostać wyrządzona. Z punktu widzenia znamion typu czynów zabronionych, o których mowa w art. 130 kk, nie ma również znaczenia wielkość ewentualnej szkody, jaka może wyniknąć dla Rzeczypospolitej Polskiej z przekazania wiadomości stanowiących przedmiot tych przestępstw.

W tym miejscu należy zwrócić uwagę, iż zapis *Kodeksu karnego* jest daleko szerszy niż termin, którym posługuje się *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych*[22], w części określającej kryteria ich klasyfikowania. Artykuł 5 cytowanej ustawy określa bowiem, iż informacjom niejawnym nadaje się określoną klauzulę („ściśle tajne", „tajne", „poufne") w przypadku, gdy ich nieuprawnione ujawninie spowoduje (a nie jedynie może spowodować) odpowiednio – „wyjątkowo poważną", „poważną" albo po prostu „szkodę" dla Rzeczypospolitej Polskiej. Na marginesie warto podkreślić, iż w doktrynie prawniczej również w odniesieniu do przytoczonych zapisów ustawy brak bliższej definicji tych pojęć, co może powodować, iż te same informacje mogą mieć różne klauzule – w zależności od subiektywnej oceny i interpretacji osoby je nadającej.

Aktualnie obowiązujący *Kodeks karny* odchodzi od przyjmowanej na podstawie art. 124 § 2 *Kodeksu karnego* z 1969 r.[23] szerokiej wykładni pojęcia w i a d o m o ś c i, obejmującej wszelkie informacje, nawet łatwe do sprawdzenia lub znane szerszemu kręgowi osób, dotyczące wszelkich faktów przyszłych, teraźniejszych lub mających nastąpić w przyszłości[24]. Z drugiej jednak strony ustawodawca dopuszcza, by wystąpiło jedynie narażenie na szkodę interesów RP. Dlatego też dla realizacji znamion przestępstwa szpiegostwa opisanego w przywołanych przepisach konieczne jest wykazanie, że w konkretnym stanie faktycznym, w odniesieniu do ustalonego zakresu informacji stanowiących przedmiot działania sprawcy, w rzeczywistości istniała realna możliwość wyrządzenia szkody państwu polskiemu[25], a przekazane bądź gromadzone w celu przekazania informacje mogły stanowić zagrożenie lub naruszenie interesów zewnętrznych lub wewnętrznych RP, ze względu na zawarty w nich, przydatny obcemu wywiadowi, zasób wiedzy.

Należy wskazać, iż wiadomości będące przedmiotem przestępstw określonych w art. 130 kk nie muszą nosić cech niejawności; warunkiem sine qua non dla bytu przestępstwa szpiegostwa nie jest również to, aby wiadomości te cechowała autentyczność[26]. Autentyczność oraz aktualność wiadomości może mieć natomiast znaczenie dla ustalenia, czy w momencie działania sprawcy także nieaktualne lub nieautentyczne wiadomości mogą wyrządzić naszemu krajowi szkodę. Nie stanowi bowiem realizacji znamion opisywanego przestępstwa zachowanie polegające na działaniu na rzecz obcego wywiadu i udzielaniu mu wiadomości nieistotnych, irrelewantnych z punktu widzenia zewnętrznych i wewnętrznych interesów RP, a więc takich, które nie mogą, nawet po opracowaniu ich przez organizację wywiadowczą, wyrządzić szkody państwu polskiemu.

---

[22] *Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych* (Dz.U. z 2010 r., Nr 182, poz. 1228).
[23] *Ustawa z dnia 19 kwietnia 1969 r. Kodeks karny* (Dz.U. z 1969 r., Nr 13, poz. 94 ze zm.).
[24] A. Marek, *Kodeks karny* ..., s. 396.
[25] S. Hoc, *Przestępstwa przeciwko* …, s. 69.
[26] S. Hoc, *Szpiegostwo w nowym* …, „Wojskowy Przegląd Prawniczy" 1998, nr 1/2, s. 25.

Takie ujęcie przedstawionej problematyki sprawia, że ocena rzeczywistych możliwości narażenia na szkodę interesów państwa polskiego jest bardzo skomplikowana lub w wielu przypadkach wręcz niemożliwa do sporządzenia. Trudno jest jednoznacznie stwierdzić, kiedy i w jakich okolicznościach obcy wywiad (w tym rozumieniu także służby państw sojuszniczych, partnerskich) użyje wiadomości na szkodę RP. Należy przy tym zdawać sobie sprawę, iż dla służb wywiadowczych, których głównym celem i zasadniczym zdaniem jest zdobywanie wszelkich informacji, nie ma w istocie wiadomości nieważnych, a wszystko zależy od tego, w jaki sposób będą one wykorzystane w przyszłości. To, co jest bezużyteczne dla jednej osoby, może być szczególnie cenne dla innej, która posiada właściwe rozeznanie sytuacji. W związku z tym, w niektórych przypadkach równie wartościowe mogą okazać się zarówno dokumenty niejawne, jak i materiały pochodzące z otwartych, legalnych źródeł[27]. Odpowiednio przeanalizowane i zestawione z innymi danymi mogą być we właściwym czasie użyte na szkodę państwa, z którego pochodziły. Doskonale ilustruje to przykład uzyskiwania przez obce służby informacji z pozoru bezwartościowych, dotyczących spraw prywatnych poszczególnych osób, ich kontaktów i zainteresowań, zwłaszcza w sytuacji, gdy tego typu osoby pełnią lub też będą pełnić w przyszłości odpowiedzialne funkcje w organach władzy, administracji i organizacjach społeczno-politycznych. Dane takie mogą posłużyć nie tylko jako materiały nacisku (w przypadku np. informacji i materiałów o charakterze kompromitującym), lecz także mogą pozwolić na pełniejsze poznanie potencjalnego celu werbunku (w sytuacji uzyskania informacji o trudnej sytuacji finansowej czy rodzinnej).

W przypadku kryminalizowanych w art. 130 *Kodeksu karnego* przestępstw o charakterze szpiegowskim, pod pojęciem s z k o d y należy zatem rozumieć uszczerbek (również ten potencjalny) w sferze prawnie chronionych dóbr (interesów) poszkodowanego, którym w tym wypadku jest państwo polskie. Narażone na ewentualną szkodę są zaś te elementy, które składają się na jego bezpieczeństwo (w rozumieniu politycznej, suwerennej, terytorialnej i obligatoryjnej organizacji społeczeństwa) oraz na bezpieczeństwo jego obywateli, a więc nie tylko niepodległość, integralność terytorialna, gwarancja zachowania ustroju konstytucyjnego, ale również prestiż na arenie międzynarodowej oraz np. stabilizacja gospodarcza. Powyższe ma znaczenie zwłaszcza obecnie, gdy modyfikacji uległy kierunki zainteresowań wywiadów. Pojęcie s z k o d y w znaczeniu opisywanym w art. 130 kk obejmuje zarówno potencjalne, możliwe do poniesienia przez pokrzywdzonego, tj. państwo polskie, straty, jak i ewentualne utracone korzyści (tak w sferze materialnej, jak i niematerialnej). Kalkulacja rzeczywistych strat i potencjalnych szkód jest szczególnie skomplikowana. O ile bowiem można oszacować uszczerbki powstałe lub mogące powstać w wyniku szpiegostwa gospodarczego (np. w związku z bezprawnym pozyskaniem przez obce służby nowatorskich technologii), to utratę bądź możliwość utraty albo osłabienie prestiżu i zaufania na arenie międzynarodowej stwierdzić niełatwo. Uszczerbki tego typu należą do bardzo trudno definiowalnych. Ocenę szkody, jak również możliwości narażenia na szkodę, dodatkowo komplikuje fakt, że niezwykle trudno jest rozstrzygnąć, kiedy i w jakich okolicznościach dana informacja, czy też pozyskany przez obce służby materiał, zostaną wykorzystane na szkodę naszego kraju.

[27] Z. Siemiątkowski, *Wywiad a władza*…, s. 33.

Oceniając zatem konkretne, ujawnione w wyniku pracy ABW lub innych służb powołanych do ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, zachowania osób wskazujące na podejrzenie prowadzenia przez nie działalności skierowanej *przeciwko Rzeczypospolitej Polskiej* albo *na szkodę Rzeczypospolitej Polskiej*, należy w szczególności pamiętać, iż zakres aktywności tych osób, podobnie jak zakres zainteresowań służb wywiadowczych wszystkich bez wyjątku państw, nie jest w istocie ograniczony, a ponadto podlega ciągłej ewaluacji. Charakter zainteresowań oraz tematyka przyciągająca uwagę obcych służb to zbiór otwarty, w praktyce często niemożliwy do precyzyjnego zdefiniowania dla służb kontrwywiadowczych. Ewentualna szkoda (rzeczywista lub potencjalna) związana z przedsiębraną działalnością szpiegowską, jest zaś trudna do dokładnego oszacowania. Tym bardziej, że, jak już wcześniej wielokrotnie podkreślono, dla służb wywiadowczych nie ma w istocie informacji bez znaczenia.

Jednocześnie należy mieć nadzieję, że na przyszłe rozstrzygnięcia w sprawach o szpiegostwo, jak również na ewentualne decyzje sądów w odniesieniu do możliwości zastosowania przez polskie służby konkretnych metod pracy operacyjnej, w szczególności kontroli operacyjnej, w sprawach prowadzonych w kierunku podejrzenia popełnienia tego czynu, będzie miało wpływ przywołane na wstępie orzeczenie, które zapadło w grudniu 2010 r. wobec Tadeusza J. Za branie udziału w działalności obcego wywiadu polski sąd uznał nie wykonywanie żadnych aktywnych przedsięwzięć skierowanych wprost przeciwko Rzeczypospolitej Polskiej, ale pozostawanie w stałej gotowości do przyjęcia zlecenia. Mimo, że w analizowanej sytuacji nie można było mówić o wystąpieniu rzeczywistej czy też potencjalnej szkody dla państwa Polskiego, jak również szczególnie trudno było wykazać wypełnienie znamienia czynu zabronionego w rozumieniu zachowania skierowanego *przeciwko Rzeczypospolitej Polskiej*, niemożliwe dla Sądu było jednak przyjęcie tezy, że opisana działalność osoby bezsprzecznie powiązanej z obcym (w tym wypadku rosyjskim) wywiadem, prowadzona na terytorium naszego kraju w sposób utajniony, bez wiedzy i zgody strony polskiej, nie jest skierowana przeciwko Rzeczypospolitej Polskiej lub też skierowana jest tylko i wyłącznie przeciwko innym państwom i w rzeczywistości w żaden sposób nie ma negatywnego przełożenia na polskie interesy.

Potrzeba zmiany postrzegania przez polskie sądy pojęć działań *skierowanych przeciwko RP* oraz *mogących wyrządzić szkodę RP* jest dla Agencji Bezpieczeństwa Wewnętrznego, jako dla służby powołanej do ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego, szczególnie istotna. Nie jest możliwe bowiem tolerowanie na polskim terytorium ujawnionej działalności podmiotów ewidentnie związanych z obcym wywiadem, bez wiedzy i zgody władz naszego kraju[28].

[28] Rozważania na temat konieczności zmian legislacyjnych w odniesieniu do art. 130 *Kodeksu karnego* autorka artykułu zawarła w publikacji: *Szpiegostwo w polskim prawie karnym – czy istnieje potrzeba zmian legislacyjnych?*, „Przegląd Bezpieczeństwa Wewnętrznego" 2010, nr 3, s. 91 - 100.

Streszczenie

Artykuł zawiera rozważania dotyczące interpretacji przywołanych w art. 130 *Kodeksu karnego* pojęć działania skierowane *przeciwko Rzeczpospolitej Polskiej* oraz działania *mogące wyrządzić szkodę Rzeczpospolitej Polskiej*. Punktem wyjścia do przeprowadzenia powyższej analizy jest skazanie w grudniu 2010 r. przez Sąd Okręgowy w Warszawie Tadeusza J., oskarżonego przez Prokuraturę Apelacyjną w Warszawie o czyn z art. 130 § 1 *Kodeksu karnego*, tj. obranie udziału w działalności obcego wywiadu przeciwko Rzeczpospolitej Polskiej. Wskazane orzeczenie, w szczególności w zakresie interpretacji przez Sąd znamion działań „przeciwko" i „na szkodę" Rzeczpospolitej Polskiej, może mieć niebagatelny wpływ nie tylko na przyszłe rozstrzygnięcia sądów w sprawach o szpiegostwo, ale również na decyzje tego organu w odniesieniu do możliwości zastosowania w konkretnych sprawach np. kontroli operacyjnej.

Abstract

The paper contains considerations regarding the interpretation of some notions of Article 130 of the Penal Code: activities directed "against the Republic of Poland" and activities that "may be detrimental to the Republic of Poland". The starting point to conduct the analysis is the fact that, in December 2010, the District Court in Warsaw announced sentence to Tadeusz J. who had been charged by the Appeal Court in Warsaw with violation of Article 130 Paragraph 1 of the Penal Code, that is, participating in activities of foreign intelligence service against the Republic of Poland. The mentioned ruling, especially as regards the Court's interpretation of sings of activities 'against' and 'to the detriment' of the Republic of Poland, may considerably influence court verdicts in espionage cases in the future, as well as decisions thereof regarding the possibility of applying in certain cases operational control.

III
TERRORYZM

Wojciech Filipkowski
Ryszard Lonca

Analiza zamachów samobójczych w aspekcie kryminologicznym i prawnym. Część III

IV. Wybrane kwestie prawne

W związku z tym, że terroryzm samobójczy jest wynikiem działania grupowego (zorganizowanego), eksperci, m.in. budzący kontrowersje dr R. Gunaratna z Institute of Defence and Strategic Studies (Singapur), sugerują **potrzebę spenalizowania** poszczególnych funkcji pełnionych przez członków grupy terrorystycznej. Na podstawie przytoczonych wyżej analiz można postawić tezę, iż w rzeczywistości grupa terrorystyczna specjalizująca się w atakach samobójczych z zasady składa się ze struktury wspierającej oraz realizacyjnej i działa na zasadzie tzw. podziału zadań „9+4". W świetle badań R. Gunaratny, w gestii komórki wspierającej taką grupę jest dziewięć obszarów działania: propaganda terrorystyczna, rekrutacja nowych członków do grupy, organizowanie jej zaplecza finansowego, organizowanie zaopatrzenia w niezbędne środki (materiały wybuchowe, dokumenty legalizacyjne i inne), zapewnienie transportu, organizowanie bezpiecznego schronienia, realizacja niezbędnego szkolenia, zapewnienie łączności oraz tworzenie fałszywych tożsamości dla członków grupy. W obszarze działania komórki realizacyjnej znajduje się: wstępna obserwacja i rekonesans celu ataku, symulacja lub trening zamachu, końcowe rozpoznanie jego celu i otoczenia oraz dokonanie ataku. R. Gunaratna twierdzi, że każda wyżej wymieniona czynność wykonywana przez członka grupy terrorystycznej powinna być uznawana za oddzielne przestępstwo, aby w sposób skuteczny móc walczyć z tym zjawiskiem poprzez karanie i izolowanie poszczególnych członków[1].

Interesującą opinię na ten temat przedstawił w marcu 2006 r. A. Spataro, specjalny prokurator koordynujący walkę z terroryzmem islamskim we Włoszech. W jego ocenie, udowodnić terroryzm, gdy nastąpi atak i mamy sprawcę, jest łatwo. Całkowicie inaczej przedstawia się problem z terroryzmem samobójczym, gdyż sprawcy ataku nie można przesłuchać, a tym bardziej osądzić. Z tego powodu – uważa Spataro – w zainteresowaniu aparatu ścigania i wymiaru sprawiedliwości pozostają tylko ci, którzy zajmują się logistyką, rekrutacją, zbieraniem funduszy czy fałszowaniem dokumentów. Jednak, jego zdaniem, udowodnienie, że dana działalność lub czyn były przygotowaniem do zamachu, jest procesem skomplikowanym i trudnym. W praktyce bardzo ciężko jest udowodnić podejrzanemu przynależność do grupy terrorystycznej, jeśli sfałszował dokument, którym następnie posłużył się zamachowiec-samobójca. Ponadto, jeśli podejrzanym jest islamista, nigdy nie ujawni informacji o swoich powiązaniach, tłumacząc się, że nie może sprzeniewierzyć się swojej wierze.

Na gruncie polskiego systemu prawa odpowiednia kwalifikacja prawna zamachu terrorystycznego nie jest sprawą prostą. Zależy od zakładanego celu, który miał być lub został osiągnięty przez zamachowców oraz od sposobu ich działania (np. użytych środ-

[1] Referat R. Gunaratny pt. *Podział struktury organizacyjnej grupy terrorystycznej ze względu na zadania*, wygłoszony 9 grudnia 2005 r. w siedzibie szwajcarskiej Policji Federalnej w Bernie.

ków). Można rozpatrywać kilka wariantów dotyczących odpowiedzialności poszczególnych osób zaangażowanych w przeprowadzenie zamachu[2]. Już to pierwsze zastrzeżenie wskazuje na konieczność rozpatrywania kwestii odpowiedzialności za **udział w zorganizowanej grupie** lub **związku mającym na celu popełnienie przestępstwa o charakterze terrorystycznym** (art. 258 § 2 kk). Należy jednak pamiętać, że współczesne ugrupowania terrorystyczne mają różne formy organizacyjne[3]. Poza tym, dochodzą kwestie kwalifikacji przestępstw z przepisu art. 115 § 20 kk.

Tab. 1. Zestawienie zadań terrorystycznych i odpowiadających im kwalifikacji prawnych.

l.p.	Opis zadania	Kwalifikacja prawna	Czy spełnia wymogi art. 115 §20 – przestępstwa o charakterze terrorystycznym
Komórka wspierająca			
1.	propaganda terrorystyczna	art. 119 §2 kodeksu karnego art. 190 §1 kodeksu karnego art. 255 §1 kodeksu karnego art. 255 §2 kodeksu karnego art. 255 §3 kodeksu karnego art. 256 kodeksu karnego	tak nie (do 2 lat pozbawienia wolności) nie (do 2 lat pozbawienia wolności) nie (do 3 lat pozbawienia wolności) nie (do 1 roku pozbawienia wolności) nie (do 2 lat pozbawienia wolności)
2.	rekrutacja nowych członków do grupy	art. 18 §2 w związku z art. 258 §2 kodeksu karnego art. 18 §3 w związku z art. 258 §2 kodeksu karnego art. 151 kodeksu karnego	tak tak tak
3.	organizacja zaplecza finansowego grupy terrorystycznej	art. 18 §3 w związku z art. 258 §2 kodeksu karnego art. 165a kodeksu karnego	tak tak
4.	organizacja zaopatrzenia w niezbędne środki	art. 18 §3 w związku z art. 258 §2 kodeksu karnego art. 167 §1 kodeksu karnego art. 171 §1 kodeksu karnego art. 184 §1 i 2 kodeksu karnego art. 263 §1 - 3 kodeksu karnego	tak tak tak tak tak (oprócz §3 – do 2 lat pozbawienia wolności
5.	zapewnienie transportu	art. 18 §3 w związku z art. 258 §2 kodeksu karnego art. 264 §2 kodeksu karnego art. 264 §3 kodeksu karnego	tak nie (do 3 lat pozbawienia wolności) tak
6.	organizacja bezpiecznego schronienia	art. 18 §3 w związku z art. 258 §2 kodeksu karnego art. 239 §1 kodeksu karnego art. 264a kodeksu karnego	tak tak tak
7.	realizacja niezbędnego szkolenia	art. 18 §3 w związku z art. 258 §2 kodeksu karnego	tak
8.	zapewnienie łączności	art. 18 §3 w związku z art. 258 §2 kodeksu karnego	tak
9.	tworzenie fałszywych tożsamości dla członków grupy	art. 18 §3 w związku z art. 258 §2 kodeksu karnego art. 270 kodeksu karnego art. 275 kodeksu karnego	tak tak nie (do 2 lat pozbawienia wolności)

[2] W analizie aspektów prawnych użyta zostanie koncepcja R. Gunaratny dotycząca podziału zadań pomiędzy komórki terrorystyczne.

[3] Szerzej na ten temat zob. W. Filipkowski, R. Lonca, *Zorganizowane grupy o charakterze terrorystycznym. Studium kryminologiczno-prawne*, „Wojskowy Przegląd Prawniczy" 2006, nr 4, s. 33 i nast.

Komórka realizująca			
1.	wstępna obserwacja i rekonesans celu ataku	art. 16 kodeksu karnego	zależne od zakwalifikowania przygotowywanego, usiłowanego i dokonanego czynu zabronionego (zamachu terrorystycznego)
2.	symulacja lub trening zamachu	art. 16 kodeksu karnego	
3.	końcowe rozpoznanie celu ataku i jego otoczenia	art. 16 kodeksu karnego	
4.	realizacja ataku	art. 13 i 18 §1 kodeksu karnego	
	wybrane przykłady czynów zabronionych:	art. 127 §1 kodeksu karnego	nie (do 3 lat pozbawienia wolności)
		art. 128 §2 kodeksu karnego	tak
		art. 140 §3 kodeksu karnego	nie (do 3 lat pozbawienia wolności)
		art. 151 kodeksu karnego	tak
		art. 168 kodeksu karnego	nie (do 3 lat pozbawienia wolności)
		art. 175 kodeksu karnego	nie (do 3 lat pozbawienia wolności)
		art. 252 §3 kodeksu karnego	nie (do 3 lat pozbawienia wolności)

Zadania wskazane w powyższym zestawieniu mogą być wykonywane oddzielnie lub wspólnie przez poszczególnych członków, ewentualnie jedna osoba wykonuje kilka z nich. Elementem łączącym wszystkie osoby jest **podział zadań** w dążeniu do osiągnięcia zamierzonego, wspólnego celu. Nie jest wymagane, aby każda z osób znała wszystkich lub część pozostałych; jest to wręcz niebezpieczne dla realizacji zadania w przypadku ujawnienia niektórych członków. Tego typu grupy nie powinny mieć struktury hierarchicznej (raczej zdecentralizowaną), gdyż czyni je to łatwiejszymi do infiltracji i rozbicia. Każdy z członków zna swoje zadanie i je wykonuje. Realizacja cząstkowego zadania przez jedną osobę często warunkuje możliwość rozpoczęcia wykonywania kolejnego przez inną.

Ważna jest świadomość pojedynczego sprawcy, że jest częścią grupy osób, których wspólnym celem jest dokonanie jednego lub więcej zamachów (tzn. przestępstw o charakterze terrorystycznym). Bezpośredni wykonawca dąży do realizacji pojedynczego ataku, celem pozostałych osób jest przygotowanie go tak szybko, jak to tylko będzie możliwe. Biorąc pod uwagę fakt, iż w przypadku ataków terrorystycznych istnieje duża rotacja samych wykonawców, jest to zrozumiałe. Inaczej rzecz się ma z członkami komórki wspierającej (częścią osób składających się na komórkę realizacyjną), którzy w sposób ciągły przygotowują kolejne zamachy, poszukując jednocześnie ich wykonawców[4]. W związku z tym, skład grupy jest zmienny.

Uwzględniając jednak dorobek orzecznictwa i doktryny odnoszący się do art. 258 kk, można zastanawiać się nad ich adekwatnością do funkcjonowania grup terrorystycznych, w tym samobójczych. Czy przytaczane we wcześniejszych częściach opracowania przykłady dałyby podstawę do przyjęcia kwalifikacji prawnej właśnie z art. 258 kk nawet, jeśli nie można by było stwierdzić terrorystycznego charakteru przestępstwa w rozumieniu art. 115 § 20 tego kodeksu? Część z nich mogłaby zostać uznana za którąś z form stadialnych lub zjawiskowych popełnienia czynu zabronio-

[4] Inaczej sprawa może wyglądać w przypadku grup powstających oddolnie. Osoby tworzące grupę we własnym zakresie zajmują się przede wszystkim przygotowaniem i realizacją jednego ataku (grupa realizacyjna) przy wsparciu ideologicznym i logistycznym z zewnątrz (np. szkolenia, dostarczanie materiałów wybuchowych czy mechanizmów zapalających).

nego w konfiguracji wieloosobowej, ale nie za udział w zorganizowanej grupie mającej na celu popełnienie przestępstwa o charakterze terrorystycznym[5]. Dlatego też powraca problem spenalizowania udziału w grupie terrorystycznej w sposób niezależny od przepisów zwalczających przestępczość zorganizowaną[6]. Pozostawienie obecnego stanu prawnego może prowadzić do trudności z zastosowaniem w Polsce przepisów o charakterze antyterrorystycznym w celu zwalczania terroryzmu[7], ale też przepisów dotyczących pomocy prawnej w sprawach karnych. W związku z tym, powstaje problem konieczności analizy ustawodawstwa antyterrorystycznego i jego zakresu[8].

1. Odpowiedzialność terrorysty-samobójcy

W przypadku udanego zamachu sprawca ginie i rozpatrywanie jego odpowiedzialności mija się z celem. Jak uczy doświadczenie, zdarzają się jednak sytuacje, w których nie dochodzi do przeprowadzenia skutecznego ataku. Może to być następstwo np. wadliwego mechanizmu lub materiału wybuchowego, ewentualnie skutecznych działań organów ścigania, które rozbroiły zamachowca zanim zdetonował ładunek.

W chwili, gdy terrorysta-samobójca oddala się od osoby (lub osób), która go przetransportowała w pobliże miejsca dokonania zamachu – takie zachowanie można uznać za **usiłowanie** dokonania czynu zabronionego (art. 13 § 1 kk). Przemawia za tym fakt, iż w zasadzie w każdej chwili może dojść do detonacji. W sytuacji, gdy nie jest możliwe dojście do celu lub sprawca zostaje wykryty przez inne osoby (w tym np. przez pracowników ochrony, żołnierzy, funkcjonariuszy organów ścigania lub innych służb), można przejść do realizacji planu awaryjnego lub postępować według zasady „im więcej ofiar tym lepiej" i zdetonować ładunek natychmiast. Po drugie, zawsze istnieje niebezpieczeństwo, że ładunek może zostać odpalony drogą radiową przez inną osobę. Ponadto, wytworzone metodami domowymi ładunki wybuchowe są bardzo niestabilne i mogą spowodować poważne, bezpośrednie zagrożenie dla życia i zdrowia osób oraz zniszczenie mienia.

Można też pokusić się o przeanalizowanie przypadku zastosowania konstrukcji tzw. usiłowania nieudolnego (art. 13 § 2 kk). Dużą popularnością „cieszą się" w interne-

[5] Poza dyskusją pozostają „związki o charakterze terrorystycznym" ze względu na wyodrębnione kierownictwo, hierarchiczną strukturę i podporządkowanie – typowe dla wysoko zorganizowanych struktur organizacyjnych.

[6] Zob. E. M. Guzik-Makaruk, W. Filipkowski, *Kryminalizacja grup terrorystycznych w ustawodawstwie RFN i Polski, Próba studium komparatystycznego*, w: *Przestępczość terrorystyczna. Ujęcie praktyczno-dogmatyczne*, K. Indecki (red.), Poznań–Białystok–Łódź 2006, WiS, s. 102 - 103.

[7] W Polsce nigdy nie odbyła się na forum publicznym rzetelna dyskusja na temat kontrowersyjnej metody zwalczania terroryzmu przez amerykańskie służby wywiadowcze oraz na temat bezpieczeństwa osób podejrzanych. Interesujące byłoby poznać opinię prawników i politologów na temat, czy w obliczu zagrożenia tym zjawiskiem akceptują praktykę porywania osób podejrzanych o terroryzm i przewożenia ich do innych państw, gdzie zeznania wymusza się torturami lub legalnymi metodami przesłuchań, choć wątpliwymi etycznie. Zob. *„Water boarding" practice banned by CIA*, „The New Zealand Herald" z dnia 16.09.2007 r.

[8] Wiele wątków związanych z polskim ustawodawstwem antyterrorystycznym znalazło swoje miejsce w pracy zbiorowej będącej owocem konferencji zorganizowanej przez Ministerstwo Spraw Wewnętrznych i Administracji oraz Agencję Bezpieczeństwa Wewnętrznego w dniach 14 - 15 maja 2008 r. w Emowie pt. *Czy Polsce potrzebna jest ustawa antyterrorystyczna?* Zob. pr. zbior. pt. *Terroryzm: materia ustawowa?* K. Indecki, P. Potejko (red.), Warszawa 2009, Agencja Bezpieczeństwa Wewnętrznego.

cie wydawnictwa na temat konstruowania bomb i innych improwizowanych materiałów wybuchowych. Osoby nie posiadające odpowiedniego przygotowania militarnego lub chemicznego mogą mieć trudności z przygotowywanem bomb działających w sposób efektywny. Może np. dojść do użycia niewłaściwych substancji chemicznych, jedynie częściowego przeprowadzenia reakcji chemicznych lub wadliwej konstrukcji zapalnika. Często, mimo iż sprawca jest przeświadczony o skuteczności takiej bomby, dokonanie zamachu jest niemożliwe ze względu na użycie środka nie nadającego się do popełnienia czynu zabronionego[9].

Kolejną kwestią jest zastosowanie instytucji skutecznego lub nieskutecznego **czynnego żalu** (art. 15 kk). Nie są to częste przypadki, ale zdarzają się. Nie podlega karze za usiłowanie ten, kto dobrowolnie odstąpił od dokonania lub zapobiegł skutkowi stanowiącemu znamię czynu zabronionego. Mogą pojawić się pewne okoliczności, które spowodują właśnie takie zachowanie, np. wyrzuty sumienia, zwątpienie w słuszność swoich zamiarów itp. Warunkiem jest jednak, aby osoby organizujące zamach nie zabezpieczały się na wypadek takiej sytuacji poprzez umieszczenie alternatywnego mechanizmu uruchamiającego ładunek w sposób zdalny. W przypadku zaistnienia nieskutecznego czynnego żalu i w sytuacji, gdy sprawca przeżył, musiałby wykazać, iż dobrowolnie starał się zapobiec skutkowi stanowiącemu znamię czynu zabronionego (np. poprzez zmniejszenie liczby ofiar lub zniszczeń, próbę zneutralizowania mechanizmu uruchamiającego ładunek wybuchowy, powiadomienie służb porządkowych, organów ścigania itp.).

2. Odpowiedzialność pozostałych członków zorganizowanej grupy terrorystycznej

Niezależnie od kształtowania się odpowiedzialności karnej bezpośredniego sprawcy konkretnego zamachu terrorystycznego do odpowiedzialności powinny być pociągnięte również osoby pozostałe. Kwestia ta występuje obok odpowiedzialności za udział w zorganizowanej grupie lub związku mającym na celu popełnienie przestępstwa o charakterze terrorystycznym – o ile uda się w ten sposób zakwalifikować ich zachowanie. Zgodnie z przyjętą w prawie polskim koncepcją odpowiedzialności osób współdziałających w popełnieniu przestępstwa, każda z nich odpowiada za własny czyn, w granicach swojej umyślności lub nieumyślności (art. art. 20 - 23 kk).

Przywołując po raz kolejny podział zadań według schematu „9+4", można stwierdzić, że zachowania osób biorących udział w przeprowadzeniu zamachu będą stanowiły różne **formy zjawiskowe** lub **stadialne** popełnienia czynu zabronionego (zamachu terrorystycznego). Najczęściej jednak ich sposób postępowania będzie można określić mianem szeroko rozumianego pomocnictwa. W niektórych szczegółowych przypadkach pewne zachowania będą mogły być zakwalifikowane jako odrębny czyn zabroniony zawarty w części szczególnej kodeksu karnego. Podając konkretne kwalifikacje karne, można kierować się przykładami zachowań bądź zdarzeń wymienionych we wcześniejszych częściach pracy.

Szerzenie propagandy terrorystycznej może wypełniać – zależnie od szczegółowych cech zachowania – znamiona typów czynów zabronionych wymienionych

[9] Podobna sytuacja występuje w przypadku, gdy organom ścigania, które rozpracowują grupę terrorystyczną, uda się w ramach czynności operacyjnych podmienić materiał wybuchowy lub mechanizm zapalający na inną bezpieczną substancję lub wadliwy mechanizm.

w art. art. 119 § 2, 255 §§ 1, 2 lub 3 kk. Wymienione w powyższych artykułach typy czynów dotyczą: po pierwsze – publicznego nawoływania do stosowania przemocy lub groźby bezprawnej wobec grupy osób lub osoby z powodu jej przynależności narodowej, etnicznej, rasowej lub wyznaniowej i po drugie – publicznego nawoływania do popełnienia wykroczenia lub zbrodni, lub pochwalania popełnienia przestępstwa. Inną możliwością jest wypełnienie znamion czynu polegającego na publicznym nawoływaniu do nienawiści na tle różnic narodowościowych, etnicznych, rasowych i wyznaniowych (art. 256 kk). Do takich zachowań może dochodzić na wiecach, uroczystościach religijnych, ale także w internecie na różnego rodzaju blogach, portalach, forach dyskusyjnych itp.[10]. W chwili obecnej tego typu groźby kierowane są pod adresem Amerykanów, Europejczyków i ogólnie chrześcijan, a ich autorami są osoby o poglądach ekstremistycznych. W szczególnych przypadkach mogą mieć zastosowanie także czyny zabronione, opisane w art. 255 §§ 2 i 3 kk. Tutaj również zakres działań, do których nakłaniają sprawcy, może być szeroki, ale generalnie dotyczą one wszelkich zachowań godzących w życie lub zdrowie, ewentualnie mienie innych ludzi. Elementem propagandy są także wszelkiego rodzaju groźby kierowane za pomocą mediów pod adresem krajów bądź ich przywódców oraz organizacji międzynarodowych.

Istotną kwestią jest rozstrzygnięcie zakresu odpowiedzialności osób za **rekrutację** nowych członków na potrzeby grup terrorystycznych lub do przeprowadzenia konkretnych zamachów. W przypadku, gdy nakłanianie do udziału w zorganizowanym związku lub grupie mającej na celu popełnienie przestępstwa o charakterze terrorystycznym dotyczy już konkretnej osoby, możemy mówić o odpowiedzialności z art. 18 § 2, w związku z art. 258 § 2 kk. Rekrutacja może również polegać na pomocnictwie osobie mającej zamiar uczestniczenia w takiej grupie lub związku (lub mającej zamiar dokonania zamachu). W szczególności dotyczy to takich zachowań, jak udzielanie rad lub informacji kandydatom, gdzie i z kim mają się spotkać, jakich środków komunikacji używać i w jaki sposób (aby np. zmylić funkcjonariuszy organów ścigania) nie wzbudzać podejrzeń, co mówić podczas zatrzymania itp.[11]. Na pewnym etapie procesu rekrutacji, a w zasadzie indoktrynacji potencjalnych sprawców zamachu, można także rozważać kwalifikację czynu z art. 151 kk – doprowadzenie namową do targnięcia się na własne życie. Należy przy tym jednak pamiętać, że samobójcza śmierć jest jedynie środkiem służącym do realizacji celu terrorystycznego.

Do niedawna kwalifikację prawną opartą na instytucji pomocnictwa otrzymałoby zachowanie polegające na **organizowaniu zaplecza finansowego** osobom biorącym udział w zorganizowanym związku lub grupie terrorystycznej[12]. Nowelizacja kodeksu

[10] Por. G. Dobrowolski, W. Filipkowski, E. Nawarecki, W. Rakoczy, *Systemy agentowe i metody sztucznej inteligencji w walce z terroryzmem w Internecie,* w: *Przestępczość terrorystyczna. Ujęcie ...*, s. 183 - - 188 oraz W. Filipkowski, *Wybrane aspekty fenomenologii cyberterroryzmu. Studium przypadku sprawy Omara Al-Hussayena*, w: *Cyberterroryzm. Nowe wyzwanie XXI wieku*, T. Jemioła, J. Kisielnicki, K. Rajchel (red.), Warszawa 2009, Wydział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie, s. 120 i nast.

[11] Zob. upubliczniony na stronach internetowych Departamentu Sprawiedliwości Stanów Zjednoczonych podręcznik Al-Kaidy – *The Al Qaeda manual* - http://www.justice.gov/ag/trainingmanual.htm.

[12] Szerzej na ten temat zob. M. Pieth, *Criminalizing the Financing of Terrorism*, „Journal of International Criminal Justice" 2006, nr 4, s. 1074 i nast. oraz *Countering the Financing of Terrorism*, T. J. Biersteker, S. E. Eckert (red.), London–New York 2008, Routledge Taylor & Francis.

karnego z 2009 r. dodała art. 165a, kryminalizujący finansowanie terroryzmu[13]. Zastanawia przede wszystkim umiejscowienie tego przepisu w rozdziale XX. dotyczącym przepisów chroniących bezpieczeństwa powszechnego, a nie w rozdziale XXXII., np. po art. 258, co rzutuje na interpretację jego zapisów[14]. Można z tego wywnioskować, iż zabronione jest finansowanie konkretnych zamachów, które albo spowodowały konkretne ofiary lub straty albo potencjalnie mogły je spowodować. Poza zakresem kryminalizacji jest natomiast zapewnianie środków finansowych na pozostałą działalność grupy terrorystycznej, co należy uznać za błąd, gdyż niewielka część pozyskiwanych środków służy bezpośrednio dokonywaniu zamachów. Ponadto większość potencjalnych sprawców tego typu czynów przekazuje datki na bliżej nieokreśloną działalność terrorystyczną, tj. dżihad, walkę z krzyżowcami etc., a nie na zakup konkretnych przedmiotów lub usług potrzebnych do dokonania konkretnych zamachów lub nawet konkretnej ich kategorii[15].

Kolejne kroki podejmowane przez komórkę wspierającą, tzn. **organizowanie zaopatrzenia w niezbędne środki, zapewnienie transportu, organizowanie bezpiecznego schronienia, realizacja niezbędnego szkolenia, zapewnienie łączności, tworzenie fałszywych tożsamości dla członków grupy** – również można zakwalifikować jako formy pomocnictwa dla zorganizowanego związku lub grupy terrorystycznej, poza szczególnymi przypadkami, gdy wyżej wymienione czynności samodzielnie stanowią typ czynu zabronionego wymienionego w części szczególnej kodeksu karnego. Mamy z tym do czynienia w przypadku, gdy sprawca:

umieszcza na statku wodnym lub powietrznym urządzenie lub substancję zagrażającą bezpieczeństwu osób lub mieniu znacznej wartości – art. 167 § 1 kk,

- bez wymaganego zezwolenia, lub wbrew jego warunkom, wyrabia, przetwarza, gromadzi, posiada, posługuje się albo handluje substancją lub przyrządem wybuchowym, materiałem radioaktywnym, urządzeniem emitującym promienie jonizujące lub innym przedmiotem czy substancją, która może sprowadzić niebezpieczeństwo dla życia lub zdrowia wielu osób albo mienia w wielkich rozmiarach – art. 171 kk,
- przewozi, gromadzi, składuje, porzuca lub pozostawia bez właściwego zabezpieczenia materiał jądrowy albo inne źródło promieniowania jonizującego, jeżeli może to zagrozić życiu lub zdrowiu człowieka lub spowodować zniszczenie w świecie roślinnym lub zwierzęcym w znacznych rozmiarach – art. 184 1 i 2 kk,
- utrudnia lub udaremnia postępowanie karne, pomagając sprawcy przestępstwa uniknąć odpowiedzialności karnej, a w szczególności jeśli sprawcę ukrywa, zaciera ślady przestępstwa, w tym i przestępstwa skarbowego, albo odbywa za skazanego karę – art. 239 §1 kk,
- bez wymaganego pozwolenia wyrabia, handluje, albo posiada broń palną lub amunicję – art. 263 § 1 i 2 kk,

---

[13] Ma on następującą treść: *Kto gromadzi, przekazuje lub oferuje środki płatnicze, instrumenty finansowe, papiery wartościowe, wartości dewizowe, prawa majątkowe lub inne mienie ruchome lub nieruchomości w celu sfinansowania przestępstwa o charakterze terrorystycznym, podlega karze pozbawienia wolności od lat 2 do 12*.

[14] Por. E. W. Pływaczewski, A. Sakowicz, w: *Kodeks karny. Część szczególna. Tom II. Komentarz do art. 212 - 316*, A. Wąsek (red.), Warszawa 2005, Lexis Nexis, s. 404.

[15] Zob. wystąpienie autorstwa E. M. Guzik-Makaruk i W. Filipkowskiego pt. *Kryminalizacja finansowania terroryzmu na tle prawnoporównawczym* podczas Ogólnopolskiej Konferencji Karnistycznej na temat *Współczesne problemy prawa karnego* (Olsztyn 20 - 21 listopada 2008 r.) zorganizowanej przez Wydział Prawa i Administracji Uniwersytetu Warmińsko-Mazurskiego. Wystąpienie zostanie opublikowane w materiałach pokonferencyjnych.

- udostępnia lub przekazuje osobie nieuprawnionej broń lub amunicję – art. 263 § 3 kk,
- wbrew przepisom przekracza granicę Rzeczypospolitej Polskiej, używając przemocy, groźby, podstępu lub we współdziałaniu z innymi osobami – art. 264 § 2 kk,
- organizuje innym osobom przekraczanie wbrew przepisom granicy Rzeczypospolitej Polskiej – art. 264 § 3 kk,
- w celu osiągnięcia korzyści majątkowej lub osobistej, umożliwia lub ułatwia innej osobie pobyt na terytorium Rzeczypospolitej Polskiej wbrew przepisom – art. 264a § 1 kk,
- podrabia lub przerabia dokument w celu użycia go za autentyczny lub takiego dokumentu jako autentycznego używa lub wypełnia blankiet, opatrzony cudzym podpisem, niezgodnie z wolą podpisanego i na jego szkodę albo takiego dokumentu używa – art. 270 kk,
- posługuje się dokumentem stwierdzającym tożsamość innej osoby albo dokument taki kradnie lub przywłaszcza, bezprawnie przewozi, przenosi, albo przesyła za granicę dokument stwierdzający tożsamość innej osoby lub jej prawa majątkowe – art. 275 kk.

Zadania właściwe dla **komórki realizacyjnej** można natomiast zakwalifikować jako karalne formy pochodu przestępstwa. Pierwsze trzy z nich noszą znamiona przygotowania. Można stwierdzić, iż sprawcy w celu popełnienia czynu zabronionego podejmują czynności mające stworzyć warunki do przedsięwzięcia czynu zmierzającego bezpośrednio do jego dokonania. W szczególności art. 16 § 1 kk wymienia następujące zachowania: wchodzenie w porozumienie z inną osobą, uzyskiwanie lub przysposabianie środków, zbieranie informacji lub sporządzanie planu działania. Koresponduje to z następującymi określeniami używanymi w schemacie „9+4":

- wstępna obserwacja i rekonesans celu ataku – dla ustalenia sposobu postępowania, doboru środków i osób potrzebnych do jego dokonania,
- symulacja lub trening zamachu – dopracowanie kolejnych jego etapów,
- końcowe rozpoznanie celu i jego otoczenia – dla dokonania ewentualnych zmian planu.

Jednakże, zgodnie z art. 16 § 2 kk, **przygotowanie** zamachu jest karalne tylko wtedy, gdy ustawa tak stanowi.

Lista czynów zabronionych, których mogą dopuścić się terroryści zawiera przygotowania do:

- zamachu stanu – art. 127 § 2 kk,
- usunięcia przemocą organu konstytucyjnego – art. 128 § 2 kk,
- osłabienia mocy obronnej Rzeczpospolitej Polskiej – art. 140 § 3 kk,
- dokonania przestępstwa określonego w art. art. 163 § 1, 165 § 1, 166 § 1 lub 167 § 1 kk (przestępstwa przeciwko bezpieczeństwu powszechnemu) – art. 168 kk,
- spowodowania katastrofy – art. art. 173 § 1 kk i 175 kk,
- wzięcia lub przetrzymywania zakładnika w celu zmuszenia organu państwowego lub samorządowego, instytucji, organizacji, osoby fizycznej lub prawnej albo grupy osób do określonego zachowania się – art. 252 § 3 kk.

Ponieważ sprawca bezpośredni ataku terrorystycznego jest częścią zarówno grupy (lub związku), jak i często jej instrumentem – można również rozważać kwestię przyjęcia instytucji współsprawstwa, sprawstwa kierowniczego lub polecającego jej członka lub członków[16]. Kolejną kwestią jest kwalifikowanie tych zachowań jako po-

[16] W niektórych przypadkach do dokonania zamachu wykorzystywane są osoby, które nie zdają sobie sprawy z tego faktu, np. doręczyciele przesyłek. Nie wyklucza to jednak odpowiedzialności osób przygotowujących zamach i kierujących postępowaniem takiej osoby.

mocnictwa do targnięcia się na własne życie – art. 151 kk. Należy jednak pamiętać o poczynionej wcześnie uwadze, iż samobójstwo jest tutaj tylko środkiem do osiągnięcia innego celu – tj. dokonania zamachu terrorystycznego.

Warto również zastanowić się nad tym, czy wskazanym powyżej czynom zabronionym, które dokonywane są w ramach grupy lub związku terrorystycznego, prawo nadaje cechę **przestępstw terrorystycznych** zgodnie z definicją zawartą w art. 115 § 20 kk. Oprócz kryteriów materialnych tam wymienionych, podstawowym wskaźnikiem o charakterze formalnym jest górna granica kary pozbawienia wolności grożącej za popełnienie danego czynu. Musi ona wynosić co najmniej 5 lat. Analizując wymienione powyżej typy czynów zabronionych i grożące za nie sankcje, można zauważyć, iż część z nich nie spełnia tego wymogu. I tak, przestępstwami o charakterze terrorystycznym nie są czyny określone w art. art. 190 § 1, 255 §§ 2 i 3, 256, 263 § 3, 264 § 2 oraz 275 kk. W przypadku karalnych przygotowań do dokonania zamachu sprawa wygląda znacznie poważniej. Spośród wymienionych wcześniej sześciu przypadków, tylko przygotowanie do usunięcia przemocą organu konstytucyjnego Rzeczpospolitej Polskiej jest zagrożone karą, której górna granica wynosi dokładnie 5 lat pozbawienia wolności (art. 128 § 2 kk). Jest to kolejny argument (pośród i tak licznej krytyki tego zapisu w literaturze) przemawiający za koniecznością jego zmiany[17]. Działalność członków grupy terrorystycznej będzie można uznać za przestępstwo, może nawet dokonane w ramach zorganizowanej grupy przestępczej (art. 258 § 1 kk) lub zbrojnej (art. 258 § 2 kk). Jednakże zgodnie z prawem nie będzie można ich uznać za przestępstwa o charakterze terrorystycznym. Pozostaje więc pytanie o zasadność i trafność takiej regulacji.

V. Próba określenia ryzyka dokonania samobójczych ataków terrorystycznych w Polsce

Z dokonanych ocen i analiz wynika, że atak terrorystyczny, także samobójczy, jest realny w każdym kraju, który w jakiś sposób, mniej lub bardziej aktywny, bierze militarny udział w konfrontacji z ugrupowaniami islamskimi. Z tej przyczyny osoby i instytucje odpowiedzialne za bezpieczeństwo obowiązane są szczególnie realnie i systematycznie dokonywać ocen ryzyka zagrożeń terrorystycznych, w tym ataków samobójczych, dla obiektów w Polsce i poza jej granicami.

Gwałtownie rosnąca liczba cywilnych ofiar operacji wojsk NATO i USA przeciwko islamskiemu ruchowi oporu, podawana przez talibów dla potrzeb propagandowych, wywołuje coraz głośniejsze i bardziej kategoryczne protesty afgańskich polityków[18]. Potencjalne zwycięstwo Zachodu w Afganistanie i w Iraku nie gwarantuje zmniejszenia ryzyka wystąpienia ataków terrorystycznych. Specjaliści z amerykańskiego Departamentu Stanu przekonują, że gdy terroryści zostaną pokonani w Iraku i Afganistanie, zaczną poszukiwać innych miejsc do konfrontacji z Zachodem. Tymi miejscami mogą być nawet kraje z niewysoką liczbą wyznawców islamu i najmniej przygotowane do walki z terroryzmem.

Spośród wyżej opisanych uwarunkowań zagrożeń terrorystycznych dla naszego kraju należy ponownie zdefiniować pojęcie **bezpieczeństwa wewnętrznego** w zakresie

[17] Obszernie na ten temat zob. K. Indecki, *Stan badań nad terroryzmem po roku 2001,* w: *Przestępczość terrorystyczna. Ujęcie* ..., s. 39 - 41.

[18] Zob. W. Jagielski, *Afgański senat zakazuje walk z talibami*, „Gazeta Wyborcza" z dnia 10.05.2007 r.

ochrony przed terroryzmem, szczególnie samobójczym. Trzeba pamiętać, że sprawcy zwykłych i samobójczych ataków terrorystycznych rekrutują się obecnie nie tylko z regionów arabskich i muzułmańskich. Wyznawcy islamu stanowią już nie tylko część ludności Indii, Indonezji, państw Azji Środkowej, które powstały po upadku ZSRR, czy rosyjskiego Kaukazu Północnego. Społeczności muzułmańskie są liczne również w krajach europejskich: w Niemczech, Wielkiej Brytanii, Hiszpanii i we Francji, w których nie tylko w łatwy sposób mogą się ukryć, ale też skąd mogą swobodnie przemieszczać się do Europy Wschodniej. Zamachy terrorystyczne dokonywane przez terrorystów-samobójców stanowią zdarzenia, które mogą wywołać głęboko sięgające, negatywne skutki psychiczne, społeczne i polityczne. Instytucje odpowiedzialne za bezpieczeństwo państwa muszą zdawać sobie sprawę z faktu, że wykrycie potencjalnego terrorysty-samobójcy jest niezmiernie trudne nawet wtedy, gdy należy on do grupy zorganizowanej o charakterze terrorystycznym.

Przykłady z krajów Europy Zachodniej wskazują, że potencjalni terroryści-samobójcy są albo „uśpieni" przez organizację (grupę) terrorystyczną, albo samobójcza grupa terrorystyczna tworzy się spontanicznie, w głębokim ukryciu. Należy pamiętać, że terrorysta, motywowany ideologicznie lub zemstą, nigdy nie przestaje być terrorystą. Nikt nie potrafi wskazać, czy i w jakiej fazie przygotowań ataki terrorystyczne mogą być skierowane na cele polskie za granicą lub w Polsce. Potencjalni terroryści wyznania islamskiego, motywowani ideologią Al-Kaidy oraz poczuciem braterstwa religii i walki, sami wyznaczają miejsca w świecie do przeprowadzenia zamachów odwetowych. Decydując się na ataki samobójcze, są przekonani, że internacjonalistyczny dżihad da im możliwość skutecznej obrony islamu przed napaścią Zachodu. Cytowany wcześniej włoski prokurator A. Spataro twierdzi, że współczesne organizacje terrorystyczne to właściwie luźne, elastyczne grupy, którym brak dowódcy i struktury wewnętrznej. Islamiści często zmieniają swoje nazwiska, przynależność do organizacji i miejsce pobytu, przemieszczając się między niewielkimi komórkami rozsianymi po całym świecie. Te kilkuosobowe komórki powstają spontanicznie, na skutek zapoznawania się za pośrednictwem internetu z wezwaniami Osamy Ben Ladena.

Przykładem bodźca pobudzajacego terroryzm samobójczy była rozpowszechniona w internecie 11 września 2007 r. przez firmę As-Sahab Media odezwa ben Ladena, w której oddał on hołd Saudyjczykowi, Walidowi al-Szehriemu, jednemu z porywaczy samolotów, które posłużyły do przeprowadzenia wrześniowych zamachów w 2001 r. W oddzielnym filmie wyemitowano również nagrany testament al-Szahriego[19].

Terroryzm samobójczy postrzegany jest przez ekstremistów islamskich jako jedyny środek walki z powodu nierównowagi sił na świecie i przekonania tkwiącego w kulturze islamskiej, że najlepiej jest zginąć w imię Boga i wartości islamskich, w sposób jak najbardziej honorowy[20].

[19] To nagranie Osamy ben Ladena pojawiło się w internecie i zostało nagłośnione przez CNN 11.09.2007 r.

[20] 1 września 2005 r. telewizja al-Dżazira wyemitowała taśmę z nagranym po angielsku testamentem 30-letniego Mohammada Sidika Khana, jednego z czterech londyńskich zamachowców-samobójców i prawdopodobnego przywódcy całej grupy. Wypowiedzi Khana przeplatały się z komentarzem Ajmana al-Zawahiriego. Obaj zagrozili Zachodowi kontynuowaniem serii zamachów w przypadku kontynuowania działań antymuzułmańskich. Khan podkreślił, że jego samobójczy czyn gotowi są skopiować liczni następcy, którzy za cenę życia chcą bronić islamu przed przemocą ze strony demokratycznych rządów europejskich.

Zjawisko współczesnego terroryzmu samobójczego można podzielić na **dwa nurty**. Pierwszy daje znać o sobie na obszarze trwającego konfliktu (wojny), gdzie terroryści-samobójcy atakują głównie militarne cele przeciwnika, jego sojuszników i własnych kolaborantów. Ataków samobójczych stosowanych wobec wojsk przeciwnika nie należy kwalifikować w kategorii terrorystycznych, ponieważ są one stałym elementem wojen i walk partyzanckich we wszystkich kulturach oraz religiach. Odmiennie definiuje się nurt terroryzmu samobójczego, atakujący cele niemilitarne (cywilne). Nawet ten może znajdować swoje cele na obszarze trwającego konfliktu militarnego (Irak, Afganistan) oraz na terytorium przeciwnika, często geograficznie oddalonym od pola walki[21]. Z tego nurtu wyłonił się, a następnie został zastosowany 11 września 2001 r., najbardziej groźny w naszej kulturze terroryzm samobójczy, atakujący cele niemilitarne na terytorium państwa nie prowadzącego wojny z krajem (narodem), z którego pochodzą terroryści. W tego typu przypadku terroryści atakują tzw. wroga urojonego i nie w imię ideologii wojny wyzwoleńczej. Z tego właśnie względu możliwe jest, że islamscy terroryści-samobójcy mogą atakować cele w Europie w ramach odwetu za obecność wojsk Zachodu w Iraku i Afganistanie. Nikt nie wie, ilu potencjalnych wyznawców islamu planuje i przygotowuje samobójcze ataki terrorystyczne w geograficznie odległych od świata islamu miejscach, jako akty zemsty za krzywdy wyrządzone wyznawcom tej religii w obu tych krajach. Nie można wykluczyć również zjawiska rywalizacji między poszczególnymi grupami terrorystycznymi w przeprowadzaniu spektakularnych ataków[22].

Zgodnie z koncepcją Europejskiej Polityki Bezpieczeństwa i Obrony (ESDP) terroryzmu, szczególnie w jego wersji samobójczej, nie da się zwalczyć, stosując wyłącznie wojskowe środki. Niezbędne jest, co zaleciła w 2003 r. parlamentom poszczególnych krajów Rada Europy, doskonalenie priorytetów i usprawnianie walki z tym zjawiskiem na poziomie prawodawczym[23]. Pełniejsza wiedza o kryminologicznych aspektach terroryzmu samobójczego przyczyniłaby się do likwidacji czynników wpływających na wzrost popierania samobójczej śmierci terrorystów i ich naśladowania przez kolejnych ochotników. Środki wojskowe i instrumenty prawne stosowane w walce z terroryzmem samobójczym będą niewystarczające bez likwidacji źródeł wpływających na wzrost poparcia dla tego zjawiska. Tymi źródłami są głównie uczucie gniewu i rozgoryczenia, powszechne w świecie islamskim, oraz trwające na tym obszarze konflikty regionalne.

[21] Za przykład mogą posłużyć terrorystki, które 5 lipca 2003 r. dokonały ataku podczas festiwalu rockowego odbywającego się na lotnisku Tuszyno pod Moskwą. W kolejce do kas biletowych wysadziły się Zulichana Elichadżyjewa i Miriam Szaripowa. Zginęło wówczas 16 osób, a 60 zostało rannych.

[22] Gdy OWP Jasera Arafata rozpoczęło rozmowy pokojowe, Hamas w 1993 r. rozpoczął serię samobójczych zamachów, stając się tym sposobem obiektem zainteresowania wszystkich mediów. Przywódca Tygrysów Tamilskich w 1987 r. zaczął posyłać do przeprowadzenia ataków samobójców, by zyskać przychylność najważniejszej grupy tamilskich separatystów.

[23] Zob. J. Solana, *Jak inteligentnie walczyć z terroryzmem*, „Gazeta Wyborcza" z dnia 8 - 9.01.2005 r.

Streszczenie

Opracowanie porusza problem jednej z metod walki współczesnego terroryzmu – ataków samobójczych. Zawiera ono dwie podstawowe tezy: po pierwsze, że przed zamachem samobójczym trudno jest się uchronić i po drugie, że tego typu zamach jest efektem działania grupy, a nie pojedynczych osób.

Przeprowadzona w niniejszej publikacji analiza zamachów samobójczych dotyczy trzech obszarów. Pierwszy z nich odnosi się do aspektów historycznych omawianego zjawiska, jego genezy i stanu współczesnego. Przedstawiane opisy zostały poparte materiałem faktograficznym.

Drugim obszarem jest kryminologiczna analiza cech sprawców oraz sposobu ich działania. W artykule scharakteryzowano takie aspekty, jak cele podejmowania zamachów samobójczych, motywacja ich sprawców oraz sposób działania grup organizujących zamachy.

Trzecim obszarem jest próba ujęcia powyższego zjawiska w ramy prawne. Poruszono tu kwestię odpowiedzialności karnej głównie osób pomagających w przeprowadzeniu zamachu i przygotowujących go. Zdaniem autorów, to właśnie na tych osobach powinna skupiać się uwaga zarówno służb specjalnych, jak i organów ścigania.

Powyższa analiza została dokonana zgodnie z założeniami zasady organizacji „9+4". W artykule wskazano również na niedoskonałości prawa polskiego dotyczące zwalczania zamachów samobójczych.

Abstract

The article focuses on issue related to one of the methods of fighting contemporary terrorism, namely suicide attacks. The Authors advance and support two principle theses: firstly, it is very difficult to prevent a suicide attack, and secondly, a suicide attack is an outcome of cooperation of a group of people, rather than a single person.

The analysis of suicide attacks illustrated in the article relates to three subject areas – first of all the historical background of the phenomena, the origins and the current state. The descriptions included in the article are supported by an extensive selection of datum.

The second area relates to criminological analysis of perpetrators' traits and their modus operandi. The article describes such aspects as the main goals for conducting suicide attacks, motivation of the suicide attackers and different types of group activities which are needed to conduct an attack.

The third area is an attempt to codify the phenomena within legal regulations. The article relates to the criminal responsibility of facilitators and organizers of the attacks. According to the authors, special services and law enforcement agencies should concentrate their affords and attention around such individuals.

The analysis has been conducted according to so called '9+4' principle for organizing a suicide attack. The Authors also point out the deficiencies of Polish penal law in that regard.

Artur Jasiński

TECHNICZNE ŚRODKI ZABEZPIECZANIA BUDYNKÓW PRZED ATAKIEM TERRORYSTYCZNYM

Wprowadzenie

Przystąpienie Polski do Unii Europejskiej i NATO, aktywny udział polskich sił zbrojnych w operacjach antyterrorystycznych w Iraku i Afganistanie oraz organizacja mistrzostw piłkarskich EURO 2012 – to główne czynniki, które powodują, że zagrożenie terrorystyczne naszego kraju wzrasta [Jałoszyński 2008, s. 55; Machnikowski 2007, s. 4 - 7]. Spośród wszystkich aktów terrorystycznych ponad 90% to ataki bombowe [Jałoszyński 2008, s. 45]. Terror bombowy jest już w Polsce znany: liczba tego typu zamachów utrzymuje się od początku lat 90. na podobnym poziomie i wynosi kilkaset rocznie. W większości zamachy bombowe w Polsce są wynikiem porachunków gangsterskich, a ich skutki są ograniczone. Jednak w przypadku ataku terrorystycznego można spodziewać się dużej liczby ofiar i spektakularnych zniszczeń, gdyż cechą współczesnego terroryzmu jest maksymalna eskalacja przemocy i dążenie do wywołania medialnego szoku o skali globalnej [Coaffee 2003, s. 6 - 8].

W krajach, które są najbardziej narażone na zamachy terrorystyczne (Izrael, USA, Wielka Brytania), oprócz działań antyterrorystycznych prowadzonych przez siły zbrojne, policyjne i służby specjalne, dużą wagę przywiązuje się do prewencji, w tym do odpowiednich metod zabezpieczania przestrzeni publicznej i najbardziej zagrożonych obiektów. Zasady projektowania tych zabezpieczeń nawiązują do znanych doktryn wykorzystujących cechy środowiskowe do prewencji kryminalnej, tj. do: *Przestrzeni obronnej* (*Defensible Space*), autorstwa amerykańskiego architekta Oskara Newmana [Newman 1972] i do *Zapobiegania przestępczości poprzez odpowiednie kształtowanie przestrzeni* (*Crime Prevention Through Environmental Design* – CPTED), powstałej w oparciu o badania C. Raya Jeffreya. Konieczność przeciwdziałania zagrożeniu terrorystycznemu spowodowała dalszą ewolucję tych doktryn. Są one obecnie rozwijane pod umowną nazwą *Design Out Terrorism* (*Projektowanie jako narzędzie ograniczenia ryzyka zamachu terrorystycznego*), co w efekcie przyniosło szereg publikacji naukowych [Coaffee 2003; Hopper, Droge 2005; Hinman 2008; Smilowitz 2008], odpowiednich unormowań, wytycznych projektowych [AIA 2001; FEMA 2003, 2007; DoD 2007] oraz zastosowań praktycznych.

Tab. 1. Strategie doktryny CPTED w zastosowaniu antyterrorystycznym.

1. Kontrola dostępu (*access control*): ograniczenie zagrożenia poprzez zróżnicowane środki kontroli dostępu: ochrona fizyczna (strażnicy), mechaniczna (bramy i zamki), elektroniczna (czujniki i sygnalizatory włamania, karty dostępu i urządzenia biometryczne). Wyznaczenie w obiekcie hierarchicznych stref, do których wstęp mają tylko uprawnione osoby. Celem jest ograniczenie potencjalnemu napastnikowi dostępu do obiektu.
2. Zapewnienie nadzoru (*surveillance*): ułatwienie użytkownikom i służbom ochrony obserwacji wnętrz i terenu wokół obiektu, szczególnie dojść i wejść, za pomocą odpowiedniej konstrukcji budynku i jego otoczenia oraz urządzeń optycznych i elektronicznych (noktowizory, CCTV). Celem jest odstraszenie, wykrycie i zneutralizowanie potencjalnych napastników.
3. Wzmocnienie terytorialne (*territorial reinforcement*): tworzenie wokół zagrożonych budynków stref chronionych (ogrodzenia, mury i patrole) oraz stref bezpieczeństwa uniemożliwiających atak na budynek przy użyciu bomby samochodowej. Służą temu zmiany organizacji ruchu kołowego i bariery tworzone przez elementy małej architektury, mury oporowe, kwiatony, rzeźby, ławy, maszty i słupki (*bollards*). Celem jest utrudnienie dokonania zamachu i ograniczenie jego skutków.
4. Utwardzenie celów (*target hardening*): zabezpieczanie potencjalnych celów ataku przed jego skutkami poprzez planowanie, środki architektoniczne i techniczne (strefowanie funkcji budynku, wzmacnianie konstrukcji i elewacji, stosowanie przeszkleń pancernych lub innych, zabezpieczanie otworów, kanałów i instalacji podziemnych, tworzenie schronów i bezpiecznych pomieszczeń, dublowanie instalacji budynku), w celu ograniczenia strat i zniszczeń powstałych w wyniku ewentualnego ataku.

Źródło: opracowanie własne.

Skutki ataku bombowego na budynek

Zagrożenia zmieniają się stale, a pomysłowość i przebiegłość terrorystów jest nieograniczona [FEMA 2003], czego przykładem było wykorzystanie samolotów pasażerskich do ataku na Pentagon i budynki World Trade Center w Nowym Jorku. Niektóre źródła podają, że Al-Kaida posiada już broń biologiczną, chemiczną i radiologiczną („brudne bomby" i tzw. *pocket nukes* – bomby kieszonkowe[1]) [Coaffee 2003, s. 76; Villamarin Pulido 2008, s. 203 - 232]. Jednak nadal najczęstszą formą zamachu terrorystycznego skierowanego przeciwko budynkom jest atak bombowy, szczególnie przy użyciu ładunku wybuchowego umieszczonego w pojeździe kołowym (tzw. *VBIED – Vehicle Borne Improvised Explosive Device*). Zamach może mieć formę statyczną, tj. zdetonowanie samochodu pozostawionego pod budynkiem (World Trade Center, Nowy Jork 1993) lub obok budynku (Oklahoma City 1995), albo dynamiczną – poprzez staranowanie ogrodzenia, bram wjazdowych lub barier przez samochód, najczęściej prowadzony przez zamachowca samobójcę (ambasady amerykańskie w Kuwejcie i Bejrucie, 1983; koszary Marines w Bejrucie, 1983). Waga typowej bomby samochodowej wynosi kilkaset kilogramów, ale w przypadku dużego samochodu ciężarowego lub cysterny może sięgać nawet kilkudziesięciu ton [FEMA 2003].

Fala uderzeniowa, która powstaje w efekcie wybuchu, ma podwójny skutek destrukcyjny: pierwotny – energia uderzenia przekazywana jest na części budynku położone najbliżej eksplozji, niszcząc jego elewację i naruszając układ podstawowych elementów konstrukcji, i wtórny – uszkodzone elementy konstrukcji mogą bowiem doprowadzić do utraty stateczności i zawalenia się fragmentów lub całej budowli. „Odpowiedź" obiektu na eksplozję można podzielić na kilka faz: w pierwszej fala uderzeniowa bezpośrednim uderzeniem niszczy jego zewnętrzną ścianę; okna i ściany osłonowe

[1] „Brudna bomba" to konwencjonalny ładunek wybuchowy otoczony materiałem rozszczepialnym; bomba kieszonkowa – to miniaturowy ładunek jądrowy o wadze kilku kilogramów.

są roztrzaskane, a elementy konstrukcji poddane dynamicznym obciążeniom. Następnie fala „opływa" budynek, oddziałując na dach i pozostałe ściany. Fala uderzeniowa, która wdziera się do wnętrza obiektu przez otwory lub zniszczoną fasadę wywiera na stropy parcie skierowane ku górze. Jest to zjawisko tym groźniejsze, że stropy nie są zwykle projektowane z myślą o tego typu obciążeniach. Fala uderzeniowa zagraża także ludziom, niszcząc ich organy wewnętrzne, a unoszące się fragmenty budynku, mebli i odłamki szkła potęgują zagrożenie [Hinman 2008].

Skala zniszczeń spowodowanych atakiem bombowym jest zależna od splotu następujących czynników: wielkości ładunku wybuchowego, odległości miejsca eksplozji od budynku i odporności budynku na skutki ataku. Podstawowym zagrożeniem związanym z atakiem bombowym jest utrata stateczności konstrukcji budowli (katastrofa budowlana). W rezultacie zamachu na Alfred P. Murrah Federal Building w Oklahoma City w 1995 r. aż 87% ofiar śmiertelnych to wynik zawalenia się budynku [FEMA 2003, s. 3 - 1]. Innym niezwykle poważnym zagrożeniem są odłamki szkła powodujące liczne zranienia. W czasie ataku bombowego na ambasadę amerykańską w Kenii (1998 r.) zabitych zostało 258 osób, a ranionych 5000, w większości właśnie przez unoszące się odłamki szkła, które mogą zostać odrzucone na ponad kilometr od miejsca eksplozji. Bardzo groźne są także spadające z górnych pięter fragmenty szyb, które także mogą

Fot. 1. Alfred P. Murrah Federal Building w Oklahoma City zniszczony w 1995 r. przez atak bombowy.

Źródło: Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks, US Federal Emergency Management Agency, 2007, s. 1 - 7.

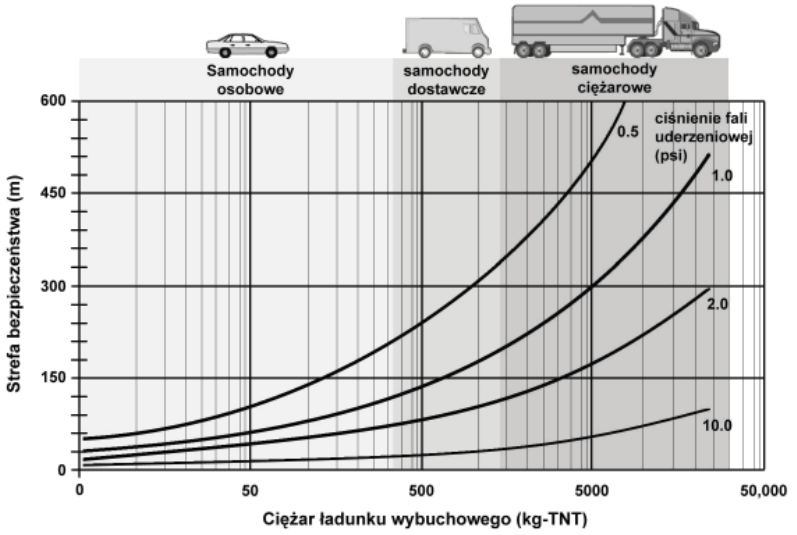
odpryskiwać na znaczne odległości [Hinman 2006].

Ochrona budynków przed atakiem terrorystycznym

Metody zabezpieczania obiektów przed atakami terrorystycznymi można podzielić na działania zmierzające do utrudnienia przeprowadzenia zamachu terrorystycznego (*Security Design*) i działania mające na celu zwiększenie odporności budynku

na skutki ataku bombowego (*Building Hardening*). Są one realizowane poprzez odpowiednie planowanie, za pomocą środków architektonicznych, technicznych i technologicznych. Projektując zabezpieczenia budynku, wyznaje się zasadę dostosowywania zabezpieczeń do poziomu zagrożenia. Wychodzi się przy tym z założenia, że całkowita ochrona obiektu przed atakiem jest niemożliwa lub nieuzasadniona z przyczyn ekonomicznych, psychologicznych i społecznych.

Najprostszym, najłatwiejszym i najtańszym sposobem zabezpieczenia budowli jest otoczenie jej strefą bezpieczeństwa i oddalenie w ten sposób ewentualnego zagrożenia (np. miejsca, w którm może zostać zaparkowany samochód) na odpowiednią – możliwie największą – odległość. Strefa bezpieczeństwa musi być otoczona solidnymi, trwale połączonymi z podłożem przeszkodami, którymi najczęściej są elementy małej architektury: ławy, żelbetowe kwiatony, słupy, masywne ogrodzenia, podesty i mury oporowe. Wjazd na chronioną posesję musi być zaopatrzony w masywne bariery i zapo-



Rys. 1. Zależność wielkości strefy bezpieczeństwa, ciężaru ładunku wybuchowego i ciśnienia fali uderzeniowej.

Źródło: opracowanie własne autora za: Reference Manual to Mitigate Potential Terrorist Attacks against Buildings, US Federal Emergency Management Agency, 2003, s. 4 - 17.

ry, których sforsowanie przez rozpędzony samochód będzie niemożliwe.

Standardy amerykańskie zalecają, aby odległość chronionego budynku od krawędzi ulicy lub niekontrolowanego parkingu wynosiła od 10 m (cele niskiego ryzyka) do 50 m (cele wysokiego ryzyka, np. miejsca chronionych zgromadzeń i budynki ambasad). Za niedopuszczalne uważa się parkowanie samochodów bezpośrednio przy budynku lub pod nim. Szybką metodę wyznaczania zależności pomiędzy wielkością strefy bezpieczeństwa (tj. odległością miejsca potencjalnego wybuchu od budynku), ciężarem ładunku wybuchowego i skutkami wybuchu (wyrażoną wartością ciśnienia psi) przedstawia załączony rysunek 1. Z analizy tego rysunku, a także zamieszczonej poniżej tabeli 2 wynika, że nawet 100-metrowa strefa bezpieczeństwa nie zabezpiecza w pełni budowli przed uszkodzeniami (na przykład w przypadku eksplozji bardzo silnego ładunku wybuchowego o wadze ponad 500 kilogramów, który może być przewie-

ziony w furgonetce lub ciężarówce).

Tab. 2. Przewidywane skutki wybuchu, w zależności od ciśnienia fali uderzeniowej.

Przewidywane zniszczenia	Ciśnienie fali uderzeniowej (psi)	Ciśnienie fali uderzeniowej (kPa)
Popękane szyby w oknach	0,15 - 0,22	1,03 - 1,51
Niewielkie uszkodzenia części budynków	0,5 - 1,1	3,4 - 7,6
Wygięte arkusze metalu	1,1 - 1,8	7,6 - 12,0
Pęknięcia murowanych ścian	1,8 - 2,9	12,0 - 20,0
Zniszczenie drewnianych budynków	powyżej 5	powyżej 34
Poważne uszkodzenie budynków o szkieletowej konstrukcji stalowej	4 - 7	27 - 48
Poważne uszkodzenie budynków o konstrukcji żelbetowej	6 - 9	41 - 62
Prawdopodobne całkowite zniszczenie większości typów budynków	10 – 12	69 - 82

Źródło: opracowanie własne za: *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings,* US Federal Emergency Management Agency, 2003, *Damage Approximation*, s. 4 - 19.

Elementem znacznie zwiększającym bezpieczeństwo budynku jest ogrodzenie, które powinno być wysokie (ponad 2,40 m) i solidne, ale przy tym ażurowe. Ogrodzenia pełne ograniczają widoczność i kontrolę terenu, ponadto mogą – szczególnie kiedy są wykonane z bloków kamiennych lub murowane z drobnych elementów – zwiększyć niszczycielską siłę eksplozji. Elementem ogrodzenia powinien być punkt kontroli wjazdu i wejścia oraz rozdzielnia poczty i zamykane pomieszczenie do składowania śmieci. Teren wokół budynku musi być uporządkowany, przejrzysty, pozbawiony elementów, w których można ukryć bombę (lub w których może ukrywać się napastnik), takich jak kwiatony, pojemniki na śmieci i gęste krzewy. Powinien być także dobrze oświetlony, dozorowany i monitorowany. Wszelkie otwory w zewnętrznych ścianach budynku, a w szczególności czerpnie powietrza do urządzeń wentylacyjnych i klimatyzacyjnych, powinny być umieszczone poza zasięgiem agresora i zabezpieczone przed możliwością wrzucenia tam ładunku wybuchowego lub gazowego.

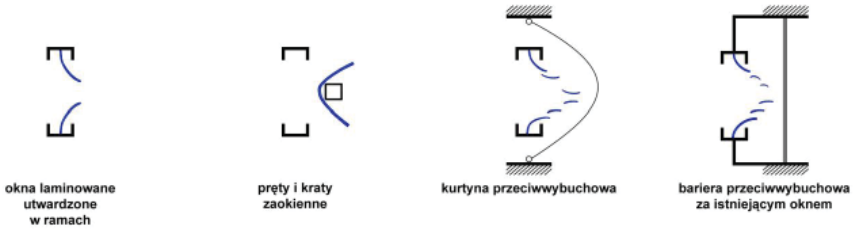
W ochronie budynku i terenu wokół niego dużą rolę odgrywają urządzenia elektroniczne, szczególnie dozór wizyjny, systemy sygnalizacji włamania i kontroli dostępu. Często wszystkie elektroniczne systemy zabezpieczające budynek zintegrowane zostają w nadrzędny system nadzoru i bezpieczeństwa, tzw. SMS (*Security Management System)*, zapewniający monitorowanie i rejestrowanie ich działania oraz wizualizację sygnałów. Zaletą systemów elektronicznych, szczególnie połączonych ze specjalnymi, wzmocnionymi różnymi typami przeszkleń, jest możliwość ograniczenia tradycyjnych, masywnych zabezpieczeń technicznych (kraty) i nadania budynkowi przejrzystego charakteru. Jednak współczesne, tzw. inteligentne, technologie, które skutecznie zabezpieczają budynek przed włamaniem, stają się bezradne wobec niszczycielskiej siły terrorystycznego ataku bombowego [Racoń-Leja, Róg 2004, s. 209].

Techniczne zabezpieczenie budynku przed skutkami wybuchu jest najtrudniejszym i najbardziej kosztownym elementem systemu zabezpieczeń antyterrorystycznych, gdyż wywołuje daleko idące implikacje przestrzenne, ingerując w formę, architekturę i sposób użytkowania budynku [Smilowitz 2008]. Idealnym zabezpieczeniem w tym przypadku jest bowiem skonstruowanie budynku pozbawionego okien, najlepiej podziemnego bunkra [ATF 2006]. Dlatego filozofia zabezpieczania budowli przed skutkami wybuchów opiera się na dwóch podstawowych przesłankach: zabezpieczaniu ich

przed zawaleniem się oraz dążeniu do ograniczenia liczby ofiar i rozmiaru zniszczeń.

Najsłabszym elementem wszelkich obiektów są okna i ściany osłonowe. Fakt ten wykorzystuje się na etapie projektowania: fragmenty przeszklone powinny ustąpić fali uderzeniowej jako pierwsze, tak aby jej energia mogła w kontrolowany sposób przejść przez wnętrze budynku, nie naruszając jego zasadniczej konstrukcji (*balanced design*) [Hinman 2006]. Jednocześnie podejmuje się działania zmierzające do ograniczenia zagrożenia wywołanego przez latające odłamki szkła poprzez zastosowanie warstwowego szkła laminowanego (bezpiecznego) oraz silne połączenie zestawów szklanych z ramami okiennymi, które z kolei muszą być dobrze osadzone w murach. Zabiegi te mają na celu spowodowanie w następstwie wybuchu „rozdarcia" tafli szklanych, które jednak powinny pozostać w ramach.

Innym systemem, który zabezpiecza przed rozpryskami szkła, są kurtyny przeciwwybuchowe (*blast curtains)*, zastosowane po raz pierwszy w czasie II wojny światowej w Londynie. Są to obciążone wzdłuż dolnej krawędzi pasy gęstej metalowej siatki (obecnie stosuje się siatki kevlarowe) zawieszone nad oknem, szersze i dłuższe od otworów okiennych. Nadmiar kurtyny zrolowany jest pod oknem w skrzynce, umieszczonej w ścianie lub stropie. Na skutek wybuchu kurtyny wyginają się, przepuszczając falę uderzeniową i skutecznie wychwytują odłamki szkła. Alternatywą dla kurtyn są wewnętrzne pręty lub kraty montowane w świetle okna, których zadaniem jest wyłapywanie fragmentów foliowanego szkła. Jednak skuteczność tego rozwiązania jest ograniczona [Hinman 2006].



Rys. 2. Przeciwwybuchowe zabezpieczenia otworów okiennych.

Źródło: opracowanie własne autora za: HINMAN E., Blast Safety of the Building, Whole Building Design Guide, Washington D.C. 2008.

Inną formą zabezpieczenia wnętrza budynku przed niszczącymi skutkami wybuchu jest wykonanie bariery przeciwwybuchowej (*blast resistant barier)* w postaci okien przeciwwybuchowych. Konstrukcja okien przeciwwybuchowych jest oparta na wykorzystaniu warstwowo klejonych arkuszy poliwęglanowych lub klejonego szkła na przemian z arkuszami poliwęglanu, zamocowanymi w bardzo solidnych ramach. W przypadku stosowania okien przeciwwybuchowych konieczna jest analiza statyczna budynku i ścian zewnętrznych w celu wyeliminowania zagrożeń, np. ewentualnego zawalenia się budynku lub wgniecenia okien wraz z ramami i częściami ścian do jego wnętrza [Hinman 2006]. W razie konieczności zabezpieczenia okien budynku tworzy się za nimi drugą warstwę elewacji, wykonaną ze szkła przeciwwybuchowego. Przegrody poliwęglanowe mocowane są w tym przypadku do stropów i tworzą rodzaj zamkniętej komory, powstałej pomiędzy oknem a przeszkodą przeciwwybuchową. Jest to najskuteczniejsze rozwiązanie chroniące ludzi i mienie. Do jego wad zalicza się jednak konieczność odpowiedniego wzmocnienia konstrukcji ścian i stropów, utratę powierzchni wewnętrznej i brak możliwości korzystania z okien.

Zaleca się, aby konstrukcja ścian osłonowych budynków narażonych na atak bombowy była stalowa lub aluminiowa, z wypełnieniem słupów i rygli dodatkowymi profilami stalowymi, a zestawy szklane laminowane – wklejane do ram za pomocą konstrukcyjnych klejów silikonowych. Prowadzone są badania zmierzające do poprawy odporności ścian osłonowych na skutki wybuchu poprzez zastosowanie kabli, które zabezpieczają szkło przed wyrwaniem z ram. Ponadto kable, łącząc ze sobą ramy okienne i rygle, nadają całej przeszklonej powłoce budynku dodatkowej elastyczności (*cable protected window system)* [Smilowitz 2008].

Na skuteczność ochrony przeciwwybuchowej obiektu duży wpływ ma kształt jego bryły: wszelkie rozczłonkowania i nadwieszenia kumulują energię wybuchu bardziej niż formy zwarte, obłe czy skośne. Właściwe jest także takie ukształtowanie funkcji wewnątrz budowli, aby strefy i pomieszczenia szczególnie chronione umieścić w głębi budynku („pudełko w pudełku"), a większe kompleksy zabudowy kształtować na zasadzie pierścieniowej, umieszczając pomieszczenia najbardziej chronione wewnątrz kompleksu. Budynki niskie, rozproszone, ukryte w zieleni, są bardziej bezpieczne od budynków wysokich. Za najbardziej narażone na atak uważa się części wejściowe obiektów: halle wejściowe i doki rozładowcze. Zaleca się, aby tego typu pomieszczenia miały formę kubatur dostawionych do głównej bryły budynku, tak aby ich ewentualne zniszczenie nie zagrażało głównej konstrukcji. Stanowczo odradza się projektowanie wolnostojących słupów, arkad i innych miejsc, w których elementy głównej konstrukcji nośnej są dostępne, nieosłonięte i narażone na zniszczenie. W wypadku wzmacniania istniejącej struktury zewnętrzne kolumny winny zostać obudowane masywnym płaszczem ze stali, o licu ustawionym w odległości 20 cm od powierzchni żelbetu [Hinman 2008].

Najbardziej odporna na skutki wybuchu jest monolityczna konstrukcja żelbetowa. Wszystkie ambasady USA, które uważa się za obiekty najbardziej narażone na atak terrorystyczny, wznoszone są obecnie właśnie w tej technologii. Układy żelbetowe posiadają wiele zalet: są wszechstronnie rozpoznane i przebadane, ich poszczególne elementy mogą być dowolnie wymiarowane i kształtowane zgodnie z potrzebami statyki, a całość jest niezwykle zwarta. Duży ciężar własny opóźnia reakcję obiektu na falę uderzeniową, co jest zjawiskiem korzystnym, gdyż w czasie kolejnych milisekund impet fali uderzeniowej maleje. Aby konstrukcja żelbetowa była odporna na wybuch, przy projektowaniu jej detali należy stosować zasady analogiczne do projektowania w obszarach zagrożonych ruchami sejsmicznymi[2]. Ponadto należy pamiętać, aby m.in.:

- symetrycznie zbroić obie powierzchnie wszystkich przegród (ścian i stropów),
- używać podpór raczej w postaci ścian niż słupów,
- łączyć zbrojenie konstrukcyjne w najmniej obciążonych miejscach,
- zwiększyć odporność elementów konstrukcji na ugięcia,
- zapewnić stateczność budynku na wypadek zniszczenia dowolnego fragmentu konstrukcji na wysokości jednego piętra i szerokości jednego przęsła,
- w popularnych układach słupowo-płytowych wzmacniać połączenie słupów ze stropami poprzez głowice płaskie lub ostrosłupowe, tworząc tzw. stropy grzybkowe [Hinman 2008].

[2] Oddziaływanie wybuchu na konstrukcję budynku jest inne niż oddziaływanie sejsmiczne: siła wybuchu jest skierowana głównie w stronę nadziemnej części budowli, energia sejsmiczna zaś oddziałuje głównie na podziemne partie budynku. Także czas zdarzenia znacznie się różni. Mimo to, zasady projektowania elementów i węzłów są podobne: przede wszystkim należy zachować ciągłość i elastyczność konstrukcji.

W budynkach zagrożonych atakiem terrorystycznym odradza się stosowanie elementów prefabrykowanych i ścian murowanych [Hinman 2008]. Dla stalowych konstrukcji szkieletowych należy stosować mechaniczne połączenia wszystkich elementów konstrukcji. Aby zabezpieczyć obiekt przed wgniataniem elementów lekkiej obudowy do wewnątrz budynku, stosowane są siatki: stalowe lub wykonane ze zbrojonych włókien polimerowych czy kevlarowych, rozpinane na zewnętrznym licu elementów konstrukcji nośnej (słupy, rygle). W projektowaniu elewacji i elementów otoczenia budynków nie należy stosować drewna, cegieł, bloczków betonowych, luksferów i innych pustaków szklanych, a także masywnych osłon przeciwsłonecznych ani żadnych innych elementów, których latające szczątki mogą być źródłem dodatkowego zagrożenia.

Projektując stropy i dachy, szczególną uwagę należy zwracać na pierwszy zewnętrzny trakt, który będzie podlegał największym obciążeniom od wybuchu. Nie należy przekraczać rozpiętości 10 metrów; preferowanym typem zbrojenia jest zbrojenie krzyżowe dwukierunkowe. Zarówno płyty, jak i belki powinny być symetrycznie zbrojone, zaś wszystkie przeszklenia dachowe i świetliki – maksymalnie odsunięte od zewnętrznej krawędzi w głąb budynku (powinny też posiadać laminowane wewnętrzne tafle szklane i być zaopatrzone w siatki łapiące odpryski szkła). Wskazane jest, aby zewnętrzne urządzenia sytuowane na dachach były solidnie mocowane do podłoża.

Na zakończenie warto odnotować bardzo dobre właściwości ziemi jako materiału chroniącego przed skutkami wybuchu [FEMA 2003, s. 3 - 17]. Budynki zakopane bądź okopane w ziemi i pokryte roślinnością oraz tzw. zielone dachy to rozwiązania wykorzystywane od dawien dawna w budowie fortyfikacji, a obecnie coraz częściej stosowane do konstruowania budynków cywilnych. Ich rosnąca popularność [Betsky 2006] związana jest z propagowaniem wartości proekologicznych i łatwością, z jaką wtapiają się w teren. Do ich wymienionych powyżej zalet należy dodać także dużą odporność na atak terrorystyczny, pod warunkiem, że uniemożliwiony zostanie wjazd samochodów na ich stropodachy.

Wnioski

Zabezpieczenia antyterrorystyczne i ich skutki przestrzenne wywołują szereg kontrowersji, a nierzadko i protestów[3]. Wskazuje się przy tym na ogół na groźbę nadmiernej ingerencji państwa w swobody obywatelskie, fortyfikację przestrzeni publicznej miast i ograniczanie dostępu do najważniejszych budynków, a także na utrwalanie szkodliwego psychologicznie syndromu „oblężonej twierdzy". Zabezpieczanie obiektów jest tylko drobnym fragmentem kompleksowych działań antyterrorystycznych, ale elementem bardzo kosztownym i widocznym. Celowość i skuteczność zabezpieczeń technicznych poddawana jest często w wątpliwość, tym bardziej, że terroryści dysponują całym arsenałem środków, które mogą wykorzystać w atakach na tzw. cele miękkie: zatłoczone obiekty publiczne, stadiony i dworce oraz środki komunikacji masowej, które jest niepomiernie trudniej chronić niż wybrane budynki. Dlatego przed podjęciem

[3] Na przykład studencki konkurs *Design Out Terror*, zorganizowany w roku 2008 w Wielkiej Brytanii, został zbojkotowany przez studentów i skrytykowany przez nauczycieli akademickich. Konkurs ten opierał się na teoretycznym założeniu, że zaatakowany został wielki publiczny plac (o rozmiarach zbliżonych do Trafalgar Square), w wyniku czego zginęło 500 osób. Zadaniem uczestników konkursu było przeprojektowanie placu tak, aby uczynić go bardziej bezpiecznym i odpornym na ewentualny atak terrorystyczny. Protestujący zarzucali organizatorom *szerzenie paranoi* i promocję autorytaryzmu [Lazell 2008].

decyzji o zabezpieczeniu antyterrorystycznym danej budowli konieczna jest kompleksowa analiza zarówno ryzyka, jak i kosztów i rezultatów tego działania, w tym skutków psychologicznych i przestrzennych. Jak pokazują przykłady z Wielkiej Brytanii i USA, dla powodzenia tego typu przedsięwzięć konieczna jest ich społeczna akceptacja, będąca zazwyczaj funkcją ogólnego poczucia zagrożenia. Najskuteczniejszymi, stosunkowo najprostszymi i najmniej inwazyjnymi metodami zabezpieczania budynków i ich użytkowników przed skutkami ataku bombowego są: zapewnienie odpowiedniej strefy bezpieczeństwa wokół obiektu i zastosowanie do wszystkich przeszkleń laminowanego szkła bezpiecznego [Hinman 2008].

W przypadku podjęcia decyzji o potrzebie zastosowania zabezpieczeń przeciwwybuchowych wysokiej klasy konieczna jest interdyscyplinarna współpraca projektantów i konsultantów do spraw zabezpieczeń w celu ograniczenia skutków przestrzennych tych działań. Niezbędne jest także dbanie o jakość, estetykę i humanizację projektowanej przestrzeni. Źle zaprojektowane zabezpieczenia mogą bowiem, po ich zrealizowaniu, przynieść większe szkody przestrzenne i społeczne niż sam terroryzm.

Bibliografia:

1. Betsky A., *Landscrapers: Building with the Land,* London 2006, Hudson and Thames.
2. Coaffee J., *Terrorism, Risk and the City. The Making of a Contemporary Urban Landscape,* Hants 2004, Ashgate Publishing.
3. Hinman E., *Upgrading Window for Blast Effect,* San Francisco 2006, Hinman Consulting Engineers, (www.hce.com/html/articles/glass.html).
4. Hinman E. E., *Blast Safety of the Building Envelope,* Whole Building Design Guide, Washington D.C. 2008, Whole Building Design Guide, (www.wbolg.org).
5. Hopper L. J., DROGE M. J., *Security and Site Design: a Landscape Architectural Approach to Analysis, Assessment, and Design Implementation,* New Jersey 2005, Wiley Publishing.
6. Jałoszyński K., *Współczesny wymiar antyterroryzmu,* Warszawa 2008, Trio.
7. Machnikowski R. M., *Polska jako potencjalny cel ataku terrorystycznego,* Łódź 2007, Centrum Studiów i Prognoz Strategicznych.
8. Newman O., *Defensible Space – Crime Prevention through Urban Design,* New York 1972, Macmillan.
9. Lazell M., *Counterterrorism Competition Blasted,* „Building Design" 21.11.2008.
10. Racoń-Leja K., RÓG M., *Rozwiązania, materiały i systemy zapewniające ochronę budynku, umożliwiające kształtowanie architektury w sposób otwarty i dostępny,* w: Wyżykowski Andrzej (red.), *Przestrzeń bezpieczna. Urbanistyczne i architektoniczne uwarunkowania kształtowania przestrzeni miejskiej dla zwiększenia bezpieczeństwa mieszkańców,* Kraków 2004, Wydział Architektury Politechniki Krakowskiej.
11. Smilowitz R., *Designing Buildings to Resist Explosive Threats,* Whole Building Design Guide, Washington D.C. 2008 (www.wbolg.org).

Normy i Wytyczne Projektowe

1. AIA 2001, *Building Security Through Design: A Primer for Architects, Design Professionals and Their Clients,* The American Institute of Architects, 2001.
2. DoD 2007, *DoD Minimum Antiterrorism Standards for Buildings,* US Department of Defence, 2007.
3. FEMA 2003, *Reference Manual to Mitigate Potential Terrorist Attacks against Buildings,* US Federal Emergency Management Agency, 2003.
4. FEMA 2007, *Site and Urban Design for Security: Guidance Against Potential Terrorist Attacks,* US Federal Emergency Management Agency, 2007.

Streszczenie

Najczęstszą formą zamachów terrorystycznych są ataki bombowe. Szczególnie groźne są ładunki wybuchowe o wielkiej mocy montowane na samochodach. Niniejsza publikacja przedstawia skutki ataku bombowego na budynek oraz architektoniczne, techniczne i technologiczne środki zabezpieczania budynków przed takim atakiem. Artykuł zwraca również uwagę na konieczność przeprowadzania kompleksowych analiz przed podejmowaniem decyzji o zabezpieczeniu antyterrorystycznym danego budynku, źle zaprojektowane zabezpieczenia mogą bowiem po ich zrealizowaniu przynieść większe szkody przestrzenne i społeczne niż sam terroryzm.

Słowa kluczowe: terroryzm, przestrzeń bezpieczna, skutki wybuchu, zabezpieczanie budynku przed atakiem terrorystycznym.

Abstract

The most frequent form of terrorist attacks are the attacks with the use of explosive devices. Vehicle Borne Improvised Explosive Device is the most deadly terrorist weapon due to the amount of explosive material that can be used. The article presents post blast effects on buildings, as well as architectural, technical and technological measures of protecting buildings against such attacks. The article draws the attention to the need of conducting appropriate and complex analysis before taking any decision about introducing additional counter-terrorist protection of a building. Badly designed and implemented security measures could be more dangerous, and bring to society and public space more damage, than terrorism itself.

Keywords: terrorism, safe zone, blast effect, introducing counter-terrorist protection measures to buildings.

Jacek Kędzierski
Krzysztof Jurczuk

Główne formy i grupy zagrożeń występujące w obrocie pocztowo-kurierskim

Transformacja polityczno-ekonomiczna i społeczna zapoczątkowana w Polsce wraz z przełomem 1989 r. przyniosła widoczne zmiany gospodarcze, które w sposób pośredni wpłynęły na rozwój różnorodnych form przestępczości. Na wzrost zagrożeń duży wpływ wywarła także gwałtowna informatyzacja polskiego społeczeństwa oraz postęp techniczno-technologiczny, szczególnie w zakresie szeroko rozumianego komunikowania się (m.in. internet, telefonia komórkowa). Naturalną konsekwencją powyższej sytuacji stało się unowocześnienie form i metod pracy polskich służb specjalnych. Również Agencja Bezpieczeństwa Wewnętrznego podjęła to wyzwanie, dostosowując swój potencjał w zakresie uzyskiwania informacji w stosunku do możliwości, jakie oferują nowoczesne rozwiązania techniczne.

Każdy funkcjonariusz służb specjalnych doskonale wie, że najsłabszym ogniwem w łańcuchu połączeń pomiędzy dwoma ośrodkami (szpiegowskim lub przestępczym) jest łączność. Znalezienie formy komunikowania się, która będzie bezpieczna pod każdym względem, jest rozwiązaniem w pełni gwarantującym konspirację i sukces. Dotyczyło to tak czasów starożytnych, jak i dotyczy współczesnych.

Łączność utajniona

Od czasu wynalezienia pisma i przekazywania w tej formie informacji, powstała potrzeba (różnie uzasadniana czy usprawiedliwiana) zapoznawania się z treścią korespondencji. Już w starożytnym Egipcie posłańcowi, którego zadaniem było przeniesienie wiadomości, golono głowę, nanoszono treść informacji na skórę i wysyłano wówczas, gdy całą głowę pokrywały gęste włosy. Aby odczytać wiadomość, należało ponownie zgolić włosy. Także korespondencja władz obcego państwa zawarta na papierze zawsze była dla służb specjalnych obiektem pożądania. Podobno nikt tak doskonale nie łamał pieczęci poczty królewskiej i nie odtwarzał pieczęci lakowych, jak służby fenickie. Podobnie do dyspozycji służb króla Władysława Jagiełły była cała korespondencja Wielkiego Mistrza Zakonu Krzyżackiego w okresie poprzedzającym bitwę pod Grunwaldem. W latach 1936 - 1938 systematycznej kontroli poddawana była, podczas tranzytowego przejazdu pociągów przez polskie Pomorze na trasie pomiędzy Królewcem a Berlinem, tajna korespondencja Rzeszy Niemieckiej. Działania te noszące kryptonim „Akcja Wózek" pozwoliły na uzyskanie fotokopii tajnych niemieckich dokumentów oraz zdjęć prototypów broni i sprzętu wojskowego przewożonego tą drogą. Współczesna historia do terminów związanych z szeroko rozumianą łącznością szpiegowską dołączyła takie pojęcia, jak: tajnopis, gotowiec, atrament sympatyczny, mikrokropka czy reliew[1]. Przyniosła również przykłady podkładania pod bloczek znaczków przyklejonych na kopercie oraz karteczek z naniesionym mikro-

[1] W. Orłowski, S. Witkowski, *Kontrwywiadowcze rozpoznanie wywiadowczych środków łączności*, Warszawa 1998, Urząd Ochrony Państwa, s. 12 - 16, 25 - 30 i 35.

tekstem, którego wywołanie w celu odczytu powoduje po chwili jego samozniszczenie. Przesyłanie pocztówek na oficjalne adresy z określonymi widokami wież kościelnych (jednej lub dwóch) czy dworców kolejowych, z dołączonym banalnym tekstem o całującej cioci, to już szpiegowskie przedszkole.

Również organizacje przestępcze prowadzące działalność przemytniczą o charakterze mafijnym wykorzystują obrót pocztowy do przekazywania informacji o charakterze niejawnym. Posługują się listem do przesyłania wszelkiego rodzaju sygnałów, rozliczeń finansowych czy np. pogróżek. Przykładem są przechwytywane grypsy więzienne nakłaniające do wykonania wyroku na osobie prokuratora. Pojedynczy list jest w masie pocztowej anonimowy i łatwy do nadania z uwagi na dostępność do usług pocztowych. Właściwie zabezpieczony, poddany profesjonalnej ochronie pracowników służb pocztowych, jest bardzo bezpiecznym środkiem łączności. Jeśli dodać do tego inwencję przestępcy, by nie ujawniać swoich danych jako nadawcy, a list skierować na umówiony adres, którym jest skrzynka kontaktowa, skrytka pocztowa lub skorzystać z usługi kurierskiej „od drzwi do drzwi", to uzyskuje on prawie pełną gwarancję bezpiecznej łączności. Niekiedy, aby ujawnić kontakty osób podejrzanych, niezbędna jest duża determinacja służb operacyjno-rozpoznawczych.

Ze względu na specyfikę tego zagadnienia, trudno jest przytoczyć nieposiadające klauzuli (jawne) współczesne przykłady wykorzystania tej formy łączności. Ale, jak zauważyły media szeroko opisujące aresztowanie rosyjskich szpiegów w USA działających w kręgu Anny Chapman, agenci, poza nowoczesnymi formami komunikacji elektronicznej, stosowali również klasyczne metody spotkań konspiracyjnych i pisania listów atramentem sympatycznym[2].

Przemyt substancji odurzających i psychotropowych

Jednym z głównych i podstawowych dochodów grup przestępczych tak w Polsce, jak i na całym świecie, jest handel narkotykami i podobnie działającymi substancjami o charakterze odurzającym. Obrót pocztowo-kurierski wykorzystywany jest do przemytu narkotyków w sposób nagminny. Proceder ten odbywa się w dwóch „relacjach handlowych": hurtownik-dealer oraz dealer-detalista.

W relacjach hurtownik-dealer zamiast ryzykować przerzut dużej ilości narkotyków przez granicę, gdzie ładunek może być narażony na ewentualne kontrole, działanie urządzeń specjalistycznych, węch specjalnie wyszkolonego do tego celu psa, w myśl kanonów sztuki przemytniczej dzieli się go na kilkadziesiąt paczek i wysyła w obrocie pocztowym. Przy zakładanym ryzyku, że kilka paczek zostanie wyłączonych z obrotu, strata jest w ogólnym bilansie dużo mniejsza, niż gdyby wykryto cały ładunek. Proceder jest skuteczny, ponieważ narkotyk w przesyłce jest trudno identyfikowalny, a do wykrycia go za pomocą np. urządzeń rentgenowskich niezbędne jest użycie dużych sił i środków oraz praktyka operatora. Proceder przemytu drogą pocztową jest skuteczny także ze względu na masę ładunków paczkowych. W hali sortowniczej urzędu węzłowego nawet dobrze wyszkolony pies może mieć pewne trudności ze zidentyfikowaniem tego typu przesyłek ze względu na ich szeroki bukiet zapachowy. Szanse na ujawnienie wzrastają w przypadku indywidualnej procedury identyfikacyjnej z pojedynczymi bagażami ustawionymi na taśmie, jednak nie zawsze jest to możliwe ze względów technicznych i ekonomicznych.

[2] M. Hujer, *Jak dobrze sprzedać szpiega*, „Forum" z 12.07.2010 r.

W przypadku przerzutu narkotyków w relacjach dealer-detalista ryzyko związane z koniecznością odbycia spotkania (np. w kawiarni czy parku), jeśli kanał jest rozpoznany, jest połączone z ewentualnym udokumentowaniem transakcji przez służby policyjne lub specjalne (np. poprzez sfotografowanie bądź nagranie). Takie działanie zastępuje się wysłaniem zwykłego, nie rzucającego się w oczy, listu zawierającego określoną dawkę narkotyku do grupy stałych odbiorców. W tej samej formie można dokonać rozliczenia finansowego za wyżej wymieniony proceder. Wagę problemu w skali światowej dostrzegła Organizacja Narodów Zjednoczonych, która 20 grudnia 1988 r. uchwaliła *Konwencję o zwalczaniu nielegalnego obrotu środkami odurzającymi i substancjami psychotropowymi*. Dokument ten został ratyfikowany w dniu 30 kwietnia 1994 r. przez Rzeczpospolitą Polską i pozostaje obowiązującym na terenie RP międzynarodowym aktem prawnym. Artykuł 19 powyższej *Konwencji* dotyczy *podjęcia działań uniemożliwiających wykorzystanie użycia poczty do nielegalnego obrotu, ujawniania przesyłek zawierających zabronione substancję o charakterze narkotycznym oraz ścigania i karania osób wykorzystujących w nielegalny sposób obrót pocztowy*[3].

Jak sugerują przykłady i doświadczenie zawodowe autorów artykułu, zadań w zakresie wykrywania substancji narkotycznych i psychotropowych w obrocie pocztowym nie zabraknie, a skala zjawiska wciąż wykazuje tendencje wzrostowe. Potwierdzeniem może być przykład z Czech z maja 2010 r., gdzie zatrzymano obywatela RP, który na lotniskach w Pradze i Brnie odebrał przesyłki nadane drogą lotniczą o łącznej wadze 15 kilogramów. Zawierały one syntetyczny środek psychotropowy w postaci białego proszku, o właściwościach zbliżonych do efedryny. Po podjęciu w 2010 r. przez polski rząd zdecydowanych działań zmierzających do wyeliminowania z polskiego rynku syntetycznych narkotyków, tzw. dopalaczy, duża część producentów i dystrybutorów przeniosła swoją działalność na terytorium Republiki Czeskiej. Wykorzystując możliwości prawne, jakie dają luki w czeskich wykazach środków zakazanych, w wielu miejscowościach zostały otwarte sklepy z „upominkami" – wiernymi odpowiednikami polskich sklepów z „przedmiotami kolekcjonerskimi". Kolejnym etapem było przesłanie e-mailem oferty do odbiorców w Polsce, a następnie realizacja zamówienia w postaci przesyłki kurierskiej poprzez Pocztę Polską (Pocztex) lub firmy komercyjne. W tym miejscu należy podkreślić, że z uwagi na obowiązujące na terytorium Unii Europejskiej przepisy przesyłki państw unijnych traktowane są jako korespondencja krajowa. Konsekwencją tego postępowania jest przede wszystkim mniej restrykcyjna forma kontroli granicznej i celnej (m.in. wyrywkowe, a nie całościowe prześwietlanie materiału pocztowego promieniami rentgena). Działając według opisanego powyżej schematu, jeden ze sklepów internetowych oferował w ramach przesyłki pobraniowej za 16 zł (przy zakupie powyżej 2 gramów – przesyłka gratis) zmodyfikowany mefedron (drobny kryształ 5-gramowy – 240 zł, gruby kryształ 5-gramowy – 350 zł, bufedron 5-gramowy – 260 zł). Sprzedający wystawia na oferowany towar faktury VAT (sic!) i zastrzega, że powyższych środków nie należy spożywać, ponieważ są szkodliwe dla zdrowia i służą do celów naukowych. Jednocześnie informuje, że na terenie Polski środki te są w pełni legalne.

[3] Dz.U. z 1995 r., Nr 15, poz. 69.

Kontrabanda pocztowa

Kolejnym poważnym zagrożeniem występującym w obrocie pocztowo-kurierskim, mogącym mieć istotne znaczenie dla szeroko rozumianego bezpieczeństwa i obronności państwa, jest zjawisko kontrabandy pocztowej. Rozpoznanie o charakterze operacyjnym prowadzone na podstawie obserwacji głównych rozdzielni pocztowych oraz sortownie operatorów komercyjnych wskazują, że w środkach obrotu pocztowo-kurierskiego dokonywany jest przemyt dokumentów osobistych, fałszywych środków płatniczych służących głównie rozliczeniom za działalność przestępczą, dzieł sztuki, numizmatów, broni małokalibrowej, amunicji, środków wybuchowych oraz materiałów radioaktywnych. Wszystkie wyżej wymienione elementy można ukryć w pakietach czy paczkach pocztowych, a nawet w liście. Kontrabanda pocztowa, podobnie jak omówiona powyżej łączność utajniona występująca w obrocie pocztowo-kurierskim, jest poprzez masowość, dostępność i anonimowość tego obrotu stosunkowo bezpiecznym środkiem kontaktowym i przerzutowym pomiędzy grupami przestępczymi.

Terroryzm pocztowy

Zamachy terrorystyczne z wykorzystaniem kanału pocztowego można w trybie roboczym podzielić na trzy grupy: o charakterze międzynarodowym, mafijnym oraz indywidualnym.

Jak najogólniej określić cechy listów czy paczek wykorzystywanych w ramach tej formy terroryzmu? Otóż, przesyłki wybuchowe charakteryzują się najczęściej następującymi cechami:

- nieproporcjonalną grubością i wagą w stosunku do formatu (wielkości) koperty,
- dziwnym zapachem,
- brakiem lub nieznanym adresem nadawcy,
- zawyżoną kwotą wartości znaczków na kopercie,
- nadrukiem „do rąk własnych".

Przesyłki posiadające wyżej wymienione cechy zawsze powinny wzbudzać zainteresowanie służb ochrony podmiotów, do których kierowana jest taka korespondencja. Przestępca przesyła często samodzielnie skonstruowaną bombę, wykorzystując zwykle tradycyjną formę korespondencji, ponieważ warunkiem skuteczności przesyłki wybuchowej jest wykorzystanie anonimowości obrotu pocztowego, ludzkiej ciekawości i nieuwagi jednocześnie. Jednak aktualne doświadczenia dotyczące możliwości przekazywania przesyłek o zawartości niezgodnej z obowiązującym prawem wskazują na stopniowe upowszechnianie się wykorzystywania usług kurierskich, świadczonych również przez największych operatorów.

W przypadku tzw. terroryzmu międzynarodowego istotą celu uderzenia jest instytucja państwa. Zamachy tego typu wymierzone są w stosunku do instytucji i urzędów państwowych oraz obiektów wojskowych. Oczywiście dominują w tym organizacje reprezentujące ekstremę polityczną, ruchy o podłożu religijno-fundamentalistycznym, anarchistycznym czy faszystowskim. Są to działania zorganizowane w sposób profesjonalny, które poza osiągnięciem celu politycznego w postaci zamanifestowania siły ugrupowania, nie powodują często indywidualnej odpowiedzialności osoby konstruującej lub wysyłającej korespondencję czy paczkę. Przesyłki wybuchowe wykorzystywane są w każdej z opisywanych grup terroryzmu.

Istnieją dwie główne formy użycia przesyłek pocztowych do przeprowadzenia zamachów poprzez umieszczenie w nich ładunku wybuchowego lub różnego typu sub-

stancji trujących. Przykłady, jakie przyniósł rok 2010 w zakresie możliwości wykorzystania np. frachtu lotniczego do przeprowadzania zamachów terrorystycznych przy użyciu przesyłek wybuchowych, wymuszają dokonanie pogłębionej analizy problemu bezpieczeństwa nie tylko kanału pocztowego czy lotnictwa, ale w ogóle powiązań gospodarczych na świecie. 29 października 2010 r. jemeńscy terroryści z Al-Kaidy przygotowali 2 przesyłki, których zawartość oficjalnie stanowiły drukarka komputerowa i tonery. Odbiorcami paczek miały być żydowskie instytucje religijne w Chicago. Pakunki zostały legalnie nadane do doręczenia w dwóch międzynarodowych korporacjach kurierskich (United Parcel Serwis – UPS i Federal Express – FedEx), które realizują usługi z terytorium Jemenu, wykorzystując własne samoloty. Podczas międzylądowania maszyn, jednej w Dubaju, a drugiej w Wielkiej Brytanii, w trakcie kontroli ujawniono, że we wnętrzu przewożonego sprzętu ukryte są materiały wybuchowe powiązane przewodami elektrycznymi z kartą telefonu komórkowego. Środkiem wybuchowym użytym w przesyłkach był pentryt, ta sama substancja, którą wykorzystano 25 grudnia 2009 r. przy próbie wysadzenia samolotu linii Northwest lecącego do USA. Powyższe wydarzenia spowodowały najpierw całkowite wstrzymanie frachtu lotniczego z Jemenu oraz Somalii (Al-Kaida w Jemenie utrzymuje kontakty z grupami terrorystycznymi w Somalii), a następnie wprowadzenie drobiazgowych kontroli przesyłek cargo. Prześwietlenia wszystkich paczek dokonywane specjalistycznymi urządzeniami mogłyby w praktyce wstrzymać wymianę handlową. Niektóre rządy państw europejskich wstrzymały lotniczy ruch towarowy z państw arabskich lub rozważały możliwość jego wstrzymania. Wprowadziły też zakaz przesyłania tą drogą tonerów do drukarek, a nawet odmowę przyjmowania samolotów towarowych na terytoriach ich krajów. Kolejnym elementem mającym wpływ na wywołanie niepokoju, a nawet paniki, było uświadomienie sobie faktu, iż transport przesyłek cargo odbywa się również przy wykorzystaniu lotów pasażerskich w rejsowych połączeniach międzynarodowych.

Organizowanie zamachów za pomocą listów z ładunkiem wybuchowym na większą skalę zanotowano w latach 80. XX wieku w Irlandii Północnej. W latach 90. broni tej zaczęli używać neonaziści w Niemczech i Austrii (burmistrza Wiednia Helmuta Zinka wybuchowy list pozbawił prawie całej dłoni). Terroryści palestyńscy wysłali wiele tego typu listów do różnych osobistości w RFN i w innych krajach Europy w trakcie finalizowania traktatu pokojowego między Izraelem a Egiptem. W dniu 12 października 2004 r. przesyłkę zawierająca bombę otrzymał polski Konsul Generalny w Monachium. W tym samym czasie podłożono jeszcze 6 podobnych przesyłek skierowanych do polityków i przedstawicieli władz samorządowych. Niemiecka policja uznała za wysoce prawdopodobny udział w wyżej wymienionych zamachach jednej z terrorystycznych organizacji muzułmańskich. W 2010 r. tą formą terroryzmu posłużyły się skrajna lewica i grupy anarchistyczne. W Atenach w listopadzie 2010 r. lewackie ugrupowanie Konspiracja Grup (Komórek) Ogniowych przesłało na adres placówek dyplomatycznych Rosji i Szwajcarii paczki, które wybuchły podczas otwierania. Kolejne przesyłki skierowane były do ambasad Bułgarii, Chile, Niemiec, Holandii, Belgii i Meksyku oraz do parlamentu Grecji. Paczki zostały przejęte przez operatora i służby bezpieczeństwa. Tylko jedna z nich eksplodowała, raniąc pracownicę firmy kurierskiej. Jednocześnie terroryści nadali przesyłki do Prezydenta Francji, Kanclerz Niemiec, Premiera Włoch oraz instytucji Europolu w Hadze i Trybunału Sprawiedliwości w Strasburgu.

Identyczny scenariusz rozegrał się nastepnie w drugiej połowie grudnia 2010 r. w Rzymie, gdzie anarchistyczna organizacja pod nazwą Nieformalna Federacja Anar-

chistyczna (FAI), rewolucyjna komórka im. Lambrosa Fountasa (nazwa ugrupowania nawiązuje do greckiego anarchisty L. Fountasa, zastrzelonego przez policję w Atenach w marcu 2010 r.) przesłała do placówek dyplomatycznych Szwajcarii i Chile paczki zawierające ładunki wybuchowe. Eksplozje będące skutkiem otwarcia przesyłek poważnie raniły dwóch pracowników tych przedstawicielstw. FAI przyznała się do zorganizowania zamachu, przesyłając list ze stosownym oświadczeniem ideologicznym. Jednocześnie do kolejnych tego typu incydentów doszło w rzymskich ambasadach Grecji, Ukrainy, Wenezueli, Danii, Irlandii i Monaco oraz w placówce Unii Europejskiej w Bernie. Tylko pierwsza z nich zawierała materiał wybuchowy. Zawartość pozostałych paczek stanowiły pojedyncze egzemplarze książek i kart pocztowych. Podobny pakunek został odnaleziony w tym samym okresie w rzymskim metrze, jednakże tym razem paczka zawierała materiał wybuchowy. Brakowało tylko zapalnika umożliwiającego zainicjowanie eksplozji. Należy podkreślić, iż Nieformalna Federacja Anarchistyczna rozpoczynała swoją działalność terrorystyczną w 2003 r., właśnie od przesłania niegroźnej, jak się okazało, bomby zapalającej na prywatny adres ówczesnego przewodniczącego Komisji Europejskiej, Romano Prodiego, w Bolonii[4].

Początek XXI w. rozwinął w pełni nową formę przestępczego wykorzystania obrotu pocztowego – listy ze śmiertelną trucizną. W dniu 18 września 2001 r. (tuż po zamachach na WTC w Nowym Jorku) amerykański biolog wojskowy wysłał z miejscowości New Jersey pięć listów zawierających przetrwalniki wąglika (*Bacillus anthracis*) do trzech stacji telewizyjnych i redakcji dwóch popularnych gazet. W wyniku zakażenia zmarło 5 osób (w tym 2 pracowników poczty amerykańskiej), a siedemnaście poważnie zachorowało. Trzy tygodnie później listy z bakteriami oraz zawartym na kartce islamskim przesłaniem otrzymali dwaj senatorzy Partii Demokratycznej. Skala psychozy, jaka powstała w wyniku tych wydarzeń w USA, a następnie na całym świecie, w tym również w Polsce, była nieporównywalna z żadną inną tego typu sytuacją. Możliwość anonimowego przesłania innej osobie śmiercionośnego proszku oddziaływała na wyobraźnię i paraliżowała przy każdym kontakcie z korespondencją w formie pisemnej. W naszym kraju również Poczta Polska odnotowała kilkadziesiąt alarmów związanych z podejrzeniem przesyłania pakunku zawierającego substancję trującą przypominającą wąglik. Potwierdzeniem możliwości rozwoju i aktualności problematyki bioterroryzmu związanego z wykorzystaniem kanału pocztowego jest przypadek z 30 lipca 2010 r., kiedy to trzech pracowników ambasady USA w Paryżu zatruło się nieznaną substancją znajdującą się w nadesłanej przesyłce. 13 września 2010 r. natomiast niezidentyfikowany proszek został wykryty w sali Izby Reprezentantów. Tego dnia amerykański Kongres miał wznowić prace legislacyjne po wakacyjnej przerwie.

W przypadku tzw. terroryzmu mafijnego istota przestępstwa związana jest z porachunkami pomiędzy gangami, mafiami i grupami przestępczymi. Ta forma przemocy może być również ukierunkowana na instytucje i urzędy państwowe. Wykonanie przesyłki zawierającej ładunek wybuchowy jest stosunkowo łatwe. Niewielki problem mogą stanowić jedynie specjalne zapalniki, które uniemożliwiają przypadkową detonację, np. w czasie sortowania przesyłek w rozdzielni pocztowej. Należy zwrócić uwagę, że bomby listowe są konstruowane w taki sposób, by do eksplozji dochodziło w momencie otwierania przesyłki przez adresata. Moc wybuchu zależy od ilości i jakości

[4] P. Kowalczuk, *Anarchiści uderzyli na ambasady w Rzymie*, „Rzeczpospolita" z 24.12.2010 r.

użytego materiału wybuchowego, natomiast obrażenia ciała zależą od kierunku wybuchu. Szczególnie niebezpieczne są eksplozje skierowane na twarz i szyję, ponieważ w czasie wybuchu „odłamkami" stają się fragmenty dłoni. Znowelizowana ostatnio ustawa o broni i amunicji umożliwia zakup broni i amunicji w sklepach internetowych oraz ich przesyłanie za pośrednictwem operatorów pocztowych[5]. Ten akt prawny dopuszcza także obrót materiałami wybuchowymi oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym. Praktyka pokaże, czy przyjęte zabezpieczenie transakcji w postaci podpisu elektronicznego będzie uniemożliwiało nadużycia w tej sferze usług.

Trzecią grupą zamachów dokonywanych przy użyciu przesyłek pocztowych jest tzw. terroryzm indywidualny. Ukierunkowany jest on głównie na zamachy wobec osób (np. porachunki osobiste). Zdarzają się także przypadki tzw. samotnej walki z systemem. Przesyłki używane w tej formie terroryzmu charakteryzują się małą siłą rażenia i skonstruowane są z prymitywnych, powszechnie dostępnych materiałów. Ta z pozoru niegroźna definicja grupy przestępstw kryje wiele przykładów ludzkich tragedii, ale także pomysłowości przestępców wykorzystujących tę formę szantażu, zemsty, zamanifestowania ideologii czy wprost choroby umysłowej. Doskonałym przykładem może być profesor matematyki z Uniwersytetu Michigan, anarchista i ekolog – Theodor Kaczyński („Unabomber"), który w latach 1979 - 1995 wysyłał do różnych instytucji w Stanach Zjednoczonych paczki z zawartością wybuchową. W wyniku jego „działalności" śmierć poniosły 3 osoby, a 23 zostały ranne.

Kanał łączności pocztowej można wykorzystać również do informowania władz o prowadzonej działalności przestępczej. W 1994 r. Sylwester Augustynek – „Gumiś" – podłożył ładunki wybuchowe w trzech kościołach i na dworcu kolejowym w Krakowie, żądając od władz miasta 500 tys. zł w niemieckich markach. Uzyskanie informacji wyprzedzających dzięki przejęciu korespondencji terrorysty do różnych organów prasowych, w której informował o swoich zamierzeniach, stawiając nowe warunki i żądania, pozwoliło na zyskanie czasu umożliwiającego podjęcie działań niezbędnych dla zminimalizowania skutków ewentualnego wybuchu oraz ewakuacji.

Podobny scenariusz rozegrał się w Republice Czeskiej, gdzie wiosną 2003 r. niezrównoważony umysłowo mężczyzna notorycznie szantażował państwo groźbą wysadzenia w powietrze mostów kolejowych. Na potwierdzenie swojej działalności ujawnił ładunek wybuchowy umieszczony pod mostem w miejscowości Ołomuniec na trasie Praga–Warszawa. Bomba zawierała śruby, gwoździe i inne elementy stalowe. Szantażysta kontaktował się z władzami poprzez listy, w których umieszczał swoje żądania. Tego typu działalność przestępcza nie należy, niestety, wyłącznie do przeszłości. W dniu 23 sierpnia 2010 r. w Wydziale Przesyłek Niedoręczalnych w Koluszkach przeprowadzona została pirotechniczna neutralizacja paczki, która zawierała ładunek wybuchowy. Niezbędna była pełna ewakuacja pracowników i klientów urzędu. W akcji, poza antyterrorystami, brali udział strażacy i policjanci.

Prasa wielokrotnie opisywała przypadki przesyłania do osób piastujących najwyższe funkcje w państwie anonimowych listów zawierających teksty obraźliwe i szkalujące, a nawet zawierające elementy amunicji. W lutym 2007 r. na adres Kancelarii Premiera została doręczona przesyłka kierowana do Prezesa Rady Ministrów

[5] *Ustawa z dnia 5 stycznia 2011 r. o zmianie ustawy o broni i amunicji oraz ustawy o wykonywaniu działalności gospodarczej w zakresie wytwarzania i obrotu materiałami wybuchowymi, bronią, amunicją oraz wyrobami i technologią o przeznaczeniu wojskowym lub policyjnym*, Dz.U. z 2011 r., Nr 38, poz. 195.

RP, której zawartość stanowiły trzy sztuki ostrej amunicji oraz kartka z „instrukcją", jak je wykorzystać. W kwietniu 2009 r. na adres biura Prezydenta Francji nadszedł list również zawierający groźby i dwa małokalibrowe naboje. Podobną korespondencję otrzymało kilku ministrów francuskiego rządu. W toku śledztwa prowadzonego po zabójstwie asystenta europosła PiS w Łodzi w październiku 2010 r. ujawniono, iż w okresie poprzedzającym tragiczne zdarzenie do przewodniczącego Sojuszu Lewicy Demokratycznej przychodziły anonimowe listy pisane niezdarnym charakterem, zawierające między innymi groźby typu „zamorduję cię"[6]. Traktowanie tego typu sytuacji z należytą powagą jest niezwykle istotne z uwagi na stosunkową łatwość skonstruowania prostych ładunków wybuchowych. W internecie bez większych problemów można znaleźć stosowne instrukcje.

Rozwój rynku usług pocztowo-kurierskich

Przedstawione powyżej różnorodne formy przestępczego wykorzystania obrotu pocztowo-kurierskiego, poparte ze zrozumiałych względów tylko wybranymi przykładami, wpisują się w przestrzeń niezwykle prężnie rozwijającej się branży usług pocztowych. Na tym rynku w okresie ostatnich dwudziestu lat zmieniło się niemal wszystko. Poza operatorem narodowym pojawili się konkurenci: duże międzynarodowe koncerny oraz lokalni przedsiębiorcy. W 1996 r. usługi pocztowo-kurierskie świadczyło 15 firm komercyjnych, w 2009 natomiast ich liczba wzrosła do 209[7]. Realizowana przez Unię Europejską liberalizacja rynku pocztowego spowodowała, że od roku 2013 przestanie obowiązywać formuła obszaru zastrzeżonego dla przesyłek do 50 gramów, które dotychczas mógł przewozić wyłącznie operator narodowy. Aktualnie konkurenci Poczty Polskiej S.A. stosują różne formy omijania ustawowych ograniczeń wagowych i cenowych. Polegają one m.in. na dociążaniu przesyłek materiałem reklamowym w postaci fragmentu blaszki lub brulionu oraz stosują opakowania (koperty), które ważą ponad 50 gramów. Zdaniem Prezesa Urzędu Komunikacji Elektronicznej *pomimo stosowania tego rodzaju praktyki, to brak jest podstaw do stwierdzenia, że podejmowanie takich działań narusza przepis art. 47 Prawa pocztowego*[8]. W praktyce stwarza to pełną konkurencyjność, ale jednocześnie oznacza, że rynek pocztowy jest dynamicznie rozwijającą się strefa gospodarki. Potencjalny przestępca będzie miał możliwość wysłania przysłowiowej widokówki poprzez innego operatora niż Poczta Polska S.A.

W omawianym okresie zmieniła się także liczba oferowanych przez pocztę usług, sposób ich wykonywania i przemieszczania przesyłek (usługa „od drzwi do drzwi", poczta hybrydowa, przekierowanie korespondencji, odejście od kolejowych ambulansów pocztowych itd.). Wymagania związane z szybkością przekazania przesyłki od nadawcy do odbiorcy spowodowały wdrożenie na dużą skalę informatyzacji technologii pocztowej (np. śledzenia przesyłek przy użyciu internetu) oraz wprowadzenie maszyn i urządzeń do automatycznego sortowania przesyłek listowych oraz paczkowych. Również na etapie doręczania zachodzą znaczące zmiany podyktowane konkurencyjnością i dostępnością (np. doręczanie przesyłek w godzinach wieczornych czy działa-

[6] D. Szyller, M. Święchowicz, *Chroń się, kto może, w BOR-ze,* „Przekrój" z dnia 02.11.2010 r.

[7] *Raport Prezesa UKE o stanie rynku usług pocztowych w Polsce w 2009 roku*, Warszawa 2010, Urząd Komunikacji Elektronicznej.

[8] *Raport Prezesa UKE dot. kontroli prywatnych operatorów pocztowych*, BIP [dostęp: 30.01.2010].

nie całodobowych paczkomatów rozmieszczonych na stacjach benzynowych (informacje o odbiorze przesyłki przekazywane są przy pomocy usługi SMS). Należy brać pod uwagę, że poziom oferowanych usług pocztowych, ich różnorodność oraz duża skala wymusi na operatorach stosowanie coraz bardziej zaawansowanych i wyrafinowanych technik, które jednak nigdy nie wyeliminują znaczącej roli czynnika ludzkiego. Dlatego nie można np. porównywać rynku usług telekomunikacyjnych z pocztowymi, ponieważ te drugie nigdy do końca nie zostaną w pełni zinformatyzowane i zautomatyzowane. Zawsze będziemy mieli do czynienia z fizycznym dostarczaniem przesyłki do maszyny czy do adresata przez człowieka. Aktualnie podmioty prowadzące działalność pocztową winny dążyć do właściwego zrozumienia problematyki bezpieczeństwa obrotu pocztowego. Pozwoli to na skuteczniejsze rozpoznanie i przeciwdziałanie wykorzystywaniu usług pocztowych do działalności przestępczej.

W świetle przedstawionych powyżej faktów można śmiało postawić tezę, że obrót pocztowo-kurierski jest wykorzystywany do działalności przestępczej lub może stanowić bezpośrednie zagrożenie o charakterze terrorystycznym czy bioterrorystycznym. Bezpieczeństwo państwa i jego obywateli, szczególnie w perspektywie zbliżającej się prezydencji Polski w Unii Europejskiej oraz organizacji turnieju piłkarskiego Euro 2012 wymaga, aby problematykę zabezpieczenia tego obrotu przed jego przestępczym wykorzystaniem potraktować szerzej i uznać za jeden z istotnych elementów w przeciwdziałaniu zagrożeniom mogącym wystąpić w tym obszarze.

Streszczenie

Artykuł stanowi próbę przybliżenia problemu występowania w obrocie pocztowo-kurierskim zagrożeń dla bezpieczeństwa państwa i obywateli. Zostały tu zdefiniowane podstawowe formy wykorzystania łączności pocztowej do działalności przestępczej, takie jak: łączność utajniona, przemyt narkotyków, kontrabanda pocztowa czy terroryzm pocztowy wykorzystujący przesyłki wybuchowe lub zawierajace niebezpieczne bakterie i wirusy. Wieloletnie doświadczenie zawodowe autorów wskazuje, że kontrola korespondencji jest często niedocenioną formą zdobywania informacji. Świadczą o tym przykłady dokonywanych przestępstw z wykorzystaniem usług pocztowo-kurierskich oraz możliwości w tym zakresie, jakie płyną z ciągłego wzrostu wolumenu przesyłek, wysyłanych ze sklepów internetowych.

Summary

The article is an attempt to bring to the attention some dangers connected with the postal and courier services which can pose a threat to national and individual security. It defines the basic forms of misuse of postal services for criminal activity such as: clandestine communications, drug smuggling and postal contraband, terrorism in the form of letter bombs or dangerous bacteria and viruses. The authors have had many years of professional experience and indicate that the control of correspondence is very often not fully appreciated source of information. The thesis is confirmed by the examples of criminal activity conducted with the use of postal and courier service. The opportunities in this area increase continuously due to the growth in the number of parcels sent from online shops.

.

IV
TECHNIKA, TECHNOLOGIA I BEZPIECZEŃSTWO INFORMATYCZNE

Brunon Czabok

Dezinformacja w telekomunikacji

W przeszłości jedynym, a dziś nadal najbardziej popularnym, sposobem identyfikacji stron połączenia telefonicznego jest przedstawianie się osoby inicjującej połączenie, zwanej zwyczajowo abonentem A i potwierdzenie w trakcie rozmowy, iż osoba odbierająca połączenie (abonent B) jest jego właściwym adresatem. Oferowana obecnie wierność przekazywanych sygnałów akustycznych dodatkowo umożliwia znającym się abonentom rozpoznawanie siebie nawzajem na podstawie charakterystycznych cech głosu. Jest to dość skuteczna metoda, chociaż z pewnością każdemu zdarzały się pomyłki związane z błędnie rozpoznanym głosem rozmówcy. Wynika to z ograniczonego pasma przenoszenia sygnału akustycznego w sieciach telekomunikacyjnych (od 300 Hz do 3400 Hz), mimo że rzeczywisty zakres widma mowy rozciąga się od około l00 Hz do ponad 8000 Hz. Pasmo telefoniczne zostało tak dobrane, aby zapewniać zrozumiałość mowy, jednak eliminuje ono pewne częstotliwości, zmieniając charakterystyczny dla poszczególnych mówców ton i barwę głosu. Gdy do tego dodamy szumy i zniekształcenia powstałe w trakcie transmisji oraz konwersji sygnału z postaci analogowej na cyfrową i odwrotnie, to mylna identyfikacja abonenta staje się możliwa. Dlatego wyspecjalizowane służby często wykorzystują hasła lub kryptograficzne metody zapewniające uwierzytelnienie stron komunikacji elektronicznej. Przeciętny użytkownik nie stosuje tak wyrafinowanych metod weryfikacji drugiego abonenta, ale współczesne systemy telekomunikacyjne oferują daleko idącą pomoc w zakresie identyfikacji abonentów dzięki rozpowszechnieniu usługi CLIP (ang. *Calling Line Identification Presentation*), czyli prezentacji numeru połączenia przychodzącego. Sieci zintegrowane cyfrowo wykorzystują specjalny kanał sygnalizacyjny, w którym przekazywane są dane niezbędne do prawidłowej obsługi połączeń. Jest tam też miejsce na numer abonenta A oraz abonenta B. Postęp techniczny sprawił, że coraz trudniej jest znaleźć telefon bez wyświetlacza, na którym może być prezentowany numer abonenta A, o ile ten nie włączył usługi CLIR (ang. *Calling Line ldentification Restriction*), tzn. nie zastrzegł swojego numeru. Oczywiście, zastrzeżenie numeru nie eliminuje go z danych zawartych w protokole sygnalizacyjnym, a jedynie zawiera dodatkową informację dla centrali końcowej, aby nie udostępniać abonentowi B prezentacji numeru. Skoncentrujmy się jednak na najczęściej spotykanym przypadku, kiedy abonent A nie ukrywa swego numeru.

Popularność usługi CLIP wprowadziła już pewne zmiany w zasadach telefonicznego savoir-vivre'u, polegające na odstąpieniu od wspomnianego na początku przedstawiania się w przypadku, gdy dzwonimy do osób znających nasz numer, np. mających go w książce telefonicznej swojego aparatu. Widząc na wyświetlaczu nazwisko znajomego albo prezentujący się numer abonenta połączenia przychodzącego lub też nadawcy SMS-a, wierzymy w jego prawdziwość, tak jak w wynik działania wykonanego na kalkulatorze. I niestety, czasem nasze zaufanie jest nadużywane. Prezentowany numer nie jest wynikiem działania prostego algorytmu (jak np. w kalkulatorze), lecz jest przekazywany z sieci do sieci. Współczesne systemy telekomunikacyjne posiadają punkty transferu sygnalizacji (ang. *Signal Transfer Point* – STP). Sieć przyjmująca połączenie nie weryfikuje numeru abonenta A, tylko prezentuje go swojemu abonentowi końcowemu (B) lub przekazuje dalej do kolejnej sieci. Każdy na pewno pamięta przed-

szkolną zabawę w „głuchy telefon" – im dłuższy jest łańcuch pośredników, tym bardziej zniekształcona zostaje informacja końcowa. Przykład jest oczywiście przejaskrawiony, gdyż nawet w przypadku połączeń międzynarodowych rzadko się zdarza, aby na drodze połączenia znalazło się więcej niż 3 operatorów. Wystarczy jednak, że jeden będzie nierzetelny i podmieni lub ustawi atrybut numeru jako zastrzeżony i na naszym wyświetlaczu pojawi się fałszywa informacja. Dezinformacja ta może być zamierzona lub powstać jako skutek uboczny zastosowanych technologii przekazywania ruchu pomiędzy sieciami poszczególnych operatorów.

Dezinformacja zamierzona

W pierwszym przypadku mamy do czynienia z sytuacją, kiedy abonent inicjujący połączenie świadomie wprowadza nieprawdziwy numer. Protokoły sygnalizacji korygują tylko elementarne błędy na poziomie transmisji pakietów, lecz, jak już wspomniano, nie zawierają mechanizmów weryfikacji numeru. We współczesnych sieciach cyfrowych powszechnie wykorzystywany jest protokół SS7 (ang. *Signaling System No. 7)*[1], który został opublikowany w 1981 r. Prawdopodobnie nie kładziono wtedy tak dużego nacisku na uwierzytelnianie i kontrolę integralności danych. W każdym razie, protokół ten jest podatny na ingerencję, a w szczególności daje możliwość wprowadzania dowolnych danych do obszaru identyfikującego abonenta A. Jest to wykorzystywane przez podmioty, które wyspecjalizowały się w spoofingu[2].

Polski przedsiębiorca z Nysy w dniu 1 czerwca 2009 r. uruchomił serwis internetowy www.wykrecnumer.pl, który oprócz usług komunikacyjnych, takich jak wysyłanie SMS-ów i prowadzenie rozmów telefonicznych w technologii VoIP[3], oferował usługę dowolnej edycji numeru inicjującego. Na podstawie złożonego przez ABW zawiadomienia o popełnieniu przestępstwa sprawą zajęła się Prokuratura Okręgowa w Opolu, której działania doprowadziły do likwidacji serwisu z dniem 04.11.2009 r., jego właścicielowi zaś, a zarazem administratorowi, postawiono zarzuty popełnienia przestępstwa z art. art. 269 § 1 kk, 287 § 1 kk, 268 §§ 1 i 2 kk, 268a § 1 kk, 269a kk, 269b § 1 kk w zw. z art. art. 11 § 2 kk i 12 kk. W grudniu 2010 r. właściciel serwisu został formalnie oskarżony m.in. o to, że nie będąc do tego upoważnionym, dokonywał zmian istotnych danych informatycznych w postaci informacji o numerach telefonów wywołujących połączenie, mających szczególne znaczenie dla obronności kraju i funkcjonowania instytucji państwowych, których celem jest obrona porządku prawnego, oraz bezprawnie wpływał – a przez to również zakłócał – na automatyczne przetwarzanie, gromadzenie i przekazywanie przez operatorów sieci wyżej wymienionych danych, co spowodowało potencjalne zagrożenia dla skutecznej realizacji zadań z zakresu obronności, bezpieczeństwa oraz ochrony porządku publicznego państwa. Za to przestępstwo prokurator zażądał kary 2 lat pozbawienia wolności. Na podstawie art. 335 § 1 kpk oskarżony zgodził się na dobrowolne poddanie się karze łącznej (postępo-

[1] Jest wiele publikacji przybliżających protokół SS7; autor artykułu posiłkował się książką D. Kościelnika, pt. *ISDN – cyfrowe sieci zintegrowane usługowo*, Warszawa 2007, WKiŁ.

[2] Spoofing (ang. *spoof* – oszukiwać, imitować, parodiować) – określenie, które w dziedzinie IT pojawiło się jako termin oznaczający podszywanie się pod inny numer IP, tzw. *IP spoofing*.

[3] Z ang. *Voice over Internet Protocol* – technologia umożliwiająca przesyłanie głosu za pomocą łączy internetowych lub innych sieci wykorzystujących protokół IP.

wanie obejmowało również inne przestępstwa) 4 lat pozbawienia wolności z warunkowym zawieszeniem jej wykonania na okres próbny 6 lat oraz karze grzywny. W tej sprawie istotny jest również fakt, iż w ramach śledztwa prokurator zabezpieczył dyski komputerowe, na których zostały zarejestrowane dane związane z zestawianiem poszczególnych połączeń i wysyłaniem SMS-ów. Może to mieć znaczenie w przypadku ewentualnych śledztw w sprawie przestępstw popełnionych przy pomocy korzystania z serwisu www.wykrecnumer.pl, gdyż dane te pozwalają na ustalenie, kto był sprawcą przestępstwa, tzn. jaki numer był podmieniony, jaki był prezentowany na dalszej drodze połączenia i kiedy miało to miejsce. Z danych tych wynika, że najczęściej podszywano się pod numer 997.

Serwis został zlikwidowany, a sprawca, niezależnie od tego, czy sąd przychyli się do wniosku o dobrowolne poddanie się karze, czy też przeprowadzi rozprawę, niewątpliwie zostanie ukarany. Jest to niekwestionowany sukces polskiego wymiaru sprawiedliwości, ale zwycięstwo w tym jednym przypadku nie przesądza o sukcesie w walce z całym procederem. Ze względu na możliwość udostępniania tego typu usług za pośrednictwem internetu, który nie respektuje granic państwowych, przeciwdziałanie temu zjawisku jest trudne i w związku z tym nadal istnieje możliwość korzystania z usług przedsiębiorców oferujących podmianę numeru. Intencją autora artykułu nie jest promowanie tego typu usług, dlatego nie zostaną tu przytoczone konkretne adresy, jednakże po wpisaniu w wyszukiwarkę hasła np. „ID spoofing" można bez trudu znaleźć kilkanaście serwisów umożliwiających wysyłanie SMS-ów lub telefonowanie z jednoczesnym podszywaniem się pod wybrany numer. Analogiczna sytuacja dotyczy również poczty elektronicznej oraz adresów IP.

Wyżej wymieniony proceder jest bardzo niebezpieczny, pozwala bowiem oszustom podszywać się nie tylko pod numery osób fizycznych, ale również ważnych instytucji (m.in. Policji, Straży Pożarnej) oraz firm, w szczególności banków, by w ten sposób wyłudzić cenne informacje lub wpływać na zachowanie się ofiary oszustwa. Możliwość podszywania się pod dowolny numer nie tylko daje duże możliwości popełniania przestępstw w sferze gospodarczej i obyczajowej, ale też może wprowadzać w błąd wymiar sprawiedliwości, służby odpowiedzialne za bezpieczeństwo państwa i bezpieczeństwo publiczne oraz poważnie utrudniać im pracę. Na podstawie ustawowych uprawnień podmioty te często przeprowadzają analizę raportów połączeń (bilingów). Raport połączeń przychodzących zawiera takie numery, jakie zostały dostarczone za pomocą protokołu sygnalizacyjnego przedsiębiorcy telekomunikacyjnemu obsługującemu abonenta B. Gdy będziemy mieli do czynienia ze *spoofingiem*, będą to numery nieprawdziwe, wprowadzające dany organ w błąd. Fałszywe numery na bilingu mogą bardzo skomplikować przedsięwzięcia operacyjne, śledcze czy analityczne, nawet gdy daną sprawą zajmuje się doświadczony oficer. Ustalenie prawdy obiektywnej absorbuje siły, środki, a przede wszystkim czas, więc nietrudno dowieść, że negatywnie wpływa to na bezpieczeństwo. Spreparowane numery mogą również podważyć znaczenie bilingu jako dowodu w procesie sądowym. Aby mieć absolutną pewność co do danych zawartych w raporcie połączeń, należy zestawić dane zawarte w bilingu przychodzącym z danymi z bilingów wychodzących poszczególnych numerów. Przedstawione metody podszywania się pod dowolny numer nie wpływają na wiarygodność bilingu wychodzącego. Każdy przedsiębiorca telekomunikacyjny, również w swoim interesie, skrupulatnie rejestruje połączenia generowane przez abonentów korzystających z zakończeń jego sieci, dlatego biling połączeń wychodzących pozostaje wiarygodnym źródłem informacji. Należy jednak dodać, że jest on dostępny w zasadzie tylko w przy-

padku połączeń generowanych przez abonentów przedsiębiorców telekomunikacyjnych prowadzących działalność na terenie RP[4].

Dezinformacja niezamierzona

Zdarzają się również sytuacje, kiedy w rejestrze połączeń przychodzących zapisywane są numery inne niż te należące do abonenta inicjującego połączenie bez jego złej woli i, w większości przypadków, bez jego wiedzy. Taka sytuacja występuje podczas stosowania bramek GSM lub wykorzystywania central końcowych do nielegalnego terminowania ruchu międzynarodowego w krajowych sieciach stacjonarnych. Transfer ruchu zagranicznego z pominięciem przeznaczonych do tego międzyoperatorskich łączy telekomunikacyjnych (interkonekt) stanowi podstawową przyczynę pojawiania się fałszywych danych w rejestrach połączeń przychodzących, przez co bardzo negatywnie wpływa na wiarygodność danych zapisywanych w systemach bilingowych. Być może określenie d e z i n f o r m a c j a n i e z a m i e r z o n a jest zbyt eufemistyczne, gdyż podmioty realizujące tego typu usługi wiedzą, że fałszują numer abonenta inicjującego połączenie, i godzą się na to. Jednak nie ulega wątpliwości, że gdyby technologia przekazywania połączeń za pomocą bramek GSM lub systemów konwertujących ruch przesyłany za pośrednictwem internetu do telefonicznych sieci stacjonarnych pozwalała przenosić pierwotny numer abonenta A, to byłoby to powszechnie praktykowane.

Nielegalne kierowanie ruchu zagranicznego bezpośrednio do sieci stacjonarnej wymaga zestawienia łącza o dużej przepustowości do jednego z krajowych operatorów sieci stacjonarnej oraz świadczenia innych usług telekomunikacyjnych pozwalających uzasadnić podpisanie umowy i budowę wspomnianego łącza. Ten sposób nielegalnego terminowania ruchu zagranicznego jest zazwyczaj realizowany przez przedsiębiorców telekomunikacyjnych, którzy wykraczają poza ramy umów podpisanych z operatorami stacjonarnymi, niejako „przemycając" ruch międzynarodowy łączem przeznaczonym do obsługi ruchu lokalnego. W procesie tym prawdziwy numer abonenta A jest zastępowany numerem krajowym z puli numeracji wykupionej przez operatora nielegalnie transferującego ruch lub numerem fikcyjnym, niezwiązanym z żadnym zakończeniem sieci. Przypadki terminowania ruchu „z internetu" bezpośrednio do sieci telefonii stacjonarnej są o wiele rzadsze niż poprzez bramki GSM. Dlatego dalsze rozważania będą dotyczyły przypadków wykorzystywania właśnie tych bramek, zwanych również FCT-ami[5] lub SIMBOX-ami[6]. Należy jednak mieć na uwadze fakt, że w obydwu technologiach nielegalnego transferowania ruchu rezultatem tego procederu jest rejestracja fałszywych danych w bilingu przychodzącym oraz nieprawdziwa informacja pojawiająca się na wyświetlaczu aparatu abonenta B.

U schyłku lat 90. XX wieku nikt nie widział zagrożenia w stosowaniu bramek GSM w centralkach PBX (ang. *Private Branch Exchange*), a sami operatorzy mobilni zachęcali klientów do tego typu rozwiązań. Pozwalało to obniżyć koszt połączeń do sieci mobilnych oraz zapewniało redundantne wyjście do sieci publicznej na wypadek awa-

[4] W niektórych przypadkach można wystąpić w tym zakresie o pomoc do odpowiednich instytucji zagranicznych, ale ze względu na czasochłonność procedur w zestawieniu z krótkim okresem retencji danych, zazwyczaj jest to nieskuteczne.

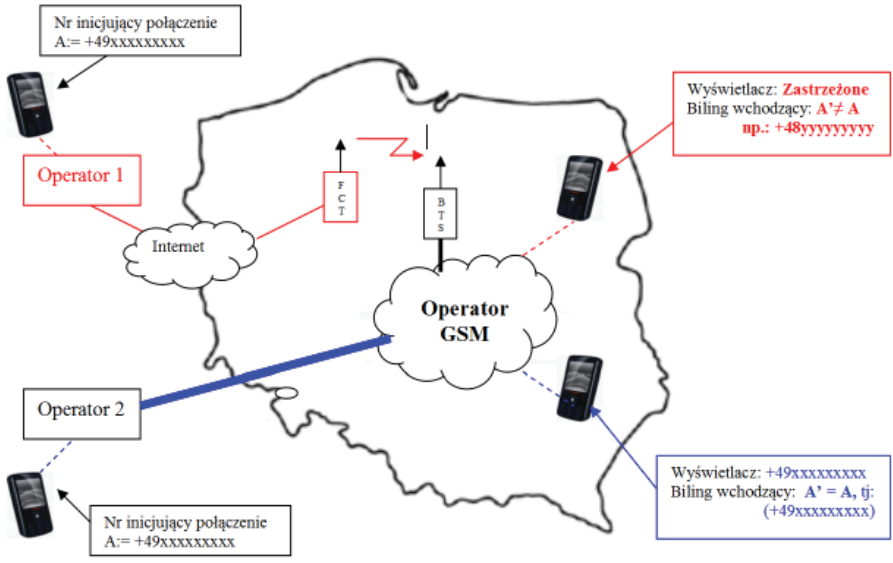
[5] FCT (ang. *Fixed Cellural Terminal*) – stacjonarny terminal komórkowy.

[6] SIMBOX – od nazwy karty SIM (ang. *Subscriber Identity Module*) oraz od ang. słowa *'box'* – skrzynka, czyli urządzenie elektroniczne umożliwiające współpracę z kartami SIM.

rii łącza przewodowego. Tego typu wykorzystanie FCT-ów jest nadal bardzo popularne i powszechnie akceptowane. W takich przypadkach trudno doszukać się jakichkolwiek uchybień prawnych, gdyż w bramkach wykorzystywane są zazwyczaj karty SIM zakupione w ramach umów abonamentowych zawartych z operatorem komórkowym przez podmiot, który za pomocą bramki udostępnia usługi dostępu do sieci mobilnych tylko abonentom wewnętrznym swojej centralki zakładowej. Połączenie z aparatu stacjonarnego na telefon komórkowy zawsze było droższe niż z jednego aparatu komórkowego na drugi, szczególnie gdy te znajdowały się w sieci jednego operatora. Uwzględniając darmowe minuty lub oferowane w niektórych taryfach darmowe połączenia wewnątrz sieci, warto podłączyć do centralki zakładowej np. cztery bramki GSM lub jedno urządzenie FCT z kilkoma kartami SIM, tj. po jednej dla każdego operatora mobilnego.

Ekspansja sieci komórkowych i wprowadzona przez operatorów komórkowych konkurencja cenowa sprawiły, że pojawiły się podmioty, które dostrzegły możliwość zarobkowania na różnicy wysokości stawek pomiędzy połączeniami z sieci stacjonarnej do mobilnej (F2M), a połączeniami wewnątrz sieci mobilnej (M2M). Innym bardzo istotnym czynnikiem dla rozwoju usług terminowania ruchu za pomocą bramek FCT był rozwój technologii VoIP, który dodatkowo pozwolił omijać drogie łącza międzynarodowe.

Najpowszechniejszy model działania przedsiębiorcy terminującego ruch za pomocą FCT-ów przedstawiono na zamieszczonym niżej rysunku.



Rys. 1. Schemat konwencjonalnej i terminowanej za pomocą FCT-u drogi połączeniowej. Kolorem czerwonym zaznaczono typową drogę połączenia nielegalnie terminowanego za pomocą urządzenia FCT, niebieskim zaś standartową drogę połączenia zestawionego z wykorzystaniem oficjalnych łączy międzyoperatorskich (interkonekt).

Same urządzenia FCT również ewoluowały od prostego interfejsu pozwalającego podłączyć zwykły telefon komórkowy, poprzez oferowane przez producentów central telefonicznych dedykowane karty z anteną i slotem na kartę SIM, aż po terminale

o dużej przepustowości, umożliwiające obsługę dużej liczby kart SIM. W stosunku do tych ostatnich bardziej pasuje określenie SIMBOX, odróżniające je od prostych urządzeń zwanych bramkami lub ogólnie FCT-ami. Należy jednak zastrzec, że w literaturze brak jednoznacznego potwierdzenia dla takiego podziału nazewnictwa. Najbardziej zaawansowane są serwery SIM, czyli SIMBOX-y, w których oddzielono część radiową urządzenia od pozostałej części obsługującej karty SIM. Na rynku dostępne są serwery wyposażone w oprogramowanie ułatwiające zarządzanie (badanie stanu kont, rotacyjne wykorzystywanie, analiza ruchu) tysiącami kart SIM zainstalowanymi w jednym miejscu. Jako moduły radiowe mogą służyć zwykłe telefony GSM, do których zamiast karty podłączany jest emulator SIM pobierający uprawnienia z kart zainstalowanych w serwerze za pomocą modułu SIM-klient, wykorzystującego protokół transmisyjny TCP/IP (ang. *Transmission Control Protocol/ Internet Protocol*)[7]. Daje to nie tylko możliwość manipulacji numerami (kartami SIM), ale również informacją o położeniu urządzenia końcowego. Zgodnie z przepisami[8] przedsiębiorca telekomunikacyjny musi udostępniać uprawnionym podmiotom informacje dotyczące lokalizacji zakończenia sieci. W przypadku serwerów SIM operator sieci komórkowej zarejestruje geograficzne położenie modułu radiowego, który kontaktował się z pozostającym w jego sieci BTS-em (ang. *Base Transceiver Station*), przy czym sam serwer z kartami SIM może być oddalony o setki kilometrów, gdyż dane z karty SIM niezbędne do logowania się do sieci komórkowej mogą być przesyłane za pomocą sieci WAN (ang. *Wide Area Network*). W takim przypadku operator sieci komórkowej może na przykład zarejestrować połączenie zrealizowane za pośrednictwem BTS-u zlokalizowanego w Warszawie, a już po kilku minutach „ten sam telefon" zaloguje się do BTS-u zlokalizowanego w Krakowie.

Przedstawione wyżej czynniki ekonomiczne i techniczne doprowadziły do pojawienia się na tyle dużej liczby podmiotów obsługujących ruch F2M za pomocą bramek GSM, że zjawisko to stało się dokuczliwe dla dużych operatorów, którzy zaczęli ponosić wymierne straty finansowe. W przypadku operatorów komórkowych zaś zaczęło się to niekorzystnie odbijać na ich wizerunku, gdyż FCT-y mają negatywny wpływ na jakość usług telefonicznych. Najwięksi operatorzy, w trosce o swoje interesy, podjęli różne próby zwalczania tego problemu (poprzez restrykcyjne zapisy w umowach, blokowanie kart *prepaid*, lobbing czy spory sądowe). Skala tego zjawiska była i nadal jest trudna do precyzyjnego określenia, gdyż większość podmiotów terminujących ruch za pomocą FCT-ów w ogóle nie jest zarejestrowana jako przedsiębiorcy telekomunikacyjni i prowadzi działalność niezgodną z przepisami[9]. Problem ten dostrzegł również Urząd Komunikacji Elektronicznej, który w lipcu 2007 r. zajął oficjalne stanowisko[10] i jako podłoże takiego stanu rzeczy wskazał wysokie stawki interkonektowe za zakańczanie ruchu przychodzącego z sieci stacjonarnych do mobilnych oraz dużą dysproporcję pomiędzy stawkami hurtowymi i detalicznymi tych usług. Ponadto Prezes UKE zadeklarował prawną i rynkową analizę problemu oraz zapowiedział organizację debaty

[7] Spośród wielu publikacji na temat protokołu TCP/IP szczególnie interesująca jest publikacja K. S. Siyana i T. Parkera zatytułowana *TCP/IP. Księga eksperta* (wyd. II, Gliwice 2002, Helion).

[8] Wymagania te wynikają z art. art. 180a i 180c *Ustawy z dnia 16 lipca 2004 r. – Prawo telekomunikacyjne* (Dz.U. z 2004 r., Nr 171, poz. 1800).

[9] Obowiązek zgłoszenia do rejestru przedsiębiorców telekomunikacyjnych został zawarty w art. 10 wyżej wymienionej ustawy.

[10] Szczegółowe informacje na ten temat można znaleźć w serwisie internetowym UKE: www.uke.gov.pl.

poświęconej korzystaniu z FCT-ów. Debata ta, zatytułowana: *Wykorzystanie urządzeń Fixed Cellular Terminal w połączeniach międzyoperatorskich* odbyła się 19.09.2007 r., a komunikat Prezesa UKE poświęcony jej wynikom oraz wszelkie materiały z tego spotkania zostały udostępnione w Biuletynie Informacji Publicznej UKE[11]. Niezależnie od powyższego, środowisko telekomunikacyjne zarzuca UKE, że nie robi nic, licząc na to, że ponieważ problem FCT-ów maleje, to sam zniknie wraz ze wzrostem konkurencji na rynku telekomunikacyjnym.

Dotychczasowe spory wokół stosowania FCT-ów miały głównie podłoże biznesowe, mało natomiast mówiło się o zagrożeniach dla obronności, bezpieczeństwa państwa oraz bezpieczeństwa publicznego wynikających ze stosowania tych technologii do transferowania ruchu pomiędzy sieciami. Nie oznacza to jednak, że kwestie bezpieczeństwa pozostały niezauważone. Dobrym przykładem może być dostępna w internecie obszerna opinia Artura Kołosowskiego na temat wpływu FCT-ów na realizację zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego[12]. Autor opinii wykazał jednoznacznie, że FCT-y *nie tylko utrudniają, lecz często wręcz uniemożliwiają realizację przez operatorów zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego.*

Wracając do użytego w tytule artykułu pojęcia d e z i n f o r m a c j a , trzeba zauważyć, że podmioty wprowadzające ruch do sieci komórkowych za pośrednictwem FCT-ów ukrywają numer za pomocą funkcji CLIR, co oznacza, że abonent B jest „delikatnie oszukiwany", otrzymując informację „numer zastrzeżony", nawet jeśli abonent A udostępnia prezentację numeru. Nie daje to możliwości popełniania przestępstw związanych z podszywaniem się pod inne osoby, ale z punktu widzenia służb zajmujących się obronnością i bezpieczeństwem państwa skutek stosowania FCT-ów niesie takie same zagrożenia, jak wcześniej opisany serwis pozwalający podszywać się pod dowolny numer. Przede wszystkim FCT-y powodują to, że ukrywane są faktyczne kontakty osób wchodzących w zainteresowanie wyżej wymienionych służb (tzw. figurantów) poprzez wprowadzenie złudzenia porozumiewania się z różnymi abonentami. W szczególności ukrywane są stałe kontakty figuranta, gdyż karty SIM podlegają w FCT-ach dużej rotacji, co sprawia, że kolejne połączenia inicjowane z tego samego numeru A będą rejestrowane w bilingu przychodzącym abonenta B jako różne numery. Połączenia zagraniczne terminowane za pomocą FCT-ów są zawsze rejestrowane w bilingach operatorów mobilnych jako krajowe. Ułatwia to osobom zaangażowanym w szpiegostwo oraz działalność terrorystyczną ukrywanie kontaktów zagranicznych. Należy również wspomnieć o pośrednich zagrożeniach wynikających z wiązania sił i środków służb oraz o wyżej opisanej deprecjacji bilingu jako dowodu w sprawie sądowej.

Podsumowanie

W artykule tym przedstawiono najbardziej powszechne sposoby wprowadzania do obiegu telekomunikacyjnego mylących informacji o numerach inicjujących połączenie. Opisana działalność często jest niezgodna z obowiązującym prawem i może

[11] Tamże.

[12] Zob.: http://www.piit.org.pl/_gAllery/73/71/7371/20080418_Opinia_FCT_2008.04.16.pdf.

ułatwiać popełnianie przestępstw, powodować uszczuplanie dochodów u niektórych przedsiębiorców telekomunikacyjnych, obniżać jakość usług telekomunikacyjnych, ale przede wszystkim niesie realne zagrożenia dla bezpieczeństwa państwa. Dlatego należy zwalczać wszelkie formy działalności pozwalające na podszywanie się pod innego abonenta podczas korzystania z usług telekomunikacyjnych. Jak wynika z opisanego przykładu, polski system prawny posiada narzędzia pozwalające skutecznie walczyć z serwisami oficjalnie oferującymi usługę podmiany numeru. Walka z terminowaniem ruchu za pomocą FCT-ów na pozór również wydaje się prosta, ponieważ przepisy regulujące działalność telekomunikacyjną[13] zabraniają nieuprawnionego przetwarzania danych transmisyjnych. Informacja adresowa o numerze abonenta A i B nie powinna być zmieniana na całej drodze połączeniowej. W praktyce sprawa jest o wiele bardziej skomplikowana, gdyż większość podmiotów transferujących ruch za pomocą FCT-ów nie jest zarejestrowana w prowadzonym przez UKE rejestrze przedsiębiorców telekomunikacyjnych, a więc nie mogą one być kontrolowane i ewentualnie karane przez ten organ. Ponadto, w odróżnieniu od serwisów oferujących *spoofing*, przedsiębiorcy transferujący ruch za pomocą FCT-ów nie rozgłaszają swojej działalności, a częsta zmiana anonimowych kart SIM (*prepaid*) sprawia, że ich działalność jest niemal niezauważalna. Podmioty te mogłyby być ścigane na zasadach ogólnych za przestępstwo z art. 268 § 1 kk, ale w tym przypadku ściganie następuje na wniosek pokrzywdzonego. I tu rodzi się pytanie: kto powinien wnioskować o ukaranie sprawcy? Obywatel, który na wyświetlaczu telefonu nie widział numeru rozmówcy, a jakość połączenia pozostawiała wiele do życzenia? Służba, która została wprowadzona w błąd i nie zdołała zapobiec popełnieniu przestępstwa bądź wykryciu sprawcy? Czy raczej państwo lub społeczeństwo, które doznało krzywdy na skutek, na przykład, zamachu terrorystycznego?

Agencja Bezpieczeństwa Wewnętrznego przeprowadziła cykl konsultacji z innymi służbami odpowiedzialnymi za bezpieczeństwo państwa oraz bezpieczeństwo i porządek publiczny, największymi przedsiębiorcami telekomunikacyjnymi oraz Urzędem Komunikacji Elektronicznej w celu wypracowania rozwiązań pozwalających na zminimalizowanie zagrożenia wynikającego ze stosowania FCT-ów. Obecnie prowadzone są konsultacje z Ministerstwem Infrastruktury poświęcone ocenie możliwych do wprowadzenia zmian prawnych pozwalających skuteczniej zwalczać wszelkie formy podmiany numerów stron połączenia telefonicznego.

Z punktu widzenia służb odpowiedzialnych za bezpieczeństwo państwa działalność telekomunikacyjna powinna być prowadzona tak, aby w razie potrzeby uprawnione podmioty mogły zidentyfikować strony połączenia, uwzględniając uwarunkowania prawne, w szczególności okres retencji danych stowarzyszonych ze świadczonymi usługami telekomunikacyjnymi.

[13] Zagadnienie to zostało uregulowane w art. 31 i 126 wymienianej już *Ustawy z dnia 16 lipca 2004 r. Prawo telekomunikacyjne* oraz doprecyzowane w wydanym na jej podstawie *Rozporządzeniu Ministra Infrastruktury z dnia 9 stycznia 2008 r. w sprawie szczegółowych wymagań dotyczących zasad adresowania dla właściwego kierowania połączeń* (Dz.U. z 2008 r., Nr 14, poz. 84).

Streszczenie

Artykuł podejmuje temat wiarygodności danych identyfikujących zakończenia sieci telekomunikacyjnych, z których inicjowane są połączenia. Przedstawiono w nim przypadki i najbardziej typowe sposoby nieuprawnionej modyfikacji tych danych. Szczególny nacisk położono na zagadnienia związane z nielegalnym terminowaniem ruchu za pomocą bramek GSM, tzw. FCT-ów (*Fixed Cellular Terminal*). Autor przedstawia i uzasadnia tezę, iż tego typu działalność rodzi zagrożenia dla bezpieczeństwa państwa oraz wskazuje na konieczność podjęcia działań zmierzających do wyeliminowania wszelkich przypadków modyfikacji danych adresowych związanych z przesyłanymi przekazami telekomunikacyjnymi.

Abstract

The article addresses the issue of reliability of data related to the telecommunication network endpoints, acting as the points of origin of the connection. Cases and the most typical methods of unauthorized modification of this data are presented in the article. Particular emphasis was put on the illegitimate telecommunication traffic termination with the FCT (Fixed Cellular Terminal) GSM gates. The author presents and justifies the thesis that such activity poses threat to the state security, that is why appropriate countermeasures should be taken to eliminate and prevent all illegitimate modification of address data related to telecommunication transfers.

Michał Młotek
Marcin Siedlarz

Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL

Wstęp

Rolą Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL działającego w ramach Departamentu Bezpieczeństwa Teleinformatycznego jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej RP do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę krytyczną. CERT.GOV.PL funkcjonuje zgodnie z przyjętymi w dniu 9 marca 2009 r. przez Komitet Stały Rady Ministrów Założeniami Rządowego Programu Ochrony Cyberprzestrzeni RP na lata 2009 - 2011 (RPOC).

Do zadań nałożonych na wyżej wymieniony Zespół i wykonywanych od momentu jego powstania w lutym 2008 r. należy:

a) kreowanie polityki w zakresie ochrony przed cyberzagrożeniami,
b) koordynowanie przepływu informacji pomiędzy podmiotami w tym zakresie,
c) wykrywanie cyberzagrożeń, rozpoznawanie ich i przeciwdziałanie im,
d) współpraca z krajowymi instytucjami, organizacjami oraz podmiotami resortowymi w zakresie ochrony cyberprzestrzeni,
e) reprezentacja RP w kontaktach międzynarodowych (w zakresie współpracy wojskowej, w porozumieniu z Centrum Koordynacyjnym Systemu Reagowania na Incydenty Komputerowe resortu obrony narodowej),
f) gromadzenie wiedzy dotyczącej stanu bezpieczeństwa i zagrożeń dla krytycznej infrastruktury teleinformatycznej,
g) reagowanie na incydenty bezpieczeństwa teleinformatycznego ze szczególnym uwzględnieniem krytycznej infrastruktury teleinformatycznej państwa,
h) prowadzenie analiz powłamaniowych,
i) tworzenie polityki ochrony systemów i sieci teleinformatycznych,
j) szkolenia i podnoszenie świadomości odnośnie do zagrożeń komputerowych,
k) przygotowywanie okresowych raportów w zakresie bezpieczeństwa teleinformatycznego państwa,
l) konsulting i doradztwo w zakresie cyberbezpieczeństwa.

System wczesnego ostrzegania o zagrożeniach w internecie – ARAKIS-GOV

Podstawowym sposobem ochrony rządowych systemów teleinformatycznych jest objęcie ich parasolem systemu wczesnego ostrzegania ARAKIS-GOV. Działanie tego systemu polega na agregowaniu informacji o zagrożeniach sieciowych na podstawie monitorowanego ruchu w sieci (za pomocą rozproszonych sond) oraz informacji ze źródeł zewnętrznych. Jego funkcjonalność to przede wszystkim informowanie o nowych zagrożeniach, opis tych zagrożeń w formie sygnatur, zapewniający środek ochronny, który może być wykorzystany w systemach wykrywania/prewencji włamań, analiza trendów związanych z zagrożeniami oraz korelacja informacji dotyczą-

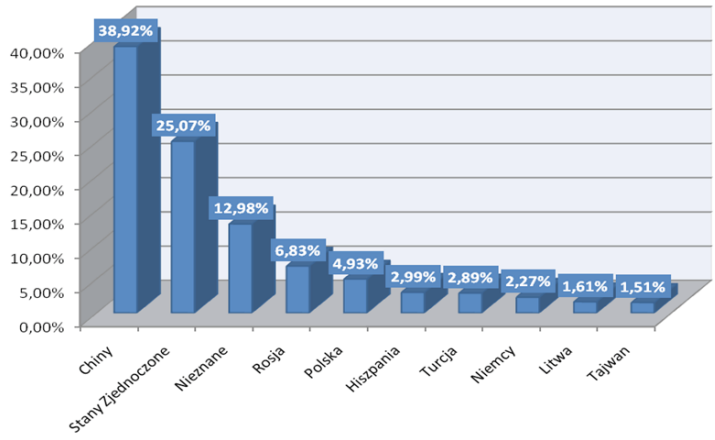
cych zdarzeń z różnych typów źródeł sieciowych oraz z różnych instytucji uczestniczących w systemie.

W przypadku ARAKIS-GOV, jego architektura rozproszonego systemu sond rozlokowanych w instytucjach administracji publicznej na styku z siecią internet, z których informacje trafiają do centrum, gdzie w systemie SEC (*Simple Event Correlator*) następuje ich agregacja i analiza, odzwierciedla spojrzenie na bezpieczeństwo z punktu widzenia zagrożenia zewnętrznego wobec wszystkich chronionych sieci. W związku z tym, mając do dyspozycji informacje o możliwych incydentach pochodzących zarówno z jednostkowych systemów zapór (*firewalli*) jak i z systemów pocztowych, sieci „Darknet”[1] i z samych sond, które znajdują się w niewykorzystywanej przez chronione podmioty adresacji IP, można w sposób semi-zautomatyzowany wykrywać anomalie powiązane z sygnaturami. W rezultacie można tworzyć gotowe sygnatury, z których skorzystać może każdy administrator sieci chronionej przez ARAKIS-GOV. W ten sposób zagrożenie jest likwidowane, zanim praktycznie wystąpi.

Aktualnie ochroną systemu ARAKIS-GOV objętych jest 16 ministerstw, 11 jednostek samorządowych oraz 42 inne jednostki, takie jak Biuro Bezpieczeństwa Narodowego, Centralne Biuro Antykorupcyjne, Zakład Ubezpieczeń Społecznych czy Senat RP.

Na podstawie informacji zebranych przez wyżej wymieniony system w roku 2010 określono lokalizację geograficzną źródłowych adresów IP, z których wykonywano ataki na polskie sieci rządowe monitorowane przez ten system.

W czołówce napastników znajdują się adresy zlokalizowane w Chinach (≈39%) i Stanach Zjednoczonych (≈25%). Należy podkreślić, iż trend ten potwierdza się również w przypadku ogólnoświatowych systemów.



Rys. 1. Rozkład procentowy ataków na sieci monitorowane w różnych państwach przez system ARAKIS-GOV.

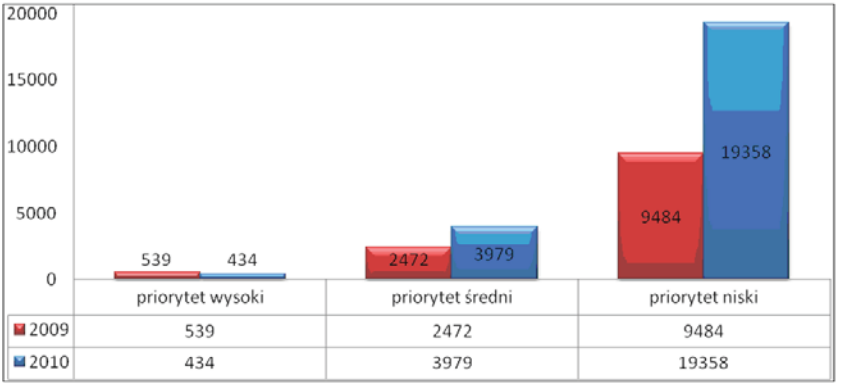
Na powyższym wykresie przedstawiającym procentowe wyliczenie ataków na monitorowane przez system ARAKIS-GOV sieci na trzecim miejscu znajduje się pozycja „nieznane”. Określenie to dotyczy adresów IP w chwili obecnej nieprzypisanych

[1] Darknet – obszar sieci posiadający rutowalne, lecz nie przypisane aktualnie żadnemu podmiotowi bloki adresów IP. Każdy pakiet z takim adresem należy traktować jako potencjalnie wrogi.

żadnemu podmiotowi. Oznacza to, iż dokonano podszycia się (podmiany adresu źródłowego IP) pod nieistniejący adres IP.

Należy zauważyć, że ze względu na specyfikę protokołu TCP/IP nie można bezpośrednio łączyć źródła pochodzenia pakietów z rzeczywistą lokalizacją zleceniodawcy ataku. Wynika to z faktu, iż w celu ukrycia swej tożsamości i fizycznej lokalizacji atakujący mogą wykorzystywać serwery pośredniczące (tzw. proxy) lub słabo zabezpieczone komputery, nad którymi wcześniej przejmują kontrolę.

W stosunku do roku 2009 system ARAKIS-GOV odnotował w roku następnym dwa razy większą całkowitą liczbę alarmów (28 109), przy czym mniejszą o priorytecie „wysokim". Zdecydowana jest przewaga alarmów o priorytecie „niskim". Tak duża liczba alarmów o priorytecie „niskim" spowodowana była obserwacją wzrostu ruchu typu BitTorrent[2] na przełomie miesiąca marca i kwietnia 2010 r. Na dalszym etapie obserwacji stwierdzono, że ruch ten zaburza obraz aktualnej sytuacji w monitorowanych sieciach, dlatego też wprowadzono filtry w systemie w celu wyeliminowania alarmów związanych z uznanym za nieszkodliwy ruchem BitTorrent.



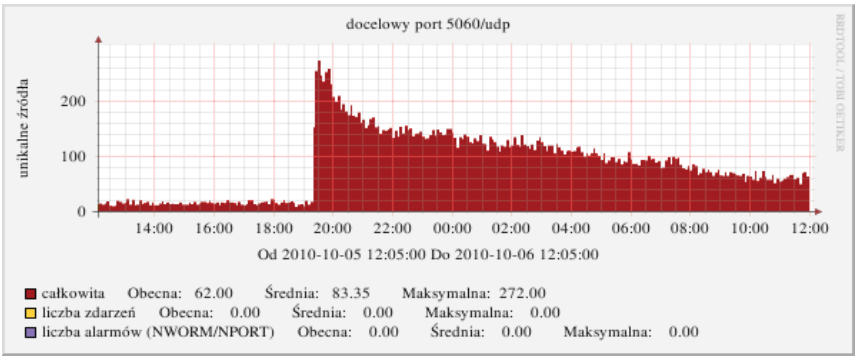
Rys. 2. Rozkład alarmów z uwzględnieniem priorytetów w latach 2009 - 2010.

W październiku 2010 r. system ARAKIS-GOV zaobserwował wzrost ruchu na porcie 5060/UDP (*Session Initiation Protocol*) – jednym z protokołów używanych w technologii telefonii internetowej VoIP. Wzrost ten widoczny był zarówno w lokalizacjach chronionych przez system, jak i w przestrzeniach adresowych Darknetu. Poniżej przedstawiono wykres obrazujący powyższą sytuację.

Ruch został zaobserwowany z ponad 400 unikalnych źródłowych adresów IP i kierowany był na ponad 1560 unikalnych adresów docelowych objętych monitoringiem przez system ARAKIS-GOV. Sytuacja ta była wynikiem skanowania w poszukiwaniu serwerów VoIP. W tym celu wykorzystano żądania OPTION protokołu SIP, które pozwalają w odpowiedzi uzyskać informacje o opcjach pracy serwera. Powyższe

[2] BitTorrent – protokół wymiany i dystrybucji plików przez internet, którego celem jest odciążenie łączy serwera udostępniającego pliki. Jego największą zaletą w porównaniu do protokołu HTTP jest podział pasma pomiędzy osoby, które w tym samym czasie pobierają dany plik. Oznacza to, że użytkownik w czasie pobierania wysyła fragmenty pliku innym użytkownikom. Ruch sieciowy dotyczący usług współdzielenia plików z zasady nie powinien być obserwowany w systemach administracji publicznej. Sytuacja zaobserwowana przez system ARAKIS-GOV może mieć zarówno charakter przypadkowego skanowania sieci przynależących do administracji publicznej, jak i świadczyć o działających w przeszłości usługach współdzielenia plików w tych sieciach.

dane zbierane były najprawdopodobniej w celu wykorzystania do ataku na serwery SIP (VoIP). Ponadto informacje tego typu dostarczają także wiedzy na temat oprogramowania, na którego podstawie działa serwer SIP.



Rys. 3. Rozkład ruchu na porcie 5060/UDP w przeciągu doby, w której wystąpiły anomalie, na podstawie danych z lokalizacji chronionych systemem.

Warto zauważyć, iż pod koniec lipca 2010 r. Zespół CERT.GOV.PL został poinformowany o incydencie, który wystąpił w jednym z Urzędów Miasta. Chodziło o kradzież impulsów telekomunikacyjnych. Na podstawie danych uzyskanych od administratora sieci lokalnej UM stwierdzono, iż chodzi o kradzież, której dokonano poprzez włamanie się na konto uprzywilejowane, które było zabezpieczone słabym hasłem. Konsekwencją powyższego było wykonanie połączeń na koszt UM o łącznym czasie 740 280 sekund (206 godzin = 8,5 dnia). Oszacowane przez Urząd Miasta straty z tytułu nieautoryzowanych połączeń telefonicznych wyniosły około 60 000 PLN.

Program badania bezpieczeństwa witryn internetowych administracji publicznej

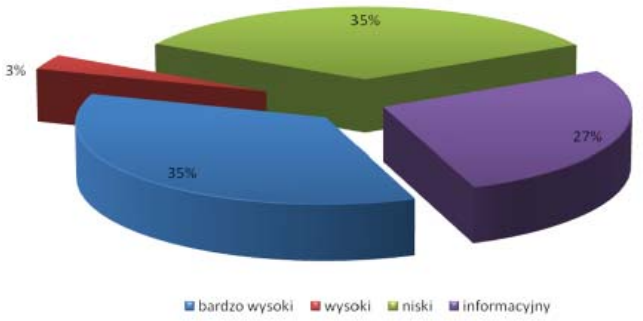
Powiększając zakres usług świadczonych przez Rządowy Zespół Reagowania na Incydenty Komputerowe CERT.GOV.PL, od dnia 1 lipca 2008 r. rozpoczęto nowy program sukcesywnego badania stanu zabezpieczeń witryn internetowych należących do instytucji administracji publicznej. Działania te mają na celu określenie poziomu bezpieczeństwa aplikacji „www" instytucji publicznych, a także usunięcie wykrytych nieprawidłowości, zanim zostaną wykorzystane przez cyberprzestępców.

W 2010 r. przebadano 93 witryny należące do 63 instytucji państwowych. Stwierdzono ogółem 1277 błędów w tym: 451 błędów o bardzo wysokim poziomie zagrożenia, 40 błędów o wysokim poziomie zagrożenia, 440 błędy o niskim poziomie zagrożenia i 346 błędów oznaczonych jako „informacyjne".

Do ważniejszych ministerstw, których witryny zostały przebadane przez Zespół CERT.GOV.PL należą:

1. Ministerstwo Spraw Wewnętrznych i Administracji,
2. Kancelaria Prezydenta RP,
3. Centrum Obsługi Kancelarii Prezesa RM,
4. Ministerstwo Spraw Zagranicznych,
5. Ministerstwo Infrastruktury,
6. Ministerstwo Finansów,
7. Ministerstwo Edukacji Narodowej,
8. Ministerstwo Pracy i Polityki Społecznej.

Ponadto testom poddane zostały strony „www" innych ważnych instytucji, takich jak:
1. Centralne Biuro Antykorupcyjne,
2. Ministerstwo Obrony Narodowej,
3. Komenda Główna Policji,
4. Kancelaria Polskiej Akademii Nauk,
5. Prokuratura Okręgowa w Bydgoszczy,
6. Państwowa Komisja Wyborcza,
7. Ministerstwo Finansów (Izby Celne i Urzędy Skarbowe).



Rys. 4. Statystyka wykrytych podatności na zawirusowanie w witrynach „www" należących do administracji publicznej (według poziomu zagrożenia).

W trakcie skanowania witryn stwierdzono, że 75% spośród nich zawierało przynajmniej jedną podatność, którą należało uznać za krytyczną dla bezpieczeństwa serwera i publikowanych na witrynie treści. Tylko w nielicznych przypadkach zabezpieczenia witryn były skuteczne i nie stwierdzono w nich żadnych podatności. Tak duże różnice w jakości zabezpieczeń systemów świadczą o bardzo zróżnicowanej wiedzy związanej z bezpieczeństwem wśród osób odpowiedzialnych za administrację i wykonanie systemów. Poniższa tabela przedstawia ranking przebadanych witryn pod względem ilości błędów krytycznych.

Tab. 1. Ocena stanu bezpieczeństwa witryn internetowych wyszczególnionych instytucji.

Stan bezpieczeństwa przebadanych witryn	Instytucja
Bardzo dobry poziom bezpieczeństwa	Centrum Obsługi Kancelarii Prezesa RM
	Prokuratura Okręgowa w Bydgoszczy
	Urząd Kontroli Skarbowej w Białymstoku
	Urząd Kontroli Skarbowej w Katowicach
	Urząd Kontroli Skarbowej w Olsztynie
	Urząd Kontroli Skarbowej w Poznaniu
Średni poziom bezpieczeństwa	Krajowa Rada Radiofonii i Telewizji
	Izba Skarbowa w Gdańsku
	Ministerstwo Sprawiedliwości
	Państwowy Instytut Geologiczny
	Urząd Komunikacji Elektronicznej
Niski poziom bezpieczeństwa	Izba Skarbowa w Krakowie
	Rządowe Centrum Legislacji
	Polska Agencja Rozwoju Przedsiębiorczości
	Centralny Ośrodek Geodezji i Kartografii
	Izba Skarbowa w Katowicach

Rozwijając wizję systemu ARAKIS-GOV na podstawie doświadczeń zdobytych podczas testów witryn internetowych, na początku IV kwartału 2009 r. uruchomiono testową wersję systemu Honey Spider Network – GOV (HSN-GOV), która wykorzystywana jest w celu monitorowania rządowych stron „www" pod względem serwowania złośliwego oprogramowania. Wyżej wymieniony system przeznaczony jest na potrzeby administracji rządowej. HSN-GOV okresowo dokonuje weryfikacji zawartości strony w poszukiwaniu złośliwego kodu JavaScript, który może infekować komputery użytkowników odwiedzających stronę „www". Obecnie monitoringiem objęto ponad 2000 stron internetowych należących do administracji rządowej (gov.pl).

Na podstawie wyników zawartych w HSN-GOV okresowo generowana jest lista stron „www", zawierająca te adresy, które zostały przez system uznane za szkodliwe. Powyższa lista (*blacklist*) wykorzystana zostanie docelowo w projekcie DNS-Blackholing, który będzie realizowany w przyszłości w jednostkach administracji rządowej.

W systemie HSN-GOV zostały zaimplementowane dodatkowe funkcjonalności mające na celu wspomaganie analiz wykonywanych przez system. Jedną z najbardziej istotnych jest metoda wykrywania mechanizmu fast-flux[3]. Ponadto HoneySpider Network korzysta ze źródeł zewnętrznych wspomagających analizy oprogramowania złośliwego, takich jak VirusTotal, Anubis czy Norman Sandbox.

Ataki ukierunkowane

Jednostki administracji publicznej, w odróżnieniu od indywidualnych użytkowników cyberprzestrzeni, są szczególnie narażone na jeden z typów wrogich działań, tj. na ataki ukierunkowane. Ten typ ataków polega najczęściej na próbie nakłonienia użytkownika do otwarcia złośliwego załącznika w poczcie e-mail.

W roku 2010 coraz częściej rejestrowano ataki ukierunkowane wykorzystujące metody socjotechniczne, takie jak spersonalizowana przesyłka wysłana z adresu, do którego odbiorca ma zaufanie (przy czym tu następuje podszycie się pod nadawcę), czy zawartość zawierająca interesujące treści z punktu widzenia odbiorcy. Trend ten znacznie się nasilił po tragedii smoleńskiej. W niecałe dwa dni po katastrofie z konta Bill Murray bbc.news@wp.pl rozsyłana była poczta e-mail zatytułowana *Looking beyond Poland's, unprecedented disaster*. Treść wiadomości dotyczyła bezpośrednio wydarzeń z 10 kwietnia 2010 r. Jednocześnie zostały do niej dołączone dwa pliki – „Page1.pdf" oraz „Draft.doc", których otwarcie mogło doprowadzić do zainfekowania sytemu.

Kilka dni później, tj. 16 kwietnia 2010 r., odnotowano kolejny przypadek wykorzystania tragedii narodowej do rozsyłania poczty internetowej zawierającej złośliwe oprogramowanie. Wiadomość *Dear colleagues! Kazakhstan head of state sends official condolences to Seym of Poland. Official text is attached. Condolences are also posted on official site* http://www.kazakhstan.org.sg/content/intro.php?act=news&c_id=726 rozsyłana z konta kazakstan.embass@mail.ru o tytule *Kazakhstan head of state sends official condolences* również zawierała złośliwy załącznik o nazwie *Official_condolences.pdf*, którego otwarcie mogło prowadzić do utraty istotnych informacji lub nawet do przejęcia komputera użytkownika.

[3] Fast-flux – jedna z technologii stosowana przy popełnianiu przestępstw internetowych, np. phishingu. Jest to mechanizm przełączający serwera DNS (jedna domena odnosi się do kilku adresów IP), w celu ukrycia stron, na które przesyłane są wyłudzone dane.

W maju 2010 r. dokonano ataku na Ministerstwo Spraw Zagranicznych. Polegał on na masowym przesyłaniu wiadomości mailowych do pracowników MSZ. Wiadomości tego typu były wysłane na 192 adresy pracowników zarówno centrali, jak i placówek zagranicznych. Była to próba podszycia się pod pracownika pomocy technicznej i zawierała prośbę o podanie nazwy użytkownika, adresu e-mail, hasła oraz numeru telefonu. Wiadomość wysyłano z maszyny przypisanej do Danii. Na podstawie informacji otrzymanych z duńskiego zespołu CERT wspomniany host został przejęty przez cyberprzestępców.

W grudniu 2010 r. natomiast odnotowano masowe rozsyłanie wiadomości mejlowych mających swoje źródło w Federacji Rosyjskiej, a adresowanych do kilku instytucji administracji publicznej w Polsce, m.in. do MSZ i ABW. Wiadomości te zawierały zainfekowane załączniki w postaci plików pdf bądź pakietu MS Office. Ich tytuły dotyczyły sytuacji m.in. wojsk NATO: *Rogozin Condemns secret NATO Pact* lub portalu Wiki Leaks i szczegółów aresztowania jego założyciela – Juliana Assange'a.

Oprócz metod socjotechnicznych, bardzo ważnym aspektem wspomnianych ataków są techniki „czysto" informatyczne. W przypadku zaobserwowanych ataków używano złośliwego oprogramowania, które wykorzystywało podatności typu „0-day" na popularne aplikacje. Oznaczało to, iż w dniu wykonania ataku nie była dostępna stosowna aktualizacja oprogramowania, która mogłaby zapobiec przełamaniu zabezpieczeń. Dodatkowo plik był wykrywany jedynie przez nieliczne silniki antywirusowe.

Wykorzystanie metod socjotechnicznych oraz phisingowych do ataku na użytkowników systemów handlu uprawnieniami do emisji CO_2

W styczniu 2010 r. właściciele kont krajowych systemów handlu uprawnieniami do emisji gazów cieplarnianych otrzymali e-maile, w których zostali poinformowani, iż w związku z powtarzającymi się atakami na systemy handlu Komisja Europejska zadecydowała o podniesieniu poziomu zabezpieczeń. Treść e-maila informowała, iż Komisja ta wskazała firmę do realizacji tego zadania, przekazując jej konieczne informacje o użytkownikach. W związku z tym należało wpisać adres wskazanej strony internetowej i potwierdzić na niej poprawność informacji. Następnie użytkownikom miał być przekazany klucz USB, dzięki któremu można by było bezpiecznie logować się do systemu.

Takie e-maile zostały przesłane do użytkowników z wielu krajów, w tym z Polski. Na uwagę zasługuje kilka szczegółów: tekst wiadomości napisany był w odpowiednim języku, w zależności od narodowości odbiorcy, na wskazaną stronę można było się dostać zarówno klikając link umieszczony w treści, jak i wpisując ręcznie adres samej domeny. Przestępcy stworzyli całą stronę internetową fałszywej firmy i umieścili na niej odpowiednie wersje językowe wraz z całym portfolio (fałszywym). Proces „potwierdzania" informacji składał się z kilku podstron, na których znajdowały się różne pytania. Na jednej z nich było pytanie o login do systemu, na innej o hasło. Jako że nie były one umieszczone obok siebie, lecz obok innych zapytań, np. o nazwę firmy, ulicę, numer budynku, kod pocztowy, miasto, numer kierunkowy itp., mogły nie wzbudzić podejrzeń. Dodatkowo, każda przesyłka e-mail była kierowana osobiście do każdej z atakowanych osób. Zawierała jej imię, nazwisko, numer telefonu służbowego oraz nazwę reprezentowanej firmy. W dużym stopniu podwyższało to zaufanie odbiorcy do prawdziwości treści. Wielu użytkowników w różnych krajach (w tym i w Polsce) podało dane, o które atakującym chodziło. Dane te natychmiast zostały wykorzystane do wykradzenia użytkownikom posiadanych przez nich uprawnień do emisji. Szkody powstałe np. w Niemczech szacowa-

ne są na trzy miliony euro. Dzięki szybkiej reakcji polskiego Krajowego Administratora Systemu Handlu Uprawnieniami, Polska nie poniosła strat.

Należy zauważyć, iż przestępcy wykorzystali metody zarówno socjotechniczne (e-mail w odpowiednim języku zawierający dane odbiorcy oraz odpowiednią formę fałszywej strony internetowej), jak i phishingowe (skupienie się na wyłudzeniu haseł i natychmiastowe ich wykorzystanie, podszycie się pod legalną stronę, duża skala ataku). Sądząc po stratach tylko jednego kraju należy sądzić, iż osiągnęli sukces. Spowodowane to było tym, że dane użytkowników rejestrów są publicznie dostępne (wymóg prawny Komisji Europejskiej), że posiadacze kont nie byli świadomi zagrożeń, a także niskim stopniem zabezpieczenia samych rejestrów (dostęp i użytkowanie chronione wyłącznie za pomocą hasła).

Streszczenie

W artykule przedstawiono proces tworzenia Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, jego zadania i misję. Poza tym szczegółowo omówiono jedno z najważniejszych narzędzi stosowanych w pracy Zespołu, tj. system wczesnego ostrzegania o zagrożeniach w sieci internet – ARAKIS-GOV. Funkcjonalność tego systemu to przede wszystkim informowanie o nowych zagrożeniach w sieci, opis tych zagrożeń (w formie sygnatur) zapewniający środek ochronny, który może być wykorzystywany w systemach wykrywania i prewencji włamań, analiza trendów związanych z zagrożeniami oraz korelacja wiadomości dotyczących zdarzeń pochodzących z różnych typów źródeł sieciowych i z różnych instytucji uczestniczących w systemie.

Zaprezentowano również program odnoszący się do bezpieczeństwa witryn należących do instytucji administracji publicznej wraz z wynikami testów. Ostatnia część niniejszej publikacji została poświęcona omówieniu najistotniejszych incydentów wykrytych przez CERT.GOV.PL w 2010 r., tj. atakom ukierunkowanym oraz próbie wyłudzenia z systemu handlu uprawnieniami jednostek emisji dwutlenku węgla.

Abstract

he following article presents the creation of Polish Governmental Computer Security Incident Response Team – CERT.GOV.PL, its key activities and main tasks and duties. The aim of this article was also to describe one of the most important tools utilized by CERT, which is: ARAKIS-GOV – the early warning system on Internet threats, as well as the effects of its operation. The primary function of the system is informing of new threats within the networks and providing the description (in a form of signatures) of the identified threats. The definitions can be implemented into intrusion identification and prevention systems. Additionally, the system allows to analyze the trends in the nature of changing threats and coordination of data flow relating to security threats originating in different networks administrated by different institutional members of the system.

The article also presents the websites security software working at the websites of state administration and the test results.

Finally, the article describes the major incidents identified by CERT.GOV.PL in 2010, that is attacks aimed at obtaining clearances for access to the system of trade in CO_2 emission units.

Aleksandra Tucholska-Lenart

Wykorzystanie metod biologii molekularnej w identyfikacji ofiar katastrof masowych i ataków terrorystycznych

W sobotę rano – 10 kwietnia 2010 r. dotarła do Polski szokująca wiadomość. O godz. 8.41.06 podczas próby podejścia do lądowania rozbił się polski samolot rządowy TU-154M wiozący na pokładzie delegację na uroczystości związane z 70. rocznicą wymordowania przez NKWD polskich oficerów w Katyniu.

Dramat rozegrał się w pobliżu lotniska wojskowego Siewiernyj pod Smoleńskiem.

W katastrofie zginęli: prezydent RP Lech Kaczyński z małżonką Marią, ostatni prezydent na uchodźstwie Ryszard Kaczorowski, posłowie, senatorowie, ministrowie, generalicja, członkowie rodzin katyńskich, duszpasterze różnych wyznań, oficerowie BOR i członkowie załogi tragicznego w skutkach lotu nr 101 (razem 96 osób).

Przez dwa tygodnie śledziliśmy trudny i bolesny dla rodzin ofiar proces identyfikacji szczątków ich bliskich. Dzisiaj wiemy, że dla 21 spośród dotkniętych tragedią rodzin jedyną nadzieją na identyfikację były badania genetyczne. Wiemy również, że badaniom tym poddane były wszystkie zwłoki i szczątki[1]. Zastosowane przez specjalistów metody biologii molekularnej nie zawiodły, zatem przyjrzyjmy się zasadom identyfikacji z wykorzystaniem tych procedur.

Nowoczesna identyfikacja osobnicza nie ogranicza się wyłącznie do identyfikacji sprawców przestępstw, ale służy również takim celom, jak identyfikacja ofiar zamachów terrorystycznych, wszelkiego rodzaju katastrof i klęsk żywiołowych, a także osób, których zwłoki lub szczątki zostały ekshumowane z grobów masowych.

Metody identyfikacji zwłok i szczątków ludzkich w zależności od stopnia ich wiarygodności zostały uszeregowane już podczas V Konferencji Komisji Interpolu ds. Identyfikacji Ofiar Katastrof Masowych i Klęsk Żywiołowych, która odbyła się w Lyonie w 1993 r. i obowiązują do tej pory.

Zgodnie z tymi wytycznymi za najbardziej wiarygodną uznano metodę identyfikacji genetycznej.

Do pozostałych, dopuszczalnych metod (zgodnie z ich efektywnością i stopniem wiarygodności) należą:

- porównanie odcisków palców, co stanowi jeden z bezpieczniejszych środków identyfikacyjnych (jeśli istnieje możliwość ich pobrania, a ofiara była daktyloskopowana przyżyciowo lub mamy dostęp do jej rzeczy osobistych, na których znajdują się porównawcze ślady linii papilarnych),
- badania porównawcze uzębienia (ważna i efektywna metoda identyfikacji, jeśli istnieje kompletna karta leczenia stomatologicznego),
- badania radiologiczne w celu ujawnienia przebytych złamań (jeśli istnieje możliwość porównania z oryginalną dokumentacją przedśmiertną), ale również jako niezwykle efektywna metoda lokalizacji i identyfikacji w ciałach ofiar takiego materiału dowodowego, jak pociski lub fragmenty ładunków wybuchowych,

[1] Janina Paradowska, *Byłem przy zamykaniu trumien w Moskwie. Przy każdej.* Wywiad z ks. Henrykiem Błaszczykiem, http://www.polityka.pl.

- porównanie danych medycznych na podstawie przebytych zabiegów chirurgicznych, np. ujawnienie braku organów typu wyrostek robaczkowy, macica, nerka lub obecność rozrusznika serca czy implantów (jeśli istnieje odniesienie w przedśmiertnej dokumentacji medycznej),
- porównanie znaków szczególnych w postaci blizn, znamion i tatuaży (zazwyczaj są unikalne, ale trzeba mieć możliwość porównania ich z opisem przedśmiertnym podanym przez bliskich ofiary),
- porównanie danych dotyczących rysopisu (płeć, szacunkowy wiek, wzrost, budowa, kolor skóry, włosów i oczu),
- identyfikacja rzeczy osobistych, takich jak odzież i biżuteria (charakterystyczna biżuteria odegrała pomocniczą rolę w identyfikacji szczątków śp. Marii Kaczyńskiej),
- identyfikacja na podstawie dokumentów ujawnionych przy zwłokach lub szczątkach (należy zawsze mieć na uwadze fakt, że mogły one ulec przemieszczeniu w trakcie zdarzenia i niekoniecznie muszą należeć do ofiary, przy której zwłokach zostały ujawnione),
- rozpoznanie przez członków rodziny lub znajomych (metoda ta, zwana okazaniem, jest uznana przez Interpol za podejście nienaukowe, o dużym stopniu ryzyka)[2].

Rodzaj i zakres badań identyfikacyjnych jest zdeterminowany przez dostepność materiału porównawczego w odniesieniu do ofiary, której szczątki zostały ujawnione na miejscu zdarzenia. Tak więc, w celu osiągnięcia pewnej identyfikacji zaleca się stosowanie kombinacji powyższych kryteriów z wyraźnym naciskiem na pobranie od wszystkich ofiar próbek biologicznych do identyfikacji genetycznej. W takiej sytuacji zawsze niezbędne będzie pobranie materiału porównawczego od krewnych, co miało miejsce także w przypadku identyfikacji ofiar katastrofy smoleńskiej. Dodać należy, że materiał ten pobierany był przez ekspertów Biura Badań Kryminalistycznych ABW.

Genetyka może pomóc także wtedy, gdy domniemana osoba nie ma żadnych krewnych (jeśli tylko jest dostęp do rzeczy osobistych ofiary). Na przedmiotach codziennego użytku, typu szczoteczka do zębów, mogą znajdować się komórki nabłonkowe, z których uzyskuje się DNA porównywane następnie z DNA ofiary. Równie cennym materiałem będą włosy zabezpieczone z grzebienia lub szczotki.

Za najbardziej efektywne narzędzie identyfikacji zwłok i szczątków ludzkich uznaje się współcześnie metody biologii molekularnej wykorzystujące DNA zawarte w jądrze komórkowym (dziedziczone po połowie od każdego z rodziców), DNA obecne w cytoplazmie komórki – tzw. DNA mitochondrialne (dziedziczone wyłącznie w linii żeńskiej) oraz analizę polimorfizmu markerów genetycznych chromosomu Y – specyficznego dla płci męskiej[3].

Badania genomowego DNA zawartego w jądrze komórkowym zabezpieczonego materiału biologicznego (krew, kości, fragmenty tkanek i narządów, włosy) polegają na określeniu tzw. profilu DNA osoby, od której pochodzi badany materiał i jego porównaniu z profilami DNA potencjalnych krewnych (rodzice, rodzeństwo, dzieci). Przeprowadzenie analiz w obrębie 16 odcinków badanego materiału pozwala uzyskać unikalny profil genetyczny. Taki test w połączeniu z określeniem płci jest wykonywany rutynowo we wszystkich przypadkach identyfikacji zwłok i szczątków ludzkich. Interpretując

[2] Identyfikacja ofiar katastrof masowych – przewodnik INTERPOLU.

[3] A. Białecka, M. Kamińska, R. Wierzchosławski, J. Wujec, *Współczesna ekspertyza kryminalistyczna z zakresu badań DNA*, w: *Kryminalistyka dla prawa – prawo dla kryminalistyki*, V. Kwiatkowska-Wójcikiewicz (red.), Toruń 2010, TNOiK, s. 63 - 79.

wyniki tych badań, zawsze należy także brać pod uwagę możliwość wystąpienia ryzyka ujawnienia zaprzeczenia ojcostwa.

Badania DNA mitochondrialnego (mtDNA) polegają na analizie sekwencji DNA występującego w cytoplazmie komórki i dziedziczonego wyłącznie w linii matczynej (wszystkie dzieci jednej kobiety mają identyczną jego sekwencję). Ten rodzaj DNA jest badany najczęściej w przypadku, gdy DNA jądrowe zostało zdegradowane wpływem ekstremalnych warunków środowiskowych, np. w wyniku procesów gnilnych zachodzących w zwłokach i szczątkach ludzkich. Uzyskany wynik badania odnosi się do wyniku badań materiału porównawczego (pochodzącego nawet od dalekich krewnych w linii matczynej) osoby, której szczątki podlegają identyfikacji.

Od kilku lat w celach identyfikacyjnych badany jest również polimorfizm obecny na chromosomie Y. W tym przypadku badane DNA dziedziczone jest wyłącznie w linii męskiej, a więc identyczne cechy będą posiadać osobnicy spokrewnieni w linii męskiej, czyli ojciec, synowie, stryj i dziadek. Materiał porównawczy do tego typu badań może zatem pochodzić od każdej osoby spokrewnionej z osobą podlegającą identyfikacji w linii męskiej. Przeprowadzając to badanie, należy również pamiętać o ryzyku ujawnienia zaprzeczenia ojcostwa.

W badaniach identyfikacyjnych zwłok i szczątków ludzkich może zachodzić konieczność przeprowadzenia kompletu wyżej wymienionych analiz. W Polsce dokonano w ten sposób identyfikacji ekshumowanych szczątków uprowadzonego i zamordowanego biznesmena Krzysztofa Olewnika[4].

Metoda genetycznej identyfikacji ofiar z zastosowaniem analizy DNA została wykorzystana w 1992 r. w badaniach szczątków kostnych ostatniego cara Rosji Mikołaja II, jego żony Aleksandry oraz ich dzieci, zamordowanych 16 lipca 1918 r. przez bolszewików. Analiza genomowego DNA zawartego w komórkach 1000 fragmentów ekshumowanych kości przeprowadzona przez naukowców z brytyjskiego Forensic Science Service potwierdziła przypuszczenie, iż w płytkim przydrożnym grobie w okolicach Jekaterynburga znajdują się m.in. szczątki członków kilkuosobowej rodziny. Badaniem DNA mitochondrialnego potwierdzono pokrewieństwo szczątków płci żeńskiej (żona cara – Aleksandra oraz ich trzy córki) ze współcześnie żyjącym krewnym w linii matczynej – księciem Edynburga Filipem. Dla ustalenia przynależności szczątków do dynastii Romanowów porównano mitochondrialne DNA domniemanego cara Mikołaja z DNA żyjących krewnych w linii matczynej – księżniczki greckiej Xenii Sfirii oraz księcia Fife'a. Uzyskany niejednoznaczny wynik badań zweryfikowano dopiero kilka lat później po badaniach ekshumowanych szczątków młodszego brata cara – księcia Gieorgija – w amerykańskim laboratorium wojskowym AFDIL (*Armed Forces DNA Identification Laboratory*)[5]. Szczątki pozostałych dwojga członków rodziny carskiej – księcia Aleksieja oraz księżniczki Marii – odnaleziono dopiero 16 lat później w odległości ok. 60 m od grobu ujawnionego w 1991 r. Tym razem badania identyfikacyjne przeprowadzili znany amerykański antropolog sądowy Anthony Falsetti oraz wybitny ekspert badań DNA z AFDIL – dr Michael Coble, potwierdzając hipotezę pochodzenia szczątków. Wyniki ogłoszono w grudniu 2008 r., zamykając tym samym jedną z najbardziej mrocznych kart historii XX wieku.

[4] http.//krzysztofolewnik.pl.

[5] P.L. Ivanow, M.J. Waldhams, R.K. Roby, M.M. Holland, V.W. Weedn, T.J. Parsons, *Mitochondrial DNA sequense heteroplasmy in the Grand Duke of Russia Georgij Romanov establishes the authenticity of the remains of the Tsar Nicholas II*, „National Genetics" 1996, vol. 12, s. 417 - 420.

Obecnie największą i najtrudniejszą operacją dotyczącą identyfikacji osób z zastosowaniem zaawansowanych metod i technologii biologii molekularnej było ustalenie tożsamości oraz liczby ofiar ataku terrorystycznego na World Trade Center z 11 września 2001 r. Zamach ten pociągnął za sobą więcej istnień ludzkich i strat niż jakikolwiek inny w USA i na świecie. Ustalenie tożsamości ofiar wymagało przeprowadzenia badań DNA zabezpieczonych szczątków ofiar oraz ich domniemanych krewnych na skalę dotąd niespotykaną. Według jednych źródeł zginęło wówczas 2749 osób, a według innych – 2752 osoby. Do stycznia 2009 r. zidentyfikowano 1614 osób. Na podstawie danych z 01.11.2009 r., w miejscu będącym pod opieką lekarza medycyny sądowej zwanym Memorial Park znajdowało się jeszcze 10 000 szczątków ludzkich, co do których nie zakończono badań identyfikacyjnych, i w związku z tym nie przeniesionio ich do miejsca pamięci w Strefie Zero. Mimo doskonałej techniki i sztabu wybitnych specjalistów sytuacja ta do dziś niewiele się zmieniła. Obecnie mówi się wprost, że nie można podać nawet przybliżonego terminu zakończenia badań. Co więcej, pojawiły się informacje, że niektóre ofiary nigdy nie zostaną zidentyfikowane, gdyż ich ciała uległy totalnemu unicestwieniu[6]. Ta sytuacja uświadamia nam, że często obserwowane, wynikające z niewiedzy, oczekiwania społeczne i naciski medialne dotyczące szybkiej identyfikacji zwłok i szczątków ludzkich z zastosowaniem analizy DNA mogą powodować niepotrzebne napięcia i wyzwalać niepokój rodzin oraz negatywne emocje. Wynika to z przekonania, że czas niezbędny do wykonania takich badań jest niezwykle krótki z uwagi na automatyzację wielu etapów pracy. Tymczasem trzeba zdawać sobie sprawę, że materiał biologiczny, na którym przychodzi pracować specjalistom z zakresu biologii molekularnej i medycyny sądowej, należy w takich sytuacjach do bardzo trudnych pod względem badawczym. Stosowane techniki i metody muszą więc być wspierane eksperckim doświadczeniem zawodowym, zarówno w zakresie kwalifikacji materiału do badań, jak i na poziomie wstępnych analiz związanych z izolacją DNA z materiału biologicznego podlegającego błyskawicznym procesom gnilnym w szczególnych warunkach środowiskowych, np. po katastrofie (oddziaływanie temperatury, wody oraz wszelkiego rodzaju zanieczyszczeń organicznych i nieorganicznych). Sytuację dodatkowo komplikuje fakt, że na co dzień laboratoria wykonują rutynowe badania na materiale dowodowym pochodzącym ze śladów biologicznych, takich jak włosy, plamy krwi, śliny, spermy, wyskrobiny spod paznokci i fragmenty naskórka. Tymczasem zgodnie z zaleceniami INTERPOLU do identyfikacji ofiar katastrof zaleca się pobieranie m.in. takiego materiału, jak kości, zęby, mięśnie, tkanka mózgowa czy krew z serca (o rodzaju pobieranej tkanki zawsze decyduje specjalista medycyny sądowej). Tego rodzaju tkanki, za wyjątkiem krwi z serca, są znacznie trudniejsze w obróbce, a sam proces izolacji DNA jest bardziej praco- i czasochłonny niż w przypadku wspomnianych badań rutynowych. Trzeba też brać pod uwagę fakt, że w przypadku np. katastrofy samolotowej większość ciał będzie rozkawałkowana, co zwielokrotni liczbę koniecznych analiz w celu przyporządkowania poszczególnych fragmentów do konkretnej osoby. Biorąc pod uwagę powyższe oraz np. potencjalną konieczność (z jakichkolwiek przyczyn) powtarzania analiz, INTERPOL zaleca, aby zwłoki nie były wydawane rodzinom, dopóki nie zostanie zakończona procedura identyfikacji wszystkich ofiar.

[6] Patrz: 9 - 11 Research.com.wtc.7net.

Zakrojone na międzynarodową skalę projekty identyfikacyjne zwłok i szczątków ludzkich zmusiły współpracujące w tej dziedzinie laboratoria kryminalistyczne i medyczno-sądowe do harmonizacji procedur i ustalenia standardów badań w celu zagwarantowania możliwości międzynarodowej wymiany wyników analiz. Procedury te zostały opracowane w formie międzynarodowej normy EN ISO/IEC 17 025, precyzującej ogólne wymagania dotyczące kompetencji laboratoriów badawczych[7]. W ubiegłym roku Rada Unii Europejskiej wydała decyzję ramową *w sprawie akredytacji dostawców usług kryminalistycznych wykonujących czynności laboratoryjne*, z której wynika, że laboratoria unijne wykonujące badania DNA dla potrzeb organów procesowych zobowiązane są uzyskać akredytację krajowych jednostek akredytujących na zgodność z wyżej wymienioną normą do dnia 30 listopada 2013 r. Wymóg ten będzie stanowił gwarancję przestrzegania norm i procedur w laboratoriach kryminalistycznych dokonujących identyfikacji osób.

Odpowiednie regulacje prawne dotyczą też procedur pobierania materiału biologicznego do badań genetycznych ze zwłok o nieustalonej tożsamości. W Polsce zagadnienia te reguluje *Zarządzenie Nr 6 Komendanta Głównego Policji z dnia 16.05.2002 r.*, które nakłada na prowadzącego czynności służbowe związane z identyfikacją NN zwłok obowiązek pobrania dwóch próbek biologicznych od tego typu zwłok w celu przeprowadzenia badań DNA. Zgodnie z obowiązującymi procedurami uprawnionym do pobrania próbek jest biegły – lekarz medycyny sądowej, gdyż tylko jego wiadomości specjalne pozwalają ocenić rodzaj materiału przydatnego do przeprowadzenia identyfikacji genetycznej NN zwłok, które często znajdują się w zaawansowanym rozkładzie gnilnym. Po przeprowadzeniu badań genetycznych profile DNA zwłok o nieustalonej tożsamości przechowuje się w policyjnej bazie danych GENOM, w celu ewentualnego ich porównania z profilami rodzin poszukujących zaginionych krewnych[8].

Wszechstronnym doświadczeniem w identyfikacji osób zaginionych, zdobytym między innymi dzięki udziałowi w projekcie identyfikacji szczątków ludzkich z grobów masowych na terenie byłej Jugosławii, dysponuje Zakład Genetyki Molekularnej i Sądowej Collegium Medicum UMK, który przeprowadził również identyfikację ofiar tragicznej w skutkach katastrofy w kopalni „Halemba"[9]. Genetyczne badania identyfikacyjne dla potrzeb organów procesowych z zastosowaniem najnowocześniejszych metod badawczych biologii molekularnej prowadzi również (od 1992 r.) Biuro Badań Kryminalistycznych ABW – wcześniej znane jako Zakład Kryminalistyki i Chemii Specjalnej UOP/ABW – dysponujące wyjątkowo doświadczoną kadrą oraz najnowocześniejszymi technologiami badań DNA[10]. Warto przypomnieć, że zespół ekspertów tego laboratorium w latach 1992 - 1993 wdrożył do polskiej kryminalistyki fenomenalną technikę amplifikacji (***P**olymerase **C**hain **R**eaction* – polimerową reakcję łańcuchową), dzięki której do badań identyfikacyjnych śladu biologicznego wystarczy ilość DNA na poziomie 2 ng,

[7] Decyzja Ramowa Rady UE 2009/905 z dnia 30.11.2009 r. w sprawie akredytacji dostawców usług kryminalistycznych wykonujących czynności laboratoryjne (Dz.U. UE. I.2009.322.14).

[8] E. Gruza, M. Goc, J. Moszczyński, *Kryminalistyka – czyli rzecz o metodach śledczych*, Warszawa 2008, Wydawnictwa Akademickie i Profesjonalne, s. 534 - 537.

[9] www.zgms.cm.umk.pl.

[10] A. Białecka, M. Kamińska, R. Wierzchosławski, J. Wujec, *Współczesna ekspertyza kryminalistyczna* …, s. 63 - 79.

czyli np. jedna cebulka włosa[11]. Zespół ten jako pierwszy w Polsce zaczął stosować tzw. multiplex PCR, co dawało możliwość identyfikacji śladów biologicznych w obrębie aż pięciu markerów genetycznych jednocześnie, podnosząc moc dyskryminacyjną wyników badań śladów biologicznych z poziomu PD = 0,71 do poziomu PD = 0,9996. Stanowiło to prawdziwy przełom w opiniowaniu na rzecz organów procesowych[12].

Omawiając sprawy genetycznej identyfikacji osób zaginionych w wyniku ataków terrorystycznych i katastrof masowych, nie sposób pominąć ustaleń, których dokonano na szczycie państw G7 w Lyonie (1996 r.), kiedy to z inicjatywy Prezydenta USA B. Clintona powstała Międzynarodowa Komisja ds. Osób Zaginionych (*International Commission on Missing Persons* – IMCP). Celem tej organizacji jest udzielanie pomocy rządom i instytucjom pozarządowym w tworzeniu skutecznych systemów identyfikacji osób zaginionych w czasie współczesnych konfliktów zbrojnych lub w wyniku łamania praw człowieka. Organizacja ta sfinansowała m.in. utworzenie dwóch w pełni wyposażonych laboratoriów genetycznej identyfikacji człowieka na terenie krajów byłej Jugosławii, przyczyniając się do identyfikacji 15 000 ofiar konfliktów etnicznych w tym regionie. Udzieliła również znacznej pomocy w procesie identyfikacji ofiar tsunami w Tajlandii i huraganu Katrina, wspomagając prace identyfikacyjne ofiar ubiegłorocznego trzęsienia ziemi na Haiti[13].

Na zakończenie warto przypomnieć, że w roku bieżącym mijają 22 lata od momentu wdrożenia badawczych metod biologii molekularnej do polskiej kryminalistyki. Nowe metody i technologie nadały niespotykany dotąd wymiar identyfikacji człowieka, którego unikalny profil DNA może zostać określony nawet w przypadku, gdy dysponujemy tylko 2 nanogramami tego materiału[14]. Tak się złożyło, że bezpośrednią przyczyną zainteresowania środowiska kryminalistycznego metodą genetycznej identyfikacji zwłok i szczątków ludzkich był brak możliwości ustalenia tożsamości aż 62 spośród 183 ofiar katastrofy samolotu pasażerskiego PLL LOT – IŁ-62M „Tadeusz Kościuszko", który rozbił się 9 maja 1987 r. w Lesie Kabackim podczas podchodzenia do awaryjnego lądowania[15]. Niedługo po tym wydarzeniu, które było największą katastrofą w historii polskiego lotnictwa, odbył się VIII Zjazd Polskiego Towarzystwa Medycyny Sądowej i Kryminologii w Poznaniu, na którym zaprezentowano film dotyczący działań prowadzonych po katastrofie. Obecny wśród uczestników zjazdu dr hab. Ryszard Słomski z Zakładu Genetyki Człowieka PAN zaproponował wówczas wykorzystanie swojej wiedzy genetycznej i doświadczenia zdobytego na uniwersytetach Illinois oraz Chica-

[11] A. Tucholska-Lenart, *Analiza locus HLA DQ alfa w identyfikacji kryminalistycznych śladów biologicznych*, program III Łódzkiego Sympozjum na temat *Przestępstwa przeciwko życiu. Cesarka*, 16 - 18.09.1993 r. oraz A. Tucholska-Lenart, H. Miąskiewicz, W. Suszczewski, J. Wujec, *Analiza locus HLA DQ alpha w identyfikacji kryminalistycznych śladów biologicznych*, „Archiwum Medycyny Sądowej i Kryminologii" 1994, nr 44.

[12] A. Tucholska-Lenart, H. Miąskiewicz, W. Suszczewski, J. Wujec, *Zastosowanie analizy markerów genetycznych w badaniach biologicznych śladów kryminalistycznych*, program II Sympozjum Nauk Sądowych, Kraków, 20 - 23 września 1994 oraz A. Tucholska-Lenart, H. Miąskiewicz, W. Suszczewski, J. Wujec, *Zastosowanie analizy markerów genetycznych w badaniach biologicznych śladów kryminalistycznych*, „Problemy Kryminalistyki" 1995, nr 207.

[13] http://www.ic-mp.org.

[14] A. Tucholska-Lenart, *XX lat kryminalistycznych badań DNA w Polsce – wspomnienia eksperta*, w: *Kryminalistyka dla prawa – prawo dla ...,* s. 49 - 61 oraz K.B. Mullis, F.A. Faloona, *Specyfic synthesis of DNA in vitro via polymerase-catalysed chain reaction*. Meth. Enzymol. 1987, Nr 155, s. 335 - 350.

[15] R. Słomski, *Trudne początki badań DNA w Polsce, w; Kryminalistyka dla prawa – prawo dla ...,* s. 37 - 47.

go w celu jak najszybszego wdrożenia w Polsce badań DNA do identyfikacji indywidualnej człowieka. Był to czas, kiedy świat poznał już pionierskie prace Aleca Jeffreys'a z Uniwersytetu w Leicester w Wielkiej Brytanii, który wykazał, że w genomie człowieka występują proste oligonukleotydowe powtórzenia, które u każdego są takie same, ale ich ilość i częstotliwość powtórzeń jest nieskończenie zmienna i charakterystyczna dla poszczególnych osobników w populacji[16]. Uczony ten zastosował techniki biologii molekularnej do ich wizualizacji, a samą metodę nazwał, z uwagi na jej specyfikę *DNA-fingerprinting.* To odkrycie oraz nowe narzędzia biologii molekularnej dawały możliwość zastosowania badań DNA w medycynie sądowej (ustalanie spornego ojcostwa i pokrewieństwa) oraz w kryminalistyce (identyfikacja indywidualna sprawców przestępstw na podstawie śladów biologicznych). Metoda ta była kosztowna, czasochłonna i metodycznie skomplikowana m.in. z uwagi na konieczność stosowania radioizotopu fosforu, ale dawała możliwość identyfikacji indywidualnej, co stanowiło absolutny przełom w badaniach śladów biologicznych. Jak pisze w swoich wspomnieniach prof. R. Słomski, jego propozycja nie spotkała się z życzliwym przyjęciem środowiska medycyny sądowej. Zainteresował się nią natomiast Zakład Kryminalistyki Komendy Głównej MO[17]. Wkrótce (1988 r.) powołano tam zespół do współpracy z Zakładem Genetyki Człowieka PAN w celu wdrożenia metody *DNA-fingerprinting* do polskiej kryminalistyki[18]. 15 maja 1989 r. została wydana pierwsza w Polsce ekspertyza (sygnowana przez prof. R. Słomskiego) dotycząca sprawy o zabójstwo, w której kategoryczną opinię sformułowano na podstawie wyników analiz z zastosowaniem nowej metody badawczej. W tym samym roku, w październiku, zespół naukowo-badawczy, w którego składzie była również autorka niniejszego artykułu, otrzymał nagrodę państwową I stopnia za wdrożenie metod biologii molekularnej do polskiej kryminalistyki[19].

Streszczenie

Autorka przedstawia zastosowanie metod biologii molekularnej w identyfikacji ofiar katastrof lotniczych i ataków terrorystycznych, kładąc nacisk na obowiązujące w tej kwestii procedury INTERPOLU. Zgodnie z nimi powyższe metody uznawane są za najbardziej wiarygodne w procedurach identyfikacji zwłok i szczątków ludzkich. Profilowanie DNA genomowego, analiza DNA mitochondrialnego oraz analiza polimorfizmu chromosomu Y to badania umożliwiające identyfikację biologicznych śladów kryminalistycznych oraz szczątków ofiar katastrof lotniczych, ataków terrorystycznych i ofiar terroru politycznego. Autorka omawia problemy związane m.in. z identyfikacją ofiar zamachu na WTC, szczątków cara Mikołaja II i jego rodziny oraz szczątków odkrytych w masowych grobach w Bośni. W końcowej części artykułu omówiony został proces wdrażania badań DNA w Polsce oraz szczególna rola w tym procesie laboratorium kryminalistycznego ABW.

---

[16] A.J. Jeffreys, V. Wilson, S.I. Thien, *Indyvidual-specyfic „ fingerprints" of human DNA,* „Nature" 1985, nr 316, s. 76 - 79.

[17] R. Słomski, *Trudne początki badań DNA...,* s. 37 - 47.

[18] A. Tucholska, *Zastosowanie techniki DNA-fingerprinting w biologii kryminalistycznej,* program II Łódzkiego Sympozjum *Przestępstwa przeciwko życiu. Cesarka*, 18 - 20.09.1989 r.

[19] J. Wójcikiewicz, *Ekspertyza genetyczna w Polsce – 20 lat później,* w: *Kryminalistyka dla prawa – prawo dla...,* s. 93 - 103 oraz A. Tucholska-Lenart, *XX lat kryminalistycznych badań DNA w Polsce ...,* w: *Kryminalistyka dla prawa – prawo dla...,* s. 49 - 61.

Abstract

The author of the article presents the use of molecular biology methods for identifying casualties of airplane crashes and terrorist attacks, underlining valid INTERPOL procedures considered to be most reliable to identification of human remains. The techniques such as DNA profiling, mitochondrial DNA and Y chromosome polymorphism analysis are frequently used to identify biological traces as well as to reveal the identity of missing persons and victims of mass disasters such as air crashes or terrorist attacks. The author describes DNA technology-based forensic identification process by quoting experiences brought about by several high-profile cases as identification of remains of Tsar Nicholas II and his family, victims of WTC terrorist attack and bodies discovered in mass graves in Bosnia. The article refers also to the process of implementing DNA research techniques in Poland and the role of the ABW forensics laboratory in this matter.

V
OCHRONA EKONOMICZNYCH INTERESÓW PAŃSTWA

Antoni Podolski

Analiza wybranych aspektów problematyki ochrony infrastruktury krytycznej

W 2010 r. weszła w życie, wraz z aktem wykonawczym, kolejna ustawa dotycząca problematyki ochrony infrastruktury krytycznej w Polsce, tym razem w kontekście ochrony prawnej. Chodzi o *Ustawę o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych*[1]. Ustawa ta określa szczególne uprawnienia (sprzeciw wobec decyzji władz spółki) przysługujące ministrowi właściwemu do spraw Skarbu Państwa w spółkach kapitałowych lub grupach kapitałowych[2] prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych, których mienie zostało ujawnione w jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, sporządzanym przez dyrektora Rządowego Centrum Bezpieczeństwa na podstawie ustawy o zarządzaniu kryzysowym. Zgodnie z ustawą dyrektor RCB na podstawie szczegółowych kryteriów, we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, sporządza jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy[3]. Ustawa jest więc (nie tylko w tym aspekcie) ściśle związana z systemem ochrony infrastruktury krytycznej w Polsce, unormowanym w znowelizowanej w 2009 r. ustawie o zarządzaniu kryzysowym. Jest to szczególnie ważne, gdyż mamy tu przykład ustawy „resortowej" dotyczącej uprawnień dwóch z ministrów (właściwych w zakresie skarbu państwa i gospodarki), która uzupełnia (w zakresie bezpieczeństwa energetycznego) podstawy systemu ochrony infrastruktury krytycznej zawarte we wspominanej ustawie o zarządzaniu kryzysowym.

Te szczególne uprawnienia ministra Skarbu Państwa obejmują możliwość wyrażenia sprzeciwu wobec podjętej przez zarząd spółki uchwały lub innej dokonanej przez ten zarząd czynności prawnej, której przedmiotem jest rozporządzanie składnikami mienia, stanowiące rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej. Mienie, o którym mowa, obejmuje:

– infrastrukturę służącą do wytwarzania albo przesyłania energii elektrycznej,
– infrastrukturę służącą do wydobycia, rafinacji i przetwarzania ropy naftowej oraz magazynowania i przesyłania rurociągami ropy naftowej i produktów ropopochodnych, jak również terminale portowe do przeładunku zarówno tych produktów, jak i ropy naftowej,

[1] Dz.U. z 2010 r., Nr 65, poz. 404.

[2] W rozumieniu art. 3 ust. 1 pkt. 44 *Ustawy z dnia 29 września 1994 r. o rachunkowości* (Dz.U. z 2009 r., Nr 152, poz. 1223; Nr 157, poz. 1241 i Nr 165, poz. 1316 oraz Dz.U. z 2010 r., Nr 47, poz. 278).

[3] Infrastruktura krytyczna obejmuje systemy: zaopatrzenia w energię, surowce energetyczne i paliwa, łączności i sieci teleinformatycznych, finansowe, zaopatrzenia w żywność, zaopatrzenia w wodę, ochrony zdrowia, transportowe, ratownicze, zapewniające ciągłość działania administracji publicznej, produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych (art. 3 ust. 2 *Ustawy o zarządzaniu kryzysowym* z dnia 26 kwietnia 2007 r. z późn. zm.).

– infrastrukturę służącą do produkcji, wydobycia, rafinacji, przetwarzania, magazynowania i przesyłania paliw gazowych gazociągami oraz terminale skroplonego gazu ziemnego (LNG)[4].

Sprzeciwem może być objęta również uchwała organu spółki dotycząca:
– rozwiązania spółki,
– zmiany przeznaczenia lub zaniechania eksploatacji składnika mienia spółki,
– zmiany przedmiotu przedsiębiorstwa spółki,
– zbycia albo wydzierżawienia przedsiębiorstwa spółki lub jego zorganizowanej części oraz ustanowienia na nim ograniczonego prawa rzeczowego,
– przyjęcia planu rzeczowo-finansowego, planu działalności inwestycyjnej lub wieloletniego planu strategicznego,
– przeniesienia siedziby spółki za granicę – jeżeli wykonanie takiej uchwały stanowiłoby rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej.

Sprzeciw jest wyrażany w formie decyzji administracyjnej w terminie 14 dni od dnia otrzymania przez ministra właściwego do spraw Skarbu Państwa informacji od pełnomocnika ochrony infrastruktury krytycznej o podjęciu przez organy spółki uchwały lub dokonaniu przez zarząd spółki czynności prawnej, o której mowa powyżej, jednak nie później niż w terminie 30 dni od dnia ich dokonania. Podmiotem realizującym uprawnienia ministra ma być pełnomocnik ds. ochrony infrastruktury krytycznej[5].

Zamysłem osób przygotowujących obie regulacje – tj. nowelizację ustawy o zarządzaniu kryzysowym oraz ustawę o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w wyżej wymienionych sektorach było właśnie uzupełnienie systemu ochrony infrastruktury krytycznej w zakresie ochrony prawnej szczególnie istotnych z punktu widzenia bezpieczeństwa państwa przedsiębiorstw energetycznych. W związku z tym, wiele regulacji zawartych w *Ustawie o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa* (…) można zrozumieć i właściwie implementować jedynie w odpowiednim powiązaniu sekwencyjnym ze stosownymi przepisami znowelizowanej ustawy o zarządzaniu kryzysowym. Te zależności obejmują po pierwsze samą kwestię określenia listy spółek, których dotyczy ustawa (jak wspomniano, będą to te podmioty, których mienie zostało przedstawione w wykazie infrastruktury krytycznej sporządzonym przez dyrektora RCB na podstawie ustawy o zarządzaniu kryzysowym), a po drugie dotyczą sposobu wyznaczania przewidzianego w ustawie pełnomocnika ds. ochrony infrastruktury krytycznej i jego relacji z odpowiednimi przepisami ustawy o zarządzaniu kryzysowym.

Dlatego poważne problemy związane z właściwą interpretacją nowych uregulowań prawnych, a zwłaszcza pozycji i zakresu działania pełnomocnika ds. ochrony infrastruktury krytycznej, wynikają z niezaistnienia właściwych warunków do powstania korelacji obydwu wyżej wymienionych ustaw. Zgodnie bowiem z harmonogramem obowiązującym w momencie uchwalania nowelizacji *Ustawy o zarządzaniu kryzysowym, Ustawa o szczególnych uprawnieniach ministra właściwego do spraw Skarbu*

[4] Art. 1 ust. ust. 1 i 2 *Ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych* (Dz.U. z 2010 r., Nr 65, poz. 404).

[5] Art. 5 *Ustawy z dnia 18 marca 2010 r. o szczególnych uprawnieniach....*

Państwa miała wejść w życie co najmniej po ponad pół roku od wdrożenia ustawy o zarządzaniu kryzysowym. Do tego czasu powinien być już opracowany i notyfikowany (art. 5b ust. 7 pkt 4 ustawy)[6] właściwym podmiotom wymieniony w ustawie o zarządzaniu kryzysowym szczegółowy wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, z podziałem na systemy. Wykaz taki przygotowywany jest (art. 5b ust. 7 pkt 1) przez dyrektora RCB we współpracy z odpowiednimi ministrami odpowiedzialnymi za te systemy na podstawie szczegółowych kryteriów pozwalających wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, biorąc pod uwagę ich znaczenie dla funkcjonowania państwa i zaspokojenia potrzeb obywateli.

Zgodnie z niedawno wydanym do ustawy o zarządzaniu kryzysowym *Rozporządzeniem Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej* procedura prowadząca do ogłoszenia wykazu i notyfikowania go zainteresowanym podmiotom jest dość skomplikowana i rozłożona w czasie. Otóż, zgodnie z wyżej wymienionym rozporządzeniem, dyrektor RCB najpierw *opracowuje kryteria pozwalające wyodrębnić infrastrukturę krytyczną w ramach systemów, o których mowa w art. 3 pkt. 2 ustawy* (…) *i przekazuje je do uzgodnień ministrom i kierownikom urzędów centralnych*[7]. Kryteria te po uzgodnieniu przedstawiane są ministrom i kierownikom urzędów, którzy w terminie 6 tygodni od ich otrzymania przedkładają dyrektorowi RCB propozycje infrastruktury krytycznej do zamieszczenia ich w wykazie, o którym mowa w art. 5b ust. 7 pkt 1 ustawy o zarządzaniu kryzysowym. Następnie dyrektor RCB ma 6 tygodni na sprawdzenie, czy powyższe propozycje odpowiadają przedłożonym kryteriom i sporządzenie wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy w formie tabeli[8]. W tabeli tej podaje się nazwę i lokalizację infrastruktury krytycznej, podległość organizacyjną, w tym w stosunku do ministrów i kierowników urzędów centralnych, jeśli taka występuje, dane operatora przedmiotowej infrastruktury lub dane podmiotu zarządzającego w jego imieniu[9]. Jednocześnie w terminie 6 miesięcy od dnia otrzymania od dyrektora RCB wyżej wymienionych kryteriów ministrowie i kierownicy urzędów centralnych przygotowują i przedkładają temuż dyrektorowi informacje dotyczące pozostającej w ich właściwości infrastruktury i związanego z nią ryzyka, zagrożeń, sposobów zapewnienia ciągłości działania oraz odtwarzania i zapobiegania zakłóceniom[10]. Na podstawie tych informacji dyrektor RCB opracowuje projekt Narodowego Programu Ochrony Infrastruktury Krytycznej, który po rozpatrzeniu

[6] „Dyrektor Rządowego Centrum Bezpieczeństwa:
1) na podstawie szczegółowych kryteriów, o których mowa w ust. 2 pkt. 3, we współpracy z odpowiednimi ministrami odpowiedzialnymi za systemy, sporządza jednolity wykaz obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy;
2) opracowuje wyciągi z wykazu infrastruktury krytycznej, o którym mowa w pkt. 1, znajdującej się w danym systemie oraz przekazuje je ministrom i kierownikom urzędów centralnych odpowiedzialnym za dany system;
3) opracowuje wyciągi z wykazu infrastruktury krytycznej, o którym mowa w pkt. 1, znajdującej się na terenie województw oraz przekazuje je właściwym wojewodom;
4) informuje o ujęciu w wykazie, o którym mowa w pkt. 1, obiektów, instalacji lub urządzeń - ich właścicieli, posiadaczy samoistnych i zależnych".

[7] *Rozporządzenie Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie Narodowego Programu Ochrony Infrastruktury Krytycznej, § 3.*

[8] Tamże, § 4.1 - 2.

[9] Tamże, § 4.3.

ewentualnych uwag przedstawiany jest do zatwierdzenia Radzie Ministrów, w terminie jednego miesiąca od daty dokonania ostatniego uzgodnienia[11]. Następnie, w terminie 6 tygodni od dnia zatwierdzenia przez Radę Ministrów NPOIK, dyrektor RCB opracowuje wyciągi z wyżej wspomnianego wykazu i przekazuje je właściwym ministrom, kierownikom urzędów centralnych i wojewodom oraz informuje na piśmie operatorów infrastruktury krytycznej o ujęciu w wykazie danych obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej[12].

Należy pamiętać, że plan ochrony tego typu infrastruktury przygotowuje się zgodnie z zapisami ustawy o zarządzaniu krzysowym i stosownego rozporządzenia Rady Ministrów (Dz.U. z 2010 r., Nr 83, poz. 542) w ciągu 9 miesięcy od powiadomienia przez dyrektora RCB o ujęciu mienia w wykazie. Samo powiadomienie spółki przez MSP nie nakłada tego obowiązku.

Zgodnie z cytowanym powyżej art. 6 ust. 5a *Ustawy o zarządzaniu kryzysowym* wspomniani właściciele, posiadacze samoistni i zależni obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej mają obowiązek wyznaczyć, w terminie 30 dni od dnia otrzymania informacji o ujęciu we wspomnianym wykazie, osobę odpowiedzialną za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej.

Z kolei na podstawie ustawy o szczególnych uprawnieniach ministra Skarbu Państwa w spółkach, które są właścicielami oraz posiadaczami samoistnymi i zależnymi obiektów, instalacji lub urządzeń infrastruktury krytycznej ujętych w wykazie dyrektora RCB, należy powołać, w porozumieniu z ministrem właściwym do spraw skarbu państwa oraz dyrektorem RCB, pełnomocnika ds. ochrony infrastruktury krytycznej[13]. Pełnomocnik ten jest pracownikiem spółki, monitorującym jej działalność w zakresie dysponowania mieniem objętym ustawą i odpowiada za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony infrastruktury krytycznej. To sformułowanie, będące dokładnym zacytowaniem treści art. 6 ust. 5a ustawy o zarządzaniu kryzysowym, wskazuje na konieczność rozpatrywania zadań pełnomocnika w ścisłej korelacji z zapisami tejże ustawy.

Trzeba zatem pamiętać, iż zgodnie z *Ustawą o szczególnych uprawnieniach ministra* (...) pełnomocnik ds. OIK może być, ale nie musi, osobą odpowiedzialną za kontakty z administracją w rozumieniu ustawy o zarządzaniu kryzysowym. Oczywiście powierzenie obu tych podobnych funkcji jednej osobie jest rozwiązaniem pożądanym z punktu widzenia praktyki i ekonomiki zarządzania oraz zgodnym z intencjami ustawodawcy.

Gdyby więc w momencie wejścia w życie wyżej wymienionej ustawy była już realizowana w tym zakresie przedmiotowym nowelizacja ustawy o zarządzaniu kryzysowym, to w stosownych spółkach byłyby już powołane osoby odpowiedzialne za

[10] Tamże, § 5.1 - 2.
[11] Tamże, § 6.1 - 3.
[12] Tamże, § 10.
[13] Stosowną kandydaturę należy przedstawić wyżej wymienionym podmiotom w terminie 5 dni od otrzymania przez zarząd spółki informacji o ujęciu w przewidzianym w ustawie o zarządzaniu kryzysowym jednolitym wykazie obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy, przygotowywanym na podstawie ustawy (art. 5b ust. 7 poz. 1) przez Dyrektora RCB.

utrzymywanie kontaktów z podmiotami odpowiednimi w zakresie ochrony infrastruktury krytycznej – a więc również z odpowiednimi podmiotami administracji publicznej, w tym przypadku z ministrem właściwym ds. Skarbu Państwa oraz dyrektorem RCB. Zgodnie z logiką takie osoby zostałyby zapewne wskazane obu tym podmiotom jako kandydaci na funkcję pełnomocnika ds. ochrony infrastruktury krytycznej przez zarząd spółki. Wywołane opóźnieniem wydania stosownych rozporządzeń do ustawy o zarządzaniu kryzysowym odmienne podejście – tj. odrębność obydwu funkcji – grozi zachwianiem systemu ochrony infrastruktury krytycznej, tak w odniesieniu do danej spółki, jak i w szerszym, ogólnopaństwowym wymiarze. Potwierdzeniem powyższej logiki przyświecającej twórcom obydwu ustaw i wskazówką ich implementacji właśnie w duchu zgodności jest zapis paragrafu 9. rozporządzenia wydanego do ustawy o szczególnych uprawnieniach ministra Skarbu Państwa[14], zgodnie z którym zarząd spółki zapewnia pełnomocnikowi warunki organizacyjno-techniczne niezbędne do efektywnego wykonywania zadań, nie narzucając konieczności organizowania odrębnych struktur organizacyjnych, a więc sugerując wykorzystanie istniejących zasobów kadrowych i organizacyjnych spółki, wynikających na przykład z realizacji ustawy o zarządzaniu kryzysowym lub innych ustaw (dla przykładu – z *Prawa Ochrony Środowiska*).

Warto przy okazji wspomnieć, że takie podejście można znaleźć również w samej ustawie o zarządzaniu kryzysowym, w której (art. 6 ust. 6) stworzono możliwość, że jeśli dla obiektów, instalacji, urządzeń i usług infrastruktury krytycznej istnieją tworzone na podstawie innych przepisów plany odpowiadające wymogom planu ochrony tej infrastruktury, uznaje się, iż wymóg posiadania takiego planu jest spełniony. W *Rozporządzeniu Rady Ministrów z dnia 30 kwietnia 2010 r. w sprawie planów ochrony infrastruktury krytycznej*, w paragrafie 6.1 - 2 opisany jest tryb postępowania w takim przypadku. Zgodnie z nim operator infrastruktury krytycznej, który posiada inny plan opracowany na podstawie odrębnych przepisów i odpowiadający wymogom rozporządzenia, może przedłożyć go dyrektorowi RCB w celu potwierdzenia posiadania takiego planu. Dyrektor, rozpatrując ten problem, kieruje się potrzebą zapewnienia ciągłości funkcjonowania infrastruktury krytycznej oraz Narodowym Planem Ochrony Infrastruktury Krytycznej i działa w trybie przewidzianym w tym rozporządzeniu w celu uzgodnienia planów ochrony przedmiotowej infrastruktury. Odmowa uzgodnienia lub uznania istniejącego planu wymaga uzasadnienia na piśmie wraz ze wskazaniem elementów wymagających poprawy lub uzupełnienia i nowego terminu przedłożenia planu.

Do szczegółowych zadań pełnomocnika ds. ochrony infrastruktury krytycznej należy:

- zapewnianie ministrowi właściwemu do spraw Skarbu Państwa informacji dotyczących dokonania przez organy spółki czynności prawnej, której przedmiotem jest rozporządzenie składnikami mienia, o których mowa w ustawie, stanowiące rzeczywiste zagrożenie dla funkcjonowania, ciągłości działania oraz integralności infrastruktury krytycznej. Ustawowy zakres zainteresowań pełnomocnika obejmuje również inne uchwały organu spółki dotyczące rozwiązania spółki, zmiany prze-

[14] *Rozporządzenie Prezesa Rady Ministrów z dnia 14.07.2010 r. w sprawie pełnomocnika ds. ochrony infrastruktury krytycznej*, Dz.U. z 2010 r., Nr 135, poz. 906.

znaczenia lub zaniechania eksploatacji składnika mienia spółki, o którym mowa w art. 1 ust. ust. 1 i 2, zmiany przedmiotu przedsiębiorstwa spółki, zbycia albo wydzierżawienia przedsiębiorstwa spółki lub jego zorganizowanej części oraz ustanowienia na nim ograniczonego prawa rzeczowego, przyjęcia planu rzeczowo-finansowego, planu działalności inwestycyjnej lub wieloletniego planu strategicznego, a także przeniesienia siedziby spółki za granicę,

- przygotowywanie dla zarządu spółki oraz rady nadzorczej spółki informacji o ochronie infrastruktury krytycznej,
- zapewnianie zarządowi spółki doradztwa w zakresie istniejącej w spółce infrastruktury krytycznej,
- monitorowanie działalności spółki w zakresie ochrony infrastruktury krytycznej,
- przekazywanie informacji o infrastrukturze krytycznej dyrektorowi Rządowego Centrum Bezpieczeństwa na jego wniosek,
- przekazywanie i odbieranie informacji o zagrożeniu infrastruktury krytycznej we współpracy z dyrektorem Rządowego Centrum Bezpieczeństwa.

Pełnomocnikowi do spraw ochrony infrastruktury krytycznej przysługuje prawo do uczestniczenia w posiedzeniach zarządu spółki dotyczących spraw, o których mowa w ustawie, z głosem doradczym oraz żądania od organów spółki wszelkich dokumentów, informacji oraz wyjaśnień dotyczących tych spraw. Zarząd spółki jest zobowiązany do informowania pełnomocnika o każdym swym posiedzeniu odnośnie do wyżej wymienionych spraw, a także do przekazywania mu dokumentów lub informacji o podjęciu uchwały lub dokonaniu przez organy spółki czynności prawnych, o których mowa w ustawie, w terminie 3 dni od dnia ich podjęcia lub dokonania. Pełnomocnik do spraw ochrony infrastruktury krytycznej, w terminie 4 dni od dnia otrzymania dokumentów lub informacji o podjęciu uchwały albo dokonaniu przez organy spółki takich czynności prawnych, przekazuje ministrowi właściwemu do spraw Skarbu Państwa oraz dyrektorowi Rządowego Centrum Bezpieczeństwa pisemną informację w tej sprawie oraz stanowisko dotyczące wniesienia sprzeciwu, wraz z jego uzasadnieniem.

Wyżej wymieniony pełnomocnik sporządza dla zarządu oraz rady nadzorczej spółki raport o stanie ochrony infrastruktury krytycznej. Raport ten jest przygotowywany co kwartał lub na żądanie zarządu spółki (albo rady nadzorczej) i powinien zawierać informacje dotyczące ochrony infrastruktury krytycznej odnośnie do ochrony fizycznej, technicznej, prawnej, osobowej, teleinformatycznej oraz planów odbudowy i przywracania stanu tej infrastruktury do sprawnego funkcjonowania. Następnie dokument ten przekazywany jest ministrowi właściwemu do spraw Skarbu Państwa oraz dyrektorowi Rządowego Centrum Bezpieczeństwa. Jeżeli jest niepełny, zawiera nieścisłości lub nie przedstawia dokładnego stanu faktycznego spraw w nim zawartych, pełnomocnik do spraw ochrony infrastruktury krytycznej jest zobowiązany, na wezwanie ministra właściwego do spraw Skarbu Państwa lub dyrektora Rządowego Centrum Bezpieczeństwa, do jego uzupełnienia we wskazanym zakresie i terminie.

Pełnomocnik, o którym mowa, sporządza sprawozdanie kwartalne z wykonanych obowiązków, które składa ministrowi właściwemu do spraw Skarbu Państwa oraz dyrektorowi Rządowego Centrum Bezpieczeństwa. Przekazywanie informacji oraz raportów, o których wspomina ustawa, następuje zgodnie z przepisami o ochronie informacji niejawnych.

Poważnym mankamentem *Ustawy o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapi-*

tałowych utrudniającym właściwą, wskazaną powyżej, jej interpretację jest ograniczona delegacja ustawowa zawarta w art. 6 ust. 8[15] do wydania rozporządzenia dotyczącego szczegółowego trybu powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz sposób wykonywania przez niego obowiązku monitorowania działalności spółki w zakresie, o którym mowa w art. 2 ust. ust. 1 i 2, czyli ograniczonego jedynie do kwestii związanych ze stanem majątku spółki, a pomijająca inne zadania związane z ochroną tego typu infrastruktury, monitorowaniem jej stanu i doradztwem dla zarządu, opisane w art. 5 ust. 2 pkt pkt 2 - 6 ustawy[16].

Streszczenie

Artykuł dotyczy problematyki ochrony infrastruktury krytycznej, w tym sposobu powoływania oraz zakresu działania pełnomocnika ds. ochrony infrastruktury krytycznej, w świetle *Ustawy o szczególnych uprawnieniach ministra właściwego do spraw Skarbu Państwa oraz ich wykonywaniu w niektórych spółkach kapitałowych lub grupach kapitałowych prowadzących działalność w sektorach energii elektrycznej, ropy naftowej oraz paliw gazowych* oraz *Ustawy o zarządzaniu kryzysowym*. Szczególną uwagę poświęcono tu zagadnieniu właściwej interpretacji i korelacji zapisów obu ustaw i wydanych do nich rozporządzeń. Jest to kwestia niezwykle istotna w kontekście procesu wyznaczania we właściwych (w świetle obu ustaw) podmiotach gospodarczych osób mających pełnić z jednej strony funkcję pełnomocnika ds. ochrony infrastruktury krytycznej, a z drugiej osób odpowiedzialnych za utrzymywanie kontaktów z podmiotami właściwymi w zakresie ochrony tego typu infrastruktury.

Abstract

This article applies to issues of critical infrastructure protection, including the appointment and the scope of activity of the Plenipotentiary for Critical Infrastructure Protection, in the light of the Special Powers Act, the Minister of the Treasury and their performance in certain capital companies or holding companies operating in the electricity, oil and gas fuels and the Law on Crisis Management. Particular attention was paid to the proper interpretation and correlation of the records of both the laws and regulations issued to them. This is a crucial issue in the context of the appointment process initiated in the right (relative to both Acts) business entities, individuals to act both as the Plenipotentiary for Critical Infrastructure Protection and liaison with relevant entities in the protection of critical infrastructure.

[15] „Prezes Rady Ministrów określi, w drodze rozporządzenia, szczegółowy tryb powoływania i odwoływania pełnomocnika do spraw ochrony infrastruktury krytycznej oraz sposób wykonywania przez niego obowiązku monitorowania działalności spółki w zakresie, o którym mowa w art. 2 ust. 1 i 2, uwzględniając konieczność efektywnego wykonywania szczególnych uprawnień ministra właściwego do spraw Skarbu Państwa w spółkach kapitałowych lub grupach kapitałowych".

[16] „2) przygotowywanie dla zarządu spółki oraz rady nadzorczej spółki informacji o ochronie infrastruktury krytycznej;
3) zapewnienie zarządowi spółki doradztwa w zakresie istniejącej w spółce infrastruktury krytycznej;
4) monitorowanie działalności spółki w zakresie ochrony infrastruktury krytycznej;
5) przekazywanie informacji o infrastrukturze krytycznej dyrektorowi Rządowego Centrum Bezpieczeństwa na jego wniosek;
6) przekazywanie i odbieranie informacji o zagrożeniu infrastruktury krytycznej we współpracy z dyrektorem Rządowego Centrum Bezpieczeństwa" (Dz.U. z 2010 r., Nr 65, poz. 404).

Piotr Herman

Zorganizowana przestępczość – przyczynek do dyskusji

Autor podjął próbę wyjaśnienia tego, czym są zorganizowane struktury przestępcze w ujęciu służb specjalnych demokratycznych państw prawa oraz wykazania, w jaki sposób aktywność tych grup w dobie globalizacji i integracji europejskiej niesie zagrożenia wewnętrzne (dla pojedynczych krajów) i zewnętrzne (ponadpaństwowe i ponadnarodowe) dla współczesnych reżimów demokracji liberalnej. Państwa te – to rozwinięte kraje bogatej Północy traktujące kraje biednego Południa jako swoją bazę surowcową i wykorzystujące ich zacofanie technologiczne i prawne oraz tanią siłę roboczą.

Przestępczość zorganizowana: ku współczesności. Nadpodziemie

W latach 90. XX wieku wykształcił się nowy typ naukowców, którzy w ciągu ostatnich piętnastu lat zmienili akademickie rozumienie i podejście do przestępczości zorganizowanej. Ich „biblią" stała się książka Diega Gambetty, profesora socjologii na Uniwersytecie w Oksfordzie zatytułowana: *Mafia sycylijska. Biznes prywatnej ochrony*[1]. Autor ten stworzył teorię dotyczącą mafii, rozwijaną przez innych naukowców, jak choćby Federica Varesego, profesora socjologii na wymienionej powyżej uczelni, który z kolei wydał publikację pt. *Mafia rosyjska. Prywatna ochrona w nowej gospodarce rynkowej*[2].

Obie wspomniane powyżej pozycje bibliograficzne to efekt wieloletnich studiów i badań terenowych, które cechuje rzetelność metodologiczna oraz duża wiedza teoretyczna naukowców. Miejsca badań terenowych (Palermo na Sycylii oraz przemysłowe miasto Perm[3] położone na zamożnym Uralu) nie zostały wybrane przypadkowo, gdyż w tych właśnie miastach mamy do czynienia z wysokim poziomem przestępczości – w tym zorganizowanej.

Skupieni wokół idei nowego postrzegania zjawiska zorganizowanej przestępczości badacze przestali postrzegać mafię (mimo, iż rozumianą jako najwyższa forma zorganizowania przestępczości, o bezpośrednich powiązaniach z władzami lokalnymi i państwowymi) jako bandę zbirów, dla których przemoc jest początkiem i końcem wszelkiego działania. Utrzymują oni (za Gambettą), iż przemoc jest jedynie narzędziem do osiągania celów, mafia zaś jest angażowana w system zapewniania ochrony. Jest to jej główna działalność[4]. Biznesem mafii jest po prostu biznes[5]. I tym przede wszystkim zorganizowana przestępczość różni się od międzynarodowego terroryzmu, którego cele są natury politycznej (skierowane przeciwko reżimowi politycznemu).

---

[1] D. Gambetta, *Mafia sycylijska. Prywatna ochrona jako biznes*, Warszawa 2009, Oficyna Naukowa.

[2] F. Varese, *Mafia rosyjska. Prywatna ochrona w nowej gospodarce rynkowej*, Warszawa 2009, Oficyna Naukowa. Wyniki badań (w tym korzystanie z bezpośrednich wywiadów z respondentami) oraz wysoka liczba rosyjskojęzycznych źródeł pisanych (książek, artykułów prasowych, pozycji naukowych) pozwoliły odtworzyć rozwiniętą podkulturę świata przestępczego.

[3] Perm jest dużym rosyjskim miastem przemysłowym. Przez dziesięciolecia pozostawał tajnym ośrodkiem przemysłu zbrojeniowego ZSRR.

[4] M. Glenny, *McMafia. Zbrodnia nie zna granic*, Warszawa 2009, W.A.B., s. 469.

[5] C.L. Johnson, *Mafijny menedżer*, Warszawa 2003, s. 36.

W tym miejscu należy podkreślić, iż osiąganie zysków finansowych przez syndykaty przestępcze wiąże się często z zawłaszczaniem pełnienia niektórych funkcji państwa. Ochrona (podstawowa działalność zorganizowanych struktur przestępczych) związana jest z jej wykonywaniem, tj. z wykonywaniem funkcji administracyjnych, policyjnych, a nawet sądowych. Przestępczość zorganizowana wykorzystuje słabość państw mających problemy z efektywnym działaniem w opisanych powyżej sferach. Jest tym bardziej skuteczna, im mniej kompetentna jest policja i im mniej skutecznie działa sądownictwo. Przestępczość gwarantuje ochronę wtedy, gdy państwo jej odmawia i uznaje ją za nielegalną. Im zaś skuteczniejsza jest ochrona transakcji nielegalnych, tym szybszy staje się rozwój rynków nielegalnych. Ochraniając, zorganizowane grupy przestępcze stosują przemoc i nie przestrzegają prawa. Tworzą tzw. nadpodziemie[6].

Nadpodziemie[7] to struktura pełniąca funkcje państwa, gdy ono swych funkcji nie pełni (nie jest w stanie spełnić z uwagi na różne czynniki, np. ułomne prawo).

Jednakże cel aktywności syndykatów przestępczych nadal posiada naturę jedynie ekonomiczną, a nie polityczną.

Podklasa

Za czołowego przedstawiciela współczesnego nurtu tzw. teorii konfliktu uznawany jest Ralf Dahrendorf. Stoi on na stanowisku, iż model społeczeństwa opiera się na istnieniu stosunków zależności między różnymi grupami społecznymi, co w konsekwencji prowadzi do konfliktu i zmian społecznych. Konflikt ten ma charakter stały i cechuje go walka o władzę pomiędzy tymi, którzy władzę mają i tymi, którzy jej nie mają. A ponieważ zawsze będzie istniał nierówny dostęp do władzy różnych grup, a co za tym idzie – dysharmonia społeczna (będąca konsekwencją tej nierówności), to konflikt jest nieunikniony; leży on po prostu u podstaw liberalnej demokracji. Obecnie zaś staje się on konfliktem pomiędzy tymi, którzy są dobrze zakotwiczeni w jakimś systemie społecznym, i tymi, którzy do tego systemu nie należą. Jest to również konflikt pomiędzy osobami, które np. mają prawa obywatelskie i pracę, i osobami, które są zmarginalizowane, pozostają bez pracy i praw obywatelskich, ale w społeczeństwie jakoś funkcjonują. Ten rodzaj konfliktu zachodzi z jednej strony pomiędzy obywatelami i państwem, a z drugiej między tymi, którzy posiadają prawa obywatelskie i tymi, którzy ich nie posiadają.

W społeczeństwach liberalnej demokracji coraz liczniejszą część ich populacji stanowią ludzie pozbawieni praw obywatelskich. Dahrendorf określił tę kategorię mianem p o d k l a s y i zdefiniował ją jako zbiorowość ludzi, którzy nigdy nie pracowali albo pracowali w marginalnych sektorach gospodarki, oraz którzy nie są w stanie się utrzymać. Bywa i tak, że są oni bezrobotni z pokolenia na pokolenie, funkcjonują właściwie poza społeczeństwem. Myśliciel dostrzega, że ta grupa staje się coraz liczniejsza. Jeżeli zauważymy rosnącą przestępczość w rozmaitych środowiskach imigranckich, to mniej więcej zdamy sobie sprawę z tego, o co Dahrendorfowi chodzi. Wskazał on, iż głównymi cechami charakterystycznymi podklasy są: brak kwalifikacji, bezrobocie, zamieszkiwanie w szczególnych rejonach miast i zależność od opieki społecznej. Wielu członków podklasy należy do mniejszości etnicznych i żyje w niekompletnych ro-

[6] F. Varese, *Mafia sycylijska*...,. s. 20.
[7] M. Glenny, McMafia…. s. 451 - 490.

dzinach. Osoby te często wykazują skłonność do aberracyjnych zachowań, takich jak: nadużywanie alkoholu i narkotyków, a także wykazywanie skłonności do zachowań przestępczych. Podklasa usytuowana jest w najbiedniejszych rejonach miasta, tworzących często wyizolowane getta[8].

Powstawanie i zasilanie opisanej powyżej kategorii społecznej związane jest z przemytem osób, które to działanie mieści się w jednej z kategorii dóbr heksagonalnych, a mianowicie obrotu żywym towarem – zarówno w zakresie współczesnego niewolnictwa (handlu ludźmi), jak i przemytu imigrantów z krajów biednego Południa do państw bogatej Północy.

Dobra heksagonalne i ich pochodne, czyli z czego zorganizowana przestępczość czerpie zyski

Przyjmując za Gambettą, że główną działalnością syndykatów przestępczych jest szeroko rozumiana ochrona, można wskazać określone typy dóbr, z których czerpią one zyski (ochrona dóbr heksagonalnych w celu osiągnięcia korzyści finansowych). Dobra te podlegają szczególnej ochronie zorganizowanych grup przestępczych. Jako, że jest ich sześć[9], tworzą figurę zwaną heksagonem (stąd nazwa „dobra heksagonalne"). Należą do nich:

1) narkotyki i używki – w tej kategorii mieszczą się przede wszystkim narkotyki, papierosy i alkohol. Ponadto należałoby tu dodać dobra związane z rozrywką i konsumpcyjne (tzw. podróbki),
2) kamienie i metale szlachetne – kategoria ta dotyczy przede wszystkim diamentów i złota,
3) broń – kategoria dotycząca broni i materiałów wybuchowych, jak również dóbr mogących służyć wykorzystaniu militarnemu (tzw. podwójnego zastosowania),
4) produkty energetyczne – głównie ropa, benzyna i gaz. Obsługa handlu tymi produktami zwykle wiąże się z tworzeniem łańcuchów spółek oraz korzystaniem z usług kancelarii prawnych, polityków i lobbystów,
5) hazard – z jednej strony związany z ogromnym kapitałem, wyjątkowo trudnym do skontrolowania, z drugiej zaś – kumulujący znaczące wpływy do budżetu i zasilający kulturę oraz sport,
6) handel ludźmi – w tej kategorii mieści się zarówno niewolnictwo, w tym porwania dla okupu i prostytucja, jak i tania siła robocza (imigranci).

Wymienione powyżej dobra nie przynoszą zysków z samego faktu istnienia. Muszą być alokowane. Działania takie są pochodnymi dóbr heksagonalnych. Ponieważ podejmowane są wbrew obowiązującemu prawu (prawom poszczególnych państw), toteż kryminalizacja tych czynów powoduje ściganie karne ich sprawców. Przykład: działaniem pochodnym dobra heksagonalnego, jakim jest narkotyk, są wszystkie działania przestępcze związane z ich wydobyciem, produkcją, transportem (przemytem) i nielegalną sprzedażą końcowemu odbiorcy (konsumentowi).

---

[8] R. Dahrendorf, *Nowoczesny konflikt społeczny. Esej o polityce wolności*, Warszawa 1993, Czytelnik. Encyklopedyczne omówienie teorii Dahrendorfa w: *Leksykon myślicieli politycznych i prawnych*, E. Kundrea, M. Maciejewski (red.), Warszawa 2006, C.H. Beck, s. 87 - 88.

[9] Opisuje je dokładnie M. Glenny w: *McMafia* ...

Może wydawać się, że rozwój nowoczesnych technologii tworzy nowe typy dóbr przynoszących zyski. Dotychczasowa praktyka nie potwierdza jednak tego założenia. Rozwój internetu został wykorzystany również w niecnych celach, niezgodnych z prawem (cyberprzestępczość). Tak naprawdę nie mamy do czynienia z nowym typem dobra przynoszącego korzyści syndykatom przestępczym, lecz z zestawem narzędzi do popełnienia czynów przestępnych (włamań do banków, oszustw, wyłudzeń, prania pieniędzy itd.), czyli z działaniami pochodnymi dóbr heksagonalnych.

Alokacja dóbr heksagonalnych przynosi zorganizowanym strukturom przestępczym określone i wymierne korzyści finansowe. Środki finansowe łączą się z trzema odrębnymi kwestiami:
– są celem przedsięwzięć przestępczych (oszustwa, wyłudzenia, wymuszenia, przestępstwa bankowe i podatkowe),
– służą finansowaniu przedsięwzięć przestępczych,
– są legalizowane poprzez zastosowanie szeregu metod (tzw. pranie pieniędzy).

Z punktu widzenia instytucji zajmujących się zwalczaniem zorganizowanej przestępczości i międzynarodowego terroryzmu (w tym służb specjalnych) w przypadku „prania pieniędzy" szuka się kapitału pochodzącego z działalności przestępczej, który ma zostać zalegalizowany, zaś w przypadku finansowania przedsięwzięć przestępczych (i terroryzmu) szuka się legalnych i „czystych" pieniędzy, które mają dopiero posłużyć do zbrodniczych celów. Różnica dotyczy jedynie czasu popełnienia przestępstwa[10].

Typy współczesnych zorganizowanych struktur przestępczych i popełnianych przez nie czynów przestępnych

Praktyka wykształciła dwa główne typy zorganizowanych struktur przestępczych[11]:
1) specjalizujące się w oferowaniu ochrony, czyli usług związanych z egzekwowaniem kontraktów[12],
2) handlarze dóbr, dzielący się na trzy podgrupy: producentów, hurtowników i detalistów. Często każda z tych podgrup powiązana jest z konkretną grupą etniczną, a wszystkie trzy nawiązują ze sobą międzynarodową współpracę. Przykład: produkcja towaru (wydobycie surowca) zawsze odbywa się w miejscu (biedne Południe) oddalonym od najbardziej zyskownych rynków detalicznych (bogata Północ).

Z uwagi na ochronę posiadania (dążenia do posiadania) dóbr heksagonalnych, zorganizowane struktury przestępcze dopuszczają się popełniania przestępstw (działań pochodnych dóbr heksagonalnych) określanych mianem p r z e s t ę p s t w z o r g a n i z o w a n y c h. Nie wszystkie ich typy wchodzą w orbitę zainteresowań służb specjalnych.

Przestępcza aktywność zorganizowanych struktur wyraża się w dokonywaniu dwóch głównych typów[13] czynów przestępnych określanych mianem:

[10] M. Glenny, *McMafia*…,. s. 240.
[11] Tamże, s. 278 - 279.
[12] F. Varese, *Mafia rosuyjska*…. s. 21.
[13] J.W. Wójcik, *Kryminologiczna ocena transakcji w procesie prania pieniędzy*, Warszawa 2001, Twigger, s. 36 - 43.

1) przestępstw kryminalnych (napady rozbójnicze, kradzieże z włamaniem, kradzieże, akty terroru kryminalnego, sabotaż, wandalizm, kradzieże samochodów, handel ludźmi itp.),
2) przestępstw gospodarczych (fałszerstwa dokumentów publicznych, oszustwa kredytowe, prywatyzacyjne, podatkowe, celne, leasingowe, giełdowe, ubezpieczeniowe, zaliczkowe (nigeryjskie), upadłościowe, wyłudzenia, parabanki, „pranie pieniędzy" (etc.).

Ostatnia z wymienionych form przybiera charakter zorganizowany częściej niż przestępczość kryminalna. Wynika to z jej większej złożoności. Wiedząc czym są dobra heksagonalne, nie można oprzeć się wrażeniu, iż pochodna działalność heksagonalna (czyli działalność przestępcza zorganizowanych struktur) związana jest przede wszystkim ze zorganizowaną przestępczością ekonomiczną. Przedsięwzięcia tego typu ze swej natury wymagają współdziałania większej grupy osób – nawet jeśli zawarły one porozumienie do dokonania jednego tylko przestępstwa (czyli działali „wspólnie i w porozumieniu") – i poprzez to tworzą łańcuchy (często skomplikowanych) powiązań[14]. I częstokroć prowadzą do osiągania wyjątkowo dużych zysków finansowych – co jest celem aktywności i sensem istnienia zorganizowanych syndykatów przestępczych. Zyski te mogą pozostawać niewykryte przez odpowiedzialne instytucje państwowe jako pochodzące z nielegalnych działań z uwagi na nakładanie się przedsięwzięć przestępczych na różne formy legalnej działalności gospodarczej, kamuflującej aktywność niezgodną z prawem. Zagrożenia te, wyrażające się wkroczeniem zorganizowanych syndykatów przestępczych do obszaru przestępstw finansowych na wielką skalę, doprowadziły do wykształcenia się w służbach specjalnych państw demokracji liberalnej wyodrębnionych komórek kontrwywiadu ekonomicznego.

Porozumienie PCN. Pachanat

Z uwagi na kompetencje przypisywane służbom specjalnym państw demokracji liberalnej szczególne znaczenie ma jeden typ aktywności zorganizowanych struktur przestępczych: powiązania syndykatów z organami władzy państwowej (a właściwie z konkretnymi osobami pełniącymi określone funkcje) w różnych krajach. Zjawisko to wydaje się występować w wielu krajach, między innymi w Chinach, gdzie określa się je mianem porozumień PCN (*Political Criminal Nexus*) oraz w Rosji, gdzie system sprawowania władzy określany bywa przez samych Rosjan nazwą *pachanat*.

„Pachan" to słowo z rosyjskiego żargonu przestępczego, oznaczające: ojca, starca, starszego wśród więźniów kryminalnych, szefa milicji kryminalnej, a także Stalina. *Pachanat* stanowi sowiecką i postsowiecką odmianę samodzierżawia[15], określanego przez rządzących Federacją Rosyjską „demokracją sterowaną". Republika federalna o semiprezydenckim (mieszanym) systemie rządów stanowi de facto faktyczną odmianę samodzierżawia.

Upadek idei komunistycznej i likwidacja ZSRR stanowiły dla współczesnej Rosji ogromny problem. Przede wszystkim doprowadziły do powstania, wzrostu i wie-

[14] W. Mądrzejowski, *Przestępczość zorganizowana. System zwalczania*, Warszawa 2008, Wydawnictwa Akademickie i Profesjonalne, s. 48 - 49.
[15] J. Felsztinski, W. Pribyłowski, *Korporacja zabójców. Rosja, KGB i Putin*, Warszawa 2008, s. 406.

loletniego trwania szeregu kryzysów: politycznego, ekonomicznego, społecznego itp. Powstało wiele nowych (zależnych i niezależnych) państw, nastąpił wzrost nacjonalizmów, terroryzmu oraz struktur mafijnych liczonych w tysiącach grup, często o określonych składach etnicznych, które utworzyły potężne nadpodziemie w Federacji Rosyjskiej. Szefowie grup przestępczych nawiązali porozumienia z osobami pełniącymi ważne funkcje w organach władz lokalnych i państwowych – w tym i w służbach specjalnych. Zmiany z okresu prezydentury Władimira Putina doprowadziły do wzmocnienia roli rosyjskich służb (nie tylko specjalnych), osłabienia wpływu oligarchów i wprowadzenia współczesnego samodzierżawia – *pachanatu*. Nie zlikwidowały jednak powiązań władz z organizacjami przestępczymi[16]

Nadal aktualne pozostaje to, co były dyrektor CIA James Woolsey przekazał w 1999 r. Krajowej Komisji Bankowej. Jego zdaniem nowopoznany Rosjanin, który przedstawiłby się jako biznesmen, faktycznie (…) *może być tym, za kogo się podaje. Może być działającym pod przykrywką oficerem rosyjskiego wywiadu. Może być członkiem rosyjskiej organizacji przestępczej. Ale* (…) *może on być wszystkim naraz – i żadna z trzech wymienionych instytucji nie miałaby zastrzeżeń co do takiego układu* (…)[17]. To jedna z ciemnych stron *pachanatu*. I problem dla służb specjalnych państw demokracji liberalnej, w których osoby opisane przez Woolseya przebywają i działają.

Jednakże nie tylko w Rosji, ale i w innych państwach (o ustrojach innych, niż liberalna demokracja) może dochodzić do wykorzystywania przez służby specjalne zorganizowanych struktur przestępczych i organizacji terrorystycznych. Dobrym przykładem ilustrującym tę tezę wydają się być Indie i Pakistan, gdzie wojny gangów w Bombaju w latach 90. XX wieku były częściowo konfliktem zastępczym między agencjami wywiadowczymi obu państw, tj. indyjskich – IB i RAW oraz pakistańskiej ISI[18].

Political Criminal Nexus (porozumienia PCN) to zupełnie nowy rodzaj powiązań pomiędzy władzą państwową a organizacjami przestępczymi. Oznaczają całkowicie skorumpowany układ pomiędzy np. przywódcami partii w Chinach, a lokalnymi potentatami (jednocześnie zazwyczaj szefami lokalnego podziemia przestępczego)[19]. Porozumienia te zarządzają całymi gospodarkami w poszczególnych regionach Chin, generują ogromny majątek (co jest kwestią ekonomiczną), osłabiają władzę (kwestia polityczna) i są przedmiotem zainteresowania prawa karnego (kwestia kryminologiczna). Należy również wskazać, iż eksportują w kierunku krajów bogatej Północy tanią siłę roboczą oraz wszelkiego rodzaju podróbki, czyli dobra heksagonalne, stając się tym samym przedmiotem zainteresowania służb specjalnych państw demokracji liberalnej.

Struktury zorganizowanych grup przestępczych typu mafijnego

Liczba zorganizowanych struktur przestępczych jest wysoka: istnieją i dobrze prosperują mafie włoskie, grupy rosyjskie, południowoamerykańskie kartele narkotykowe, chińskie triady, grupy wietnamskie, japońska yakuza, grupy boryokudan itd.

[16] To, czy takie zmiany były w ogóle możliwe, stanowi odrębną kwestię, nie poruszaną w niniejszym artykule.
[17] M. Glenny, *McMafia*…. , s. 172.
[18] Tamże, s. 227.
[19] Tamże, s. 495.

Cechą charakteryzującą te systemy jest etniczność oraz rozwinięta podkultura świata przestępczego (specyficzne: język, normy zachowania, sposób ubierania, rytuały inicjacji, hierarchia i bezwzględnie egzekwowana dyscyplina). Z tego też powodu postanowiono opisać struktury wybranych trzech typów grup mafijnych: sycylijskiej Cosy Nostry, jej amerykańskiej odmiany oraz grup rosyjskojęzycznych. Zaznaczyć należy, iż grupy te charakteryzują się wyjątkowo wysokim stopniem zorganizowania wśród struktur przestępczych funkcjonujących we współczesnym świecie. Mimo dużej różnorodności (i liczby) zorganizowanych grup przestępczych, mogą one przyjmować strukturę hierarchiczną opartą na jednym z dwóch modeli[20]:

– syndykatu władzy, gdy powstają na bazie terytorialnej (często przybierają nazwę obszaru znajdującego się pod jej kontrolą); przykład: sycylijska Cosa Nostra,
– syndykatu przedsiębiorczości, gdy wytwarzają funkcjonalnie wyspecjalizowane struktury, świadcząc usługi ochrony w poszczególnych sektorach gospodarki (np. mafia kredytowa, narkotykowa, itp.); przykład: amerykańska Cosa Nostra.

Amerykańska Cosa Nostra

Mafia amerykańska jest organizacją posiadającą wyraźnie zdefiniowane role i reguły działania. Powinna składać się z dwudziestu czterech mafijnych rodzin, koordynowanych na szczeblu krajowym przez *comissione* (pełni funkcje arbitrażowe). Na czele każdej z rodzin stoi *boss*, któremu podporządkowane są jasno wyodrębnione stanowiska: *underboss* (zastępca szefa), *consigliere* (doradca), *caporegime* (nadzorca) oraz *soldato* (żołnierz mafijny) [21].

Sycylijska Cosa Nostra

Niemal identyczna jest struktura mafii sycylijskiej. Na czele rodziny stoi *capo famiglia* (szef), który wyznacza *vicecapo* (zastępcę szefa) i *consigliere* (doradcę). Szeregowi członkowie to *soldati*, zwani również *operai*. Dowodzą nimi *capodecina*, podlegający bezpośrednio szefowi rodziny. Działania mafii w konkretnej prowincji koordynuje *commissione provincionale*, znana jako *cupola*, utworzona przez *capi mandamento* (każdy reprezentuje trzy rodziny). Ponad nią stoi jeszcze *commissione regionale*, znana również jako *cupola regionale*, której szefuje *rappresentante*, zwany również *segretario* (niejako „pierwszy wśród równych")[22].

Rosyjskie grupy mafijne

W przypadkach rosyjskich grup mafijnych szczególną rolę odgrywa najwyższa kategoria osób ze świata przestępczego, tzw. *wory w zakonie*, czyli członkowie specyficznego bractwa „honorowych" złodziei (dominującą pozycję w środowisku kryminalistów osiągnęli oni w warunkach więziennych, w tzw. gułagach)[23]. Zazwyczaj *wor w zakonie* staje się osobą stojącą na czele rosyjskiej zorganizowanej grupy przestępczej

[20] F. Varese, *Mafia rosyjska*…. s. 207.
[21] Tamże, s. 203.
[22] Tamże, s. 204 - 206 i 214.
[23] Tamże, s. 190.

i znany jest jako *awtoritiet* (autorytet). Pracuje dla niego kilku *brigadirów*[24]. Przed *brigadirem* odpowiadają *bojewiki*, których rozkazy wykonują *torpiedy* (torpedy – „żołnierze" znajdujący się na samym dole hierarchii). Niektóre z takich grup sprawują silną kontrolę nad określonym terytorium, inne zaś stają się syndykatami przedsiębiorczości. Specyfika państwa rosyjskiego wydaje się wyrażać m.in. w podziale rynku „ochrony" na dwa segmenty: mafia dostarcza „ochronę" małym i średnim firmom, zaś duży biznes chroniony jest przez firmy działające na styku instytucji państwa i sektora prywatnego[25].

Warto zaznaczyć, że w samej Rosji funkcjonują również inne grupy mafijne, które nie przejęły tradycji *worów w zakonie*, zorganizowane na bazie etnicznej (np. grupy czeczeńskie).

Przestępczość zorganizowana w ujęciu służb specjalnych: próba zdefiniowania pojęcia

Na podstawie dotychczasowych rozważań można wskazać, iż w zakresie działań służb specjalnych państw demokracji liberalnej pozostaje rozpoznawanie i zwalczanie określonych czynów przestępnych popełnianych przez struktury zorganizowanej przestępczości. W orbitę zainteresowań służb nie wchodzą wszystkie zorganizowane grupy przestępcze, ani wszystkie czyny przestępne przez nie popełniane.

Z uwagi na międzynarodowy charakter działań przestępczych (syndykaty przedsiębiorczości) i wymuszoną w związku z tym współpracę z wieloma „miejscowymi" grupami (syndykaty władzy), w praktyce to, co określane jest jako „zorganizowane struktury przestępcze" to zazwyczaj dziesiątki niepowiązanych ze sobą (instytucjonalnie), większych i mniejszych grup, działających poza obszarem, na którym powstały. Zazwyczaj posiadają one określoną hierarchię, podział zadań i cechują się hermetycznością wewnętrzną i zewnętrzną, wyrażającą się również w sytuacjach, gdy członek grupy ląduje w więzieniu. Takie cechy można jednak wychwycić w tych grupach, które funkcjonują przez dłuższy czas. Istnieją również spiski, które powstają jedynie dla dokonania „wspólnie i w porozumieniu" określonego czynu przestępnego (czynów przestępnych). Wszystko to są jednak nadal różne postacie związku przestępczego.

Polskie prawo karne wyróżnia dwie formy zorganizowanej przestępczości: zorganizowaną grupę i zorganizowany związek przestępczy[26]. Zgodnie z orzecznictwem polskich sądów związek jest szczególną postacią porozumienia. Charakteryzuje się ist-

[24] Dotychczas nie ustalono, czy dana brygada mafijna, na której czele stoi *brigadir*, płaci *awtoritietowi* za zgodę na działalność na jego terenie, czy też jest integralną częścią większej grupy, na czele której stoi *awtoritiet*. Więcej w: F. Varese, *Mafia rosyjska*…,. s. 213.

[25] Tamże, s. 208 - 210.

[26] W art. 258 *Ustawy z dnia 6 czerwca 1997 r. Kodeks karny* (Dz.U. z 1997 r., Nr 88, poz. 553 z późn. zm.) przewidziana została odpowiedzialność za udział w związku przestępczym lub zorganizowanej grupie mającej na celu popełnienie przestępstwa (również o charakterze terrorystycznym). Należy zaznaczyć, iż w art. 64 § 2 kk enumeratywnie wymienione zostały cztery grupy sprawców, tzw. multirecydywistów, tj:
- sprawców, którzy z popełnienia przestępstwa uczynili sobie stałe źródło dochodu,
- sprawców, którzy popełniają przestępstwo, działając w zorganizowanej grupie albo związku mających na celu popełnienie przestępstwa,
- sprawców przestępstwa o charakterze terrorystycznym,
- sprawców określonych w art. 258 kk.

nieniem stałej więzi organizacyjnej grupy osób (co najmniej trzech), mających wspólny cel, konkretny program i formy współdziałania, zamierzoną stałość istnienia, kierownictwo, formy członkostwa, strukturę, środki i dyscyplinę organizacyjną. Zorganizowana grupa to również porozumienie kilku sprawców (co najmniej trzech), mające na celu popełnianie przestępstw (w celu osiągnięcia korzyści), lecz o uproszczonej i luźniejszej niż związek strukturze organizacyjnej (innymi słowy: zorganizowana grupa jest niższym stopniem organizacji w odniesieniu do związku przestępczego)[27].

Zorganizowane grupy przestępcze tworzą sieci wzajemnych powiązań. Zwykle oferują ochronę i współdziałają w łańcuchu działań przestępczych (pochodnych dóbr heksagonalnych) od miejsca wydobycia lub wytworzenia określonego dobra heksagonalnego do miejsca jego detalicznego zbytu oraz w eksploatacji tych dóbr. Celem działań jest osiągnięcie korzyści ekonomicznych. Z uwagi na osiąganie wysokich zysków finansowych oraz budowanie wpływu w różnych środowiskach społecznych (i politycznych) oraz przejmowanie części funkcji państwa, stanowią zagrożenie dla bezpieczeństwa wewnętrznego i zewnętrznego (ponadnarodowego i ponadpaństwowego) poszczególnych państw demokracji liberalnej. Struktury te zagrażają również globalizacji i wszelkim działaniom integracyjnym poszczególnych państw.

Zorganizowane grupy przestępcze w Polsce

Polskie służby specjalne zajmują się rozpoznawaniem i zwalczaniem jedynie niektórych kategorii zorganizowanej przestępczości, tj. tych, które zostały wskazane przez ustawodawcę w aktach prawnych regulujących działalność tychże służb (ABW, AW, SKW, SWW, CBA). Przykładowo, do zadań Agencji Bezpieczeństwa Wewnętrznego należy między innymi zwalczanie międzynarodowych zorganizowanych grup przestępczych zajmujących się w szczególności produkcją, przemytem i handlem narkotykami oraz bronią, a także przestępczością ekonomiczną[28]. Podkreślenia wymaga fakt, iż rozpoznawanie i zwalczanie (wybranych form) przestępczości to jedynie część zadań przypisanych przez ustawodawcę służbom specjalnym.

Zupełnie inaczej ustawodawca skonstruował zadania Policji, przypisując tej instytucji zwalczanie wszelkich istniejących form przestępczości (bez względu na typ zagrożenia czy formę; ściganiu podlega zarówno złodziej piwniczny, jak i przestępca powodujący olbrzymie straty). W jej strukturze od dziesięciu lat funkcjonuje Centralne Biuro Śledcze (w założeniu zwalczające jedynie tzw. „poważną" przestępczość).

W Polsce służy 98 tys. policjantów[29], w samym zaś CBŚ 2200 osób[30]. Służby specjalne zatrudniają nieporównywalnie mniejszą liczbę funkcjonariuszy. Dla największej

[27] R. Góral, *Kodeks karny. Praktyczny komentarz*, Warszawa 2000, Wydawnictwo Zrzeszenia Prawników Polskich, s. 110 - 112.

[28] Art. 5 *Ustawy z dnia 24.05.2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu* (Dz.U. z 2010 r. Nr 29, poz. 154).

[29] *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2010 roku*, dostępny [online] http://www.abw.gov.pl/portal/pl/236/575/Raporty.html.

[30] P. Kacak, *Ostatnia deska ratunku*, „Policja 997" z dnia 7 maja 2010 r.

z nich, ABW, w 2009 r. przyznano „aż" 5490 etatów[31]. Ilu jednak z tych funkcjonariuszy zajmuje się rozpoznawaniem i zwalczaniem przestępczości zorganizowanej?

Aby to ustalić należy, przyjrzeć się innym strukturom organizacyjnym. CBŚ to Biuro Komendy Głównej Policji. Jego działania, w połączeniu z pracą policjantów pionów kryminalnych, przynoszą wymierne rezultaty. Samo Biuro składa się z 25 jednostek organizacyjnych (Wydziałów i Zarządów). Działa, opierając się na strukturach policji w terenie. Funkcjonariusze ABW pełnią zaś służbę w jednej z trzydziestu pięciu jednostek organizacyjnych (Departamentów, Biur, Centrów i Delegatur), przy czym rozpoznawanie i zwalczanie przestępczości zorganizowanej można przypisać jedynie dwóm: Departamentowi Ochrony Ekonomicznych Interesów Państwa i Zwalczania Przestępczości Zorganizowanej oraz Departamentowi Postępowań Karnych[32]. Można przyjąć, iż wyżej wymienioną kompetencję ustawową realizuje łącznie około 600 funkcjonariuszy.

W Polsce ściganiem przestępczości zorganizowanej zajmują się również inne instytucje bezpieczeństwa wewnętrznego i porządku publicznego, np. 1300 funkcjonariuszy Straży Granicznej[33].

Wskazane powyżej trzy elementy różnicujące służby specjalne i policję (różnorodne zadania i kompetencje ustawowe[34], odmienne rozwiązania organizacyjne oraz różna liczba funkcjonariuszy) wpływają na to, iż w zupełnie różny sposób angażują one siły i środki w rozpoznawanie i zwalczanie przestępczości zorganizowanej. Jednak oficjalnie publikowane wyniki pracy obu struktur są porównywalne.

Zestawiając dane przekazane przez Agencję Bezpieczeństwa Wewnętrznego[35] oraz Centralne Biuro Śledcze Komendy Głównej Policji[36] i Straż Graniczną[37] można stwierdzić, że w 2010 r.:

1) liczba zorganizowanych grup przestępczych pozostających w zainteresowaniu wyniosła:
   – w przypadku ABW – 162 grupy (50 grup narkotykowych i 112 ekonomicznych, z czego 78 międzynarodowych),
   – w przypadku CBŚ – 547 grup (501 grup polskich, 36 międzynarodowych, 7 grup rosyjskojęzycznych i 3 grupy cudzoziemskie inne),
   – w przypadku SG – 220 grup (z czego 115 o charakterze międzynarodowym);

[31] M. Henzler, *Etaty i budżety służb specjalnych*, „Polityka" z dnia 26 października 2009 r, [online] http://www.polityka.pl/kraj/analizy/1500287,1,etaty-i-budzety-sluzb-specjalnych.read [dostęp: 30.03.2011]. Pozostałe cztery służby otrzymały znacznie mniej tych „limitów": AW – 1034, CBA – 1000, SKW – 1100, SWW zaś – 549 (należy zaznaczyć, że liczba etatów nie pokrywa się z faktyczną liczbą zatrudnionych funkcjonariuszy i pracowników cywilnych).

[32] *Zarządzenie Nr 73 Prezesa Rady Ministrów z dnia 26 czerwca 2002 r. w sprawie nadania statutu Agencji Bezpieczeństwa Wewnętrznego* (M.P. z 2002 r., Nr 26, poz. 432 z późn. zm.).

[33] Dane w posiadaniu autora.

[34] Rozdzielenie kompetencji pomiędzy policję i służby nie jest możliwe. Wszystkie pracują przedmiotowo, a nie podmiotowo, rozpoznając nie poszczególne przestępstwa, lecz zorganizowane grupy przestępcze, aktywne w wielu równych sferach jednocześnie (narkotyki, korupcja, przestępczość gospodarcza itp.). W związku z tym, nacisk kładziony jest na współpracę służb, a nie na podejmowanie (skazanych na porażkę) prób rozdzielania kompetencji.

[35] *Raport z działalności Agencji Bezpieczeństwa Wewnętrznego w 2010 roku*, [online] http://www.abw.gov.pl/portal/pl/236/575/Raporty.html.

[36] *Raport statystyczny 2010: Sprawozdanie z działalności Centralnego Biura Śledczego KGP w 2010 roku*, [online] http://cbs.policja.pl/portal/cbs/380/9890/Raporty_z_dzialalnosci.html.

[37] Dane w posiadaniu autora.

2) liczba osób objętych zainteresowaniem w sprawach operacyjnych dotyczących przestępczości zorganizowanej wyniosła:
   – w przypadku ABW – 2668 osób,
   – w przypadku CBŚ – 5600 osób,
   – w przypadku SG – 2511 osób;
3) liczba zorganizowanych grup przestępczych występujących w śledztwach wyniosła:
   – w przypadku SG – brak danych,
   – w przypadku ABW – 72 grupy,
   – w przypadku CBŚ – 150 grup;
4) liczba podejrzanych w śledztwach, z zarzutami z art. 258 kk (udział w zorganizowanej grupie przestępczej) wyniosła:
   – w przypadku ABW – 378 podejrzanych (345 Polaków i 33 cudzoziemców),
   – w przypadku CBŚ KGP – 1700 podejrzanych (1588 Polaków i 112 cudzoziemców).

Jak wynika z powyższych zestawień, w samym tylko 2010 r. jedynie wybrane instytucje bezpieczeństwa wewnętrznego (ABW jako służba specjalna, CBŚ jako część policji oraz SG) zidentyfikowały 929 zorganizowanych grup przestępczych działających na terytorium Polski, obejmując zainteresowaniem operacyjnym 10 794 osoby.

I, co istotne, co najmniej 239 zorganizowanym grupom przestępczym przypisano charakter międzynarodowy. Stwierdzono ponadto coroczny wzrost aktywności cudzoziemskich międzynarodowych zorganizowanych grup przestępczych.

A nie są to dane pełne (dotyczą bowiem wybranych instytucji bezpieczeństwa wewnętrznego i porządku publicznego). Ulegną one zwiększeniu w przypadku zsumowania danych, które można uzyskać od pozostałych czterech polskich służb specjalnych (AW, SKW, SWW, CBA) oraz innych instytucji. Poza tym należy wziąć pod uwagę, że nieznana jest tzw. ciemna liczba przestępstw (przestępstw nie zgłoszonych, o których istnieniu organa ścigania w ogóle nie wiedzą).

Powyższe liczby wyraźnie wskazują na realne zagrożenia państwa polskiego ze strony zorganizowanej przestępczości.

Przestępczość zorganizowana – ewolucja

Tragedia z 11 września 2001 r. spowodowała przedefiniowanie przez państwa demokratyczne (oraz ich służby specjalne) pojęcia terroryzm międzynarodowy oraz podejścia do zwalczania zagrożenia, które niesie dla nich to zjawisko. Wydaje się jednak, że stosunek do zwalczania zorganizowanych struktur przestępczych, jak również samego rozumienia, czym one są i jakie niosą zagrożenia, nie uległ zmianie od połowy lat 90. ubiegłego wieku. W tym jednak czasie globalizacja i procesy integracyjne uległy zdecydowanemu rozszerzeniu. W stosunku do pierwszej połowy ostatniej dekady XX w. obserwujemy w miarę swobodny przepływ kapitału, ludzi, usług i towarów. Zorganizowana przestępczość szeroko korzysta z tych udogodnień w celu osiągania jak największych zysków. W tym znaczeniu jednak „swobodny przepływ" związany jest także z ochroną i alokacją dóbr heksagonalnych. Czy rozumienie tych zagrożeń i przeciwdziałanie im przez współczesne służby specjalne państw demokratycznych nie powinno ulec przedefiniowaniu?

Streszczenie

Autor nie krytykuje globalizacji. W artykule porusza jedynie ciemną stronę wolnego przepływu kapitału, dóbr i usług oraz ludzi we współczesnym świecie. Przedstawia również struktury przestępczości zorganizowanej z punktu widzenia demokratycznych służb specjalnych i wyjaśnia, dlaczego termin przestępczość zorganizowana rozumiany jest przez służby specjalne demokratycznego państwa prawa nieco inaczej, niż przez instytucje policyjne.

Artykuł porusza kilka istotnych zagadnień, takich jak: problem podklas (odnoszący się do osób wywodzących się z niższej klasy społecznej i *Political Criminal Nexus* – PCN jako porozumienia przestępczo-politycznego). Jednocześnie ukazuje bezpośrednie powiązania świata polityki z aktywnością zorganizowanych struktur przestępczych. Jak wynika z jego treści, celem działania obu podmiotów jest osiągnięcie korzyści finansowych (ekonomicznych) poprzez przejęcie i posiadanie określonych dóbr. Autor określa je mianem dóbr heksagonalnych. W ich skład wchodzą: (1) narkotyki i używki, (2) kamienie i metale szlachetne, (3) broń, (4) produkty energetyczne, (5) hazard oraz (6) handel ludźmi.

W artykule ukazano, że dochód syndykatów przestępczych często wiąże się z przejmowaniem niektórych funkcji państwa, np. ochronnych. Ochrona związana jest z wykonywaniem funkcji administracyjnych, policyjnych, a nawet sądowych wtedy, gdy państwo ich nie realizuje.

W publikacji podkreślono również, że cel zorganizowanych struktur przestępczych jest natury ekonomicznej, a nie politycznej i że to obywatele demokratycznego państwa prawa, jako konsumenci, włączają się do podziemnego świata zorganizowanej przestępczości poprzez konsumpcję (popyt) dóbr heksagonalnych.

Na zakończenie autor podjął próbę zdefiniowania pojęcia przestępczość zorganizowana w ujęciu służb specjalnych demokratycznego państwa prawa.

Abstract

The author does not criticize globalization. The article touches upon the dark side of this fact, such as: free flow of capital, services and goods, as well as hampered free movement of people in present world. The author describes the structures of organized crime from the perspective of intelligence services of a democratic state. He explains why intelligence services define the term *organized crime* differently than those adopted in practice by the Police.

The article applies to many questions, such as: the problems of subclass (problems of people below the lower-working class) and Political Criminal Nexus (PCN as crime and political agreements). They were shown direct relationship with criminal activity of organized structures. The purpose of their actions is to achieve the greatest financial benefit (economic) through ownership and allocation of specific goods. The author refers to this concept as *hexagonal goods*: (1) drugs and stimulants, (2) precious stones and metals, (3) weapons, (4) energy products, (5) gambling and (6) human trafficking.

The author has shown that financial profit by the crime syndicates is often associated with acquisition of some functions of state. Protection is associated with executing administrative functions, police and judicial authorities then when the state fails to fulfil such functions.

The author stressed that the aim of organized criminal groups has an economic nature, not political. Citizens in democratic states, as consumers, are involved in functioning of the underground world of international organized crime through the consumption (demand) of hexagonal goods.

At the end the author undertook the task of defining *organized crime* from the perspective of the special services of democratic state.

VI
HISTORIA

Włodzimierz Suleja

Ignacy Matuszewski

Żył intensywnie i burzliwie. Na czas jego aktywności przypadły dwie wojny światowe, odrodzenie i militarna klęska II Rzeczypospolitej, ministerialne zaszczyty i okres politycznej niełaski. Był żołnierzem, politykiem, dyplomatą i publicystą. Faktami ze swego życiorysu mógłby obdzielić kilka osób, a w każdym przypadku nie byłyby to zdarzenia pozbawione znaczenia.

Przyszły szef Oddziału II Naczelnego Dowództwa Wojska Polskiego przyszedł na świat w roku 1891. Jego ojciec, po którym odziedziczył imię i zapewne literacki talent, również Ignacy, zapisał się w historii polskiej literatury jako znakomity krytyk. Syn wyrastał zatem w środowisku, w którym wczesne rozbudzenie intelektualne było i towarzyską normą, i niekwestionowaną drogą umysłowego rozwoju. Wybór drogi życiowej nie był jednak zbyt łatwy. Matuszewski studiował architekturę w Mediolanie, prawo w Dorpacie, filozofię w Krakowie na Uniwersytecie Jagiellońskim, a w rządzonej przez Rosjan Warszawie – rolnictwo.

U progu życiowych wyborów młodego Ignacego nadeszła I wojna światowa. Matuszewski spędził ją w szeregach rosyjskiej armii, gdzie dosłużył się stopnia sztabskapitana (dowodził m.in. oddziałem wywiadowczym). Jego rola wyraźnie wzrosła po wybuchu rewolucji lutowej, zwłaszcza zaś od momentu, gdy z rosyjskiej armii zaczęły wyodrębniać się polskie korpusy. To właśnie wówczas Matuszewski wysunął się na czoło grupy oficerów (w gronie tym byli m.in. Stefan Hubicki i Tadeusz Lechicki), którzy doszli do wniosku, że prawdziwym przywódcą polskiego wysiłku niepodległościowego jest nie kto inny, tylko *pozasłużbowy brygadier Legionów Polskich*, Józef Piłsudski, czemu dali wyraz, forsując podczas piotrogrodzkiego zjazdu wojskowych – Polaków uchwałę uznającą przyszłego Naczelnika za patrona swych poczynań. Ambitne, ale i nierealne, plany ściągnięcia Piłsudskiego za linię frontu zostały rychło przekreślone przez Niemców. Jednak nić ideowego porozumienia doprowadziła niebawem do powstania organizacji. Matuszewski, współtwórca Związku Broni, wiosną 1918 r. nawiązuje kontakt z kresowymi strukturami Polskiej Organizacji Wojskowej. W porozumieniu z nimi, wraz z innymi spiskowcami, podejmuje, niestety bez powodzenia, próbę przejęcia kontroli nad stacjonującym w Bobrujsku dowództwem I Korpusu. A wszystko po to, by podjąć walkę z Niemcami. Zagrożony represjami, przedostaje się do Kijowa, gdzie kontynuuje swe prace w szeregach konspiracji niepodległościowej (kieruje akcjami wywiadowczymi miejscowej POW). W roku 1918 Matuszewski dwukrotnie został skazany na śmierć – najpierw przez bolszewików, nieco później przez Niemców.

Nowa sytuacja, związana z zakończeniem I wojny światowej, stała się dla Matuszewskiego punktem wyjścia dla kolejnych, coraz poważniejszych, działań prowadzonych odtąd już na rozkaz samego Piłsudskiego. Naczelnik i Naczelny Wódz rychło docenił walory swego podkomendnego, toteż zaczął powierzać mu niezwykle delikatne misje, sytuując go zarazem w budowanych od podstaw strukturach wywiadu i kontrwywiadu. Matuszewski, który jesienią 1918 r. przybył do Warszawy jako kurier POW, już w połowie listopada powrócił do stolicy Ukrainy i z polecenia Tymczasowego Naczelnika Państwa prowadził rozmowy sondażowe z reprezentantami tamtejszych sił politycznych. Misja ta, choć nie przyniosła natychmiastowych rezultatów, pozwoliła

Piłsudskiemu na wyrobienie sobie opinii o potencjalnych zagrożeniach i sojuszniczych perspektywach. Samemu wysłannikowi zaś wystawiła opinię osoby i kompetentnej, i zdolnej do samodzielnych działań.

Kijowska misja wyznaczyła przyszłą wojskową karierę Matuszewskiego. Do Warszawy powrócił w początkach drugiej dekady grudnia i od razu został skierowany do pracy w Oddziale VI Ministerstwa Spraw Wojskowych. Był to jednak zaledwie dwutygodniowy epizod. Następnie, znów jako osobisty wysłannik Piłsudskiego, znalazł się w Poznaniu. To tajemnicza karta w jego życiorysie. Aktywność Matuszewskiego w Wielkopolsce, zwłaszcza zaś przesyłane przez niego raporty i analizy, świadczą o zainteresowaniu Naczelnika możliwością stworzenia na tym terenie militarnego „faktu dokonanego", do czego też niebawem doszło.

Wywiązanie się z dwóch niezwykle trudnych, a przy tym prowadzonych w całkowicie odmiennych realiach, misji doprowadziło Matuszewskiego do Oddziału II Naczelnego Dowództwa Wojska Polskiego. Służbę tam rozpoczął z dniem 29 grudnia 1918 r. Jego pierwszym przydziałem służbowym była Sekcja II (czyli Biuro Wywiadowcze), którym kierował niemal do końca sierpnia 1920 r., kiedy to powierzono mu zwierzchnictwo nad całym Oddziałem II.

Nie ulega wątpliwości, że już pierwszy przydział oznaczał, iż Matuszewski uznany został za „ideowego" piłsudczyka. Związał się zatem, i to na stałe, z ludźmi z najbliższego otoczenia Marszałka, stając się zarazem niezwykle ważną postacią w przygotowującym plany wojenne gronie jego współpracowników. Jego dyskretną obecność odczuwa się praktycznie we wszystkich znaczących przedsięwzięciach wojennych podejmowanych przez Polskę w czasie walk o jej granice. Matuszewski współuczestniczy w przygotowywaniu operacji wileńskiej wiosną 1919 r., jest nieocenionym ekspertem w sprawach ukraińskich, zwłaszcza w kontaktach z Symenem Petlurą (przekutych ostatecznie w sojusz polityczno-militarny), bierze wreszcie udział w organizacji wyprawy kijowskiej. Jego pieczy podlegał również radiowywiad, który odegrał, jak wynika z badań G. Nowika, nieocenioną i długo niedocenianą rolę, zwłaszcza w zmaganiach z Sowietami.

Matuszewski, co należy podkreślić szczególnie, miał znakomite rozeznanie zwłaszcza w sprawach rosyjskich. W czasie, gdy po zwycięskiej bitwie warszawskiej i zwieńczonej podobnym sukcesem operacji niemeńskiej rysowała się niepodległość kraju, zdecydowanie optował za utrzymaniem na wschodzie politycznej, a jeśli to możliwe nawet militarnej, aktywności. Nie podzielał złudzeń dużej grupy polityków, najrozmaitszych zresztą opcji, że wobec bliskiej finalizacji pokojowych rokowań przyszłą granicę wschodnią należy uznać za zupełnie bezpieczną. Co więcej, przestrzegał – o czym świadczy powstały w tym właśnie czasie w kierowanej przez niego strukturze referat specjalny pt. *Nasza polityka względem Rosji w związku z chwila obecną* – że niedocenianie lub lekceważenie problemu rosyjskiego *kryje w sobie podwójne niebezpieczeństwo*. Podwójne, związane bowiem zarówno z utrzymaniem się u władzy bolszewików, jak i ich mało prawdopodobnej, ale wciąż możliwej klęski. Matuszewski nie miał wątpliwości, że w przypadku objęcia przez bolszewików Kremla *po dłuższym czy krótszym wytchnieniu rzucą się niewątpliwie na Polskę*. Gdyby zaś władzę nad Rosją odzyskali „biali" przewidywał, iż z całą pewnością nie zechcą uznać zawartego przez Rosję pokoju, który bez wątpienia jest dla niej uciążliwy. Nie dziwi zatem jego konkluzja, że *podpisanie z bolszewikami traktatu pokojowego nie rozwiązuje wcale kwestii polsko-rosyjskich stosunków, a zmusza Państwo Polskie do stosowania nadal równie czynnej, jak przezornej polityki w tej sprawie*.

Gruntowniejsze przybliżenie poglądów Matuszewskiego wydaje się celowe nie tylko z powodu zajmowanej przez niego pozycji (nota bene, jako ekspert wojskowy został on wydelegowany przez Naczelnego Wodza do Rygi, gdzie toczyły się rokowania pokojowe), lecz także przede wszystkim po to, by przybliżyć sposób jego rozumowania i przesłanki, na których opierał swe analizy. Analizy te były w pełni zbieżne z dalekosiężnym programem stworzonym przez Piłsudskiego, a dotyczącym kwestii wschodnich. Matuszewski starał się jak najskuteczniej realizować zamysły federacyjne na powierzonym mu odcinku. Podobną rolę odgrywał zresztą i w czasie pokoju – wystarczy przywołać choćby jego działania, kiedy to, ponownie z rozkazu Piłsudskiego, monitorował zabiegi polskiej dyplomacji w czasie warszawskiej konferencji państw bałtyckich w marcu 1922 r.

W czasie pobytu w wojsku Matuszewski dosłużył się stopnia pułkownika. Nigdy nie poprzestawał na doskonaleniu jedynie umiejętności praktycznych, o czym świadczy ukończenie (z wysoką lokatą) Szkoły Sztabu Generalnego. W Oddziale II przesłużył jednak tylko do końca 1924 r. Był ideowym piłsudczykiem, czego zresztą nie ukrywał. Toteż i jego objęła przeprowadzana w wojsku „czystka". Jednak odsunięcie go na boczny tor nie było dla niego nazbyt uciążliwe, został bowiem mianowany attaché wojskowym w Rzymie.

Nowy etap w życiu Matuszewskiego rozpoczął się po zamachu majowym. Ściągnięty do kraju, w listopadzie 1926 r. zostaje naczelnikiem wydziału w Ministerstwie Spraw Zagranicznych, a w kilka miesięcy później dyrektorem Departamentu Administracyjnego w tymże ministerstwie. Trudno nie dostrzec, że pełnił w ten sposób w jednym z głównych resortów funkcję swoistego „męża zaufania" Marszałka. W służbie dyplomatycznej pozostawał do momentu uformowania się rządu Kazimierza Świtalskiego. Z Bukaresztu, gdzie od roku 1928 stał na czele poselstwa, został sprowadzony do Ministerstwa Skarbu przez nowego premiera. Była to nominacja tyleż zaskakująca, co trafna. Świtalski, jak wspominał po latach, poszukiwał takiego kandydata na ministra tego resortu, który *swojej zgody na takie czy inne przedsięwzięcie nie uzależnia tylko od tego, ile to będzie kosztowało dziś czy w latach następnych, ale prócz tego kryterium będzie umiał dzięki swym szerszym horyzontom myśleć nie tylko buchalteryjnie, ale i politycznie*.

Na propozycję Świtalskiego i Piłsudski, i prezydent Mościcki zareagowali początkowo zdziwieniem; sam zainteresowany zaś do przejęcia nowych obowiązków wcale się nie kwapił. Swemu przyszłemu zwierzchnikowi wyjaśniał, dlaczego woli służbę dyplomatyczną od zajmowania się sprawami wewnętrznymi. Dowodził, że w dyplomacji *istnieje tolerancja dla takich metod, jak bluffowanie, jak nieszczerość, jak wprowadzanie drugiej strony w błąd, jak wreszcie uciekanie się do szantażu, gdy ma on szanse udania się. Ale te same metody, gdy ucieka się do nich w stosunku do własnych rodaków, a nie w stosunku do obcych, mierżą go i nie miałby ochoty do konieczności ich stosowania w polityce wewnętrznej.*

Świtalskiemu jednak udało się ostatecznie przełamać te skrupuły. Matuszewski kierował resortem skarbu (poza zespołem Świtalskiego) aż w czterech kolejnych gabinetach. Nie był to okres łatwy, przypadł bowiem na kryzys gospodarczy. W tych skrajnie trudnych realiach Matuszewskiemu udało się utrzymać zarówno równowagę budżetową, jak i zadbać o stabilizację krajowej waluty. Z ministerstwem musiał się jednak pożegnać, i to z powodu niezadowolenia samego Marszałka. Piłsudski miał mu za złe, że zdecydował się na redukcję wydatków wojskowych i obniżenie (aż o 15%) pensji zawodowym wojskowym.

Odejście z rządowej ekipy było równoznaczne z zepchnięciem Matuszewskiego na boczny tor, ale nie oznaczało wyeliminowania go z kręgu szeroko rozumianego sanacyjnego obozu decyzyjnego. Jako były minister podjął pracę w zespole redakcyjnym rządowej „Gazety Polskiej". Lektura jego artykułów przekonuje, że przejawiał nie tylko talent literacki, lecz także że cechowała go wyjątkowa przenikliwość polityczna. Z pracy w „Gazecie" wycofał się po śmierci Marszałka w roku 1936, zajmując coraz bardziej krytyczne stanowisko wobec jego politycznych następców.

Matuszewski z ogromnym niepokojem obserwował przede wszystkim rozwój sytuacji międzynarodowej. Lektura jego artykułów zamieszczanych na łamach redagowanej przez niego „Polityki Narodów" świadczy o tym, że geopolityczne położenie II Rzeczypospolitej uznawał za skrajnie niebezpieczne, a możliwości obronne za niedostateczne. On, w dobie kryzysu zwolennik redukcji wydatków na armię, na rok przed wybuchem wojny domagał się wydatnego zwiększenia wojskowego budżetu i modernizacji sił zbrojnych, a szczególnie formowania dywizji pancernych. Nie miał złudzeń, że Polska przetrwa militarną konfrontację z niemiecką Rzeszą. Obawiał się też, i dawał temu wyraz, że niemieckiemu uderzeniu towarzyszyć będzie agresja sowiecka…

W czasie niemieckiej agresji rola, jaką odegrał Matuszewski, okazała się trudna do przecenienia. Wprawdzie nie dowodził na polu bitwy, ale wespół z Henrykiem Floyar-Rajchmanem ewakuował z Banku Polskiego przez Rumunię i Turcję 75 ton złota, przekazując te zasoby do dyspozycji rządu RP. We Francji, pomimo usilnych starań, nie otrzymał wojskowego przydziału, toteż po jej klęsce wyemigrował do Stanów Zjednoczonych. Dotarł tam we wrześniu 1941 r.

Za oceanem Matuszewski stał się jednym z największych krytyków linii politycznej gabinetu Sikorskiego i jego następców. Ostro ją zwalczał (czynił to końca życia), oskarżając zwłaszcza o nadmierną uległość wobec ZSRR. Organizował też Polonię amerykańską, współtworząc Komitet Narodowy Polaków Amerykańskiego Pochodzenia i powołując do życia, wespół z Wacławem Jędrzejewiczem, funkcjonujący w Nowym Jorku do dziś Instytut Józefa Piłsudskiego. Podczas wojny spadło na niego wyjątkowo dotkliwe nieszczęście – w czasie Powstania Warszawskiego Niemcy zamordowali jego córkę Ewę. Sam Matuszewski zmarł nagle, tuż po wojnie, w sierpniu 1946 roku.

Streszczenie

Ignacy Matuszewski (1891 - 1946) to jeden z najwybitniejszych polityków dwudziestolecia międzywojennego. Wprost z rosyjskiej armii trafił w 1918 r. do POW, stamtąd zaś do odrodzonego Wojska Polskiego, w którym stanął na czele Biura Wywiadowczego, a od sierpnia 1920 r. do Oddziału II Naczelnego Dowództwa. W Wojsku Polskim dosłużył się stopnia pułkownika, kończąc swą misję jako attaché wojskowy w Rzymie. Po zamachu majowym objął ważne funkcje w MSZ – m.in. posła w Bukareszcie. W 1928 r. został ministrem skarbu w gabinecie K. Świtalskiego, pełniąc tę funkcję do roku 1931. We wrześniu 1939 r. jest jednym z organizatorów ewakuacji polskiego złota; szykanowany na emigracji, jako piłsudczyk emigruje do USA, skąd ostro zwalcza linię polityczną Sikorskiego i jego następców. Zmarł nagle w sierpniu 1946 r.

Abstract

Matuszewski, Ignacy (1891-1946) is one of the most prominent politicians of the interwar decades. From the Russian Army in 1918, goes to the POW, and next to the Polish Army, where he becomes the head of Intelligence Bureau, and since August 1920, the Division II High Command. While serving in the Polish Army he was promoted to the rank of colonel. His last position was military attache in Rome. Following the May Coup is in the Ministry of Foreign Affairs (MP in Bucharest). In the years 1928 - 1931 Chancellor of the Exchequer in the government of K. Switalski. In September 1939, is one of the organizers of the evacuation of Polish gold - emigrates to the U.S., where it fights hard political line Sikorski and his successors. Died suddenly in August 1946.

Zespół funkcjonariuszy
Biura Ewidencji i Archiwum Agencji Bezpieczeństwa Wewnętrznego[1]

PRÓBA DOKONANIA BILANSU WSPÓŁPRACY KGB - SB W LATACH 1970 - 1990. Cz. II

Ochrona kontrwywiadowcza jednostek Armii Radzieckiej stacjonujących na terenie PRL

Po zakończeniu II wojny światowej z jednostek Armii Czerwonej (a od 1946 r. Armii Radzieckiej) stacjonujących na terenie Europy Środkowej i Południowej na podstawie dyrektyw podpisanych przez Stalina utworzono tzw. Grupy Wojsk:
– Centralną (na bazie 1. Frontu Ukraińskiego) rozlokowaną w latach 1945 - 1955 na terenie Austrii i Węgier, a od 1968 r. w Czechosłowacji,
– Południową (na bazie 3. Frontu Ukraińskiego) stacjonującą w latach 1945 - 1947 na terenie Rumunii i Bułgarii, a od 1957 r. na Węgrzech,
– Okupacyjną (na bazie 1. Frontu Białoruskiego) znajdującą się w Niemczech, która w 1956 r. zmieniła nazwę na „Grupa Wojsk Radzieckich w Niemczech", a od 1989 r. na „Zachodnia Grupa Wojsk",
– Północną (na bazie 2. Frontu Białoruskiego), ulokowaną na terenie Polski[2].

Utworzenie wymienionych Grup Wojsk Armii Czerwonej było jednym z elementów postanowień konferencji jałtańskiej, traktujących Europę Środkowo-Wschodnią jako radziecką strefę wpływów. Początkowo stacjonowanie tych Grup opierało się na zapisach porozumienia pomiędzy PKWN i rządem radzieckim w sprawie stosunków między radzieckim dowództwem a administracją polską z 26 lipca 1944 r. Regulowało ono jednak pobyt Armii Czerwonej na terytorium Polski tylko w okresie wojny[3]. Dopiero w latach 50. podpisano umowy, które odnosiły się do pobytu tych wojsk na terenie Polski; tj. *Umowę między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Związku Socjalistycznych Republik Radzieckich o statusie prawnym wojsk radzieckich w Polsce, podpisaną w Warszawie dnia 17 grudnia 1956 roku*[4] oraz *Porozumienie między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Związku Socjalistycznych Republik Radzieckich o wzajemnej pomocy prawnej w sprawach związanych z czasowym stacjonowaniem wojsk radzieckich w Polsce, podpisane w Warszawie dnia 26 października 1957 roku*[5].

---

[1] Opracowanie pod redakcją Roberta Oska i Mirosława Grabowieckiego.

[2] J. Hytrek-Hryciuk, *Rosjanie nadchodzą! Ludność niemiecka a żołnierze Armii Radzieckiej (Czerwonej) na Dolnym Śląsku w latach 1945 - 1948*, Wrocław 2010, IPN Oddział we Wrocławiu, s. 17 - 29.

[3] P. Piotrowski, *Organizacja i dyslokacja Armii Czerwonej/Radzieckiej na terytorium Polski w latach 1944 - 1993*, w: *W objęciach Wielkiego Brata: Sowieci w Polsce 1944 - 1993*, K. Rokicki, S. Stępień (red.), Warszawa 2009, IPN, s. 123 - 149.

[4] *Umowa między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Związku Socjalistycznych Republik Radzieckich o statusie prawnym wojsk radzieckich w Polsce, podpisana w Warszawie dnia 17 grudnia 1956 roku,* Dz.U. z 1957 r., Nr 29, poz. 127.

[5] *Porozumienie między Rządem Polskiej Rzeczypospolitej Ludowej a Rządem Związku Socjalistycznych Republik Radzieckich o wzajemnej pomocy prawnej w sprawach związanych z czasowym stacjonowaniem wojsk radzieckich w Polsce, podpisane w Warszawie dnia 26 października 1957 roku*, Dz.U. z 1958 r., Nr 37, poz. 167.

Większość sił lądowych Północnej Grupy Wojsk Armii Radzieckiej (dalej: PGWAR) zlokalizowano w dwóch miejscach: w Świętoszowie i w Bornem-Sulinowie. Oba garnizony były wyłączone spod jurysdykcji Polski. Wojska lotnicze (4. Armia Lotnicza) rozlokowane zostały wzdłuż zachodniej granicy naszego kraju, m.in. w Bagiczu, Legnicy, Kluczewie i Brzegu. Marynarka wojenna ZSRR utrzymywała w Świnoujściu Brygadę Kutrów Rakietowo-Torpedowych[6].

Dodatkowo na terenie Polski znajdowały się dwa sztaby Armii Radzieckiej: Sztab Dowództwa Zachodniego Kierunku Strategicznego z siedzibą w Legnicy oraz Sztab PGWAR, który w 1984 r. został przeniesiony z Legnicy do Świdnicy[7].

Jednostki AR były uznawane przez SB za obiekty o dużym znaczeniu. Wiele z nich zaliczano do kategorii „A", co oznaczało najwyższą rangę znaczenia militarnego. Wobec tych jednostek musiały być podejmowane działania zmierzające do zapewnienia im jak najlepszej ochrony kontrwywiadowczej. Na początku lat 70. w Wydziałach II KWMO (kontrwywiad), na których obszarze stacjonowały jednostki AR, powstały Sekcje VI (tzw. sekcje wojskowe), których zadaniem była ochrona garnizonów AR[8]. Funkcjonowanie wojsk radzieckich na terytorium Polski powodowało systematyczne kontakty funkcjonariuszy Wydziału II z przedstawicielami KGB rezydującymi przy jednostkach AR. I tak, np. Sekcja VI Wydziału II KWMO w Łodzi miała za zadanie m.in. organizowanie i wykonywanie pracy kontrwywiadowczej w zakresie operacyjnej ochrony obiektów wojskowo-obronnych Wojska Polskiego oraz jednostki AR w Łowiczu, współpracę z innymi wydziałami KWMO oraz z Wojskową Służbą Wewnętrzną[9] i kontrwywiadem wojskowym AR[10]. Natomiast Sekcja VI WUSW w Szczecinie realizowała przedsięwzięcia związane z zabezpieczaniem ćwiczeń wojskowych na poligonach, jak również współpracowała z Wydziałem Specjalnym KGB w Kluczewie, któremu przekazywała m.in. informacje dotyczące przebywania zachodnich dyplomatów na ochranianym terenie[11].

Współdziałanie Wydziałów II z oficerami kontrwywiadu AR realizowane było na podstawie wytycznych Dyrektora Departamentu II MSW z dnia 15 maja 1978 r. *Dla za-*

---

[6] M.L. Krogulski, *Okupacja w imię sojuszu: Armia Radziecka w Polsce 1956 - 1993*, Warszawa 2001, s. 47 - 48.

[7] We wrześniu 1984 r. powołano główne dowództwa Zachodniego i Południowo-Zachodniego Kierunku Strategicznego. Dowództwo Zachodniego Kierunku Strategicznego rozmieszczono w Legnicy; aby zwolnić pomieszczenia sztabowe, dowództwo PGWAR przeniesiono wówczas do Świdnicy. Zachodniemu Kierunkowi Strategicznemu podlegały wojska stacjonujące na terenie NRD, Czechosłowacji, Polski, Białorusi i zachodniej Ukrainy. Dowództwo to zostało rozwiązane w czerwcu 1992 r.; wówczas do Legnicy powróciło Dowództwo PGWAR. Źródło: P. Piotrowski, *Organizacja i dyslokacja Armii Czerwonej/Radzieckiej ...,* s. 133.

[8] Wydział VI Departamentu II zajmował się ochroną kontrwywiadowczą transportu międzynarodowego, inwigilacją środowisk krótkofalowców, a także ochroną obiektów strategiczno-obronnych Wojska Polskiego i PGWAR. Wydział VI Departamentu II miał swoje odpowiedniki w terenie jako Sekcje VI Wydz. II KWMO (od 1983 r. WUSW). Źródło: *Aparat bezpieczeństwa w Polsce. Kadra kierownicza tom III 1975 - 1990*, P. Piotrowski (red.), Warszawa 2008, IPN, s. 24 - 50.

[9] Wojskowa Służba Wewnętrzna zajmowała się kontrwywiadem wojskowym. Źródło: B. Kapuściak, *Instrukcje pracy kontrwywiadowczej Wojskowej Służby Wewnętrznej wraz z instrukcjami prowadzenia dokumentacji i ewidencji (1957 - 1990)*, Kraków 2010, IPN, s. 15 - 16.

[10] *Zakres pracy i struktura organizacyjna Wydziału II KWMO w Łodzi z dnia 17 maja 1971 r.* Źródło: Archiwum Instytutu Pamięci Narodowej Oddział w Łodzi [dalej: AIPN Ld], IPN Ld Pf10/925, k. 293 - 319.

[11] Informacja (brak naniesionej daty) dotycząca zabezpieczenia obiektów WP i AR na terenie województwa szczecińskiego. Sprawa obiektowa krypt. Tarcza. Źródło: Archiwum Instytutu Pamięci Narodowej Oddział w Szczecinie [dalej: AIPN Sz], IPN Sz 011/2074, t. 3, k. 47.

pewnienia bezpieczeństwa radzieckich jednostek wojskowych przebywających zgodnie z Układem Warszawskim na terenie Polski, organy bezpieczeństwa PRL utrzymują kontakty z odpowiednimi organami kontrwywiadu Armii Radzieckiej(...)[12]. Opierając się na powyższych wytycznych zarówno SB, jak i organa kontrwywiadu AR miały dokonywać wzajemnej wymiany informacji, udzielać sobie pomocy i wspólnie przeprowadzać przedsięwzięcia operacyjno-agenturalne mające na celu ochronę jednostek wojskowych AR na terenie Polski. Dodatkowo podstawą do organizacji pracy operacyjnej Sekcji VI Wydziałów II w tej kwestii były wytyczne Departamentu II MSW z czerwca oraz lipca 1983 r. Współdziałanie obu służb ukierunkowane było na:

– wspólne opracowywanie kontrwywiadowczego planu zabezpieczania jednostek AR,
– udoskonalanie systemu kontrwywiadowczego zabezpieczenia jednostek i obiektów AR w celu ujawniania agentury zachodnich służb specjalnych,
– wspólne wypracowanie sytuacji operacyjnych z zamiarem zastosowania przedsięwzięć operacyjnych zmierzających do dezinformowania przeciwnika,
– wspólne podejmowanie działań operacyjnych mających na celu ujawnianie podejrzanych zainteresowań jednostką AR oraz osób mogących pozostawać w zainteresowaniu obcych służb. Dotyczyło to m.in. obywateli polskich zatrudnionych w jednostkach AR w charakterze pracowników kontraktowych i osób pracujących w instytucjach świadczących usługi na rzecz AR oraz było ukierunkowane na ujawnianie kontaktów oficerów AR z cywilami. Zgodnie z wyżej wymienionymi wytycznymi z oficerami kontrwywiadu AR współdziałał m.in. Wydz. II WUSW w Skierniewicach oraz grupa II RUSW w Łowiczu i Sochaczewie[13].

W latach 70. Wydział VI Departamentu II założył dwie sprawy obiektowe o kryptonimach „Zapora" i „Tarcza". Sprawy te miały swoje odpowiedniki w terenie, które prowadziły Sekcje VI Wydziałów II Komend Wojewódzkich MO[14].

Celem sprawy obiektowej krypt. Zapora było kontrwywiadowcze zabezpieczenie obiektów wojskowych WP znajdujących się na terenie podległym WUSW. W jej ramach tego typu zabezpieczeniem obejmowano również jednostki wojskowe AR stacjonujące na terenie danego województwa. W prowadzonej sprawie praca operacyjna koncentrowała się m.in. na: (...) *rozbudowie sieci osobowych źródeł informacji* (...) *kontynuowaniu i prowadzeniu nowych działań ofensywnych w stosunku do służb przeciwnika w oparciu o sprawdzoną, pewną agenturę typowaną w takich działaniach* (...) *zacieśnianiu współpracy z Oddziałem Specjalnym przy Północnej Grupie Wojsk Armii Radzieckiej, zwłaszcza w zakresie przekazywania informacji naprowadzających na działalność szpiegowską, realizowaniu wspólnych przedsięwzięć w sprawach kombinacji operacyjnych (z udziałem agentury kontrwywiadu Armii Radzieckiej) oraz podejmowaniu wspólnych przedsięwzięć ofensywnych wobec wrogich ośrodków wywiadowczych* (...)[15].

---

[12] H. Marchel, *Kontrwywiadowcza ochrona obiektów wojskowych w latach 1980 - 1983 przed penetracją wywiadowczą przedstawicieli dyplomatycznych krajów kapitalistycznych akredytowanych w PRL na przykładzie woj. skierniewickiego*, praca dyplomowa, Legionowo 1985, WSO, Źródło: AIPN Ld, IPN Ld Pf 16/695, k. 105.

[13] *Informacja dotycząca organizacji kompleksowego systemu kontrwywiadowczego zabezpieczenia obiektów wojskowych przez Rejonowe Urzędy Spraw Wewnętrznych*. Źródło: AIPN Ld, IPN Ld 019/42, t. 3, k. 60 - 61.

[14] Sprawa obiektowa krypt. Zapora została zarejestrowana pod nr 33127 dn. 03.07.1972 r. przez Wydz. VI Dep. II MSW. Akta archiwalne nie zachowały się. Sprawa obiektowa krypt. Tarcza zarejestrowana została 18.05.1971 r. Źródło: Archiwum Instytutu Pamięci Narodowej [dalej: AIPN], IPN BU 01419/484, k. 7.

[15] H. Marchel, *Kontrwywiadowcza ochrona obiektów wojskowych w latach 1980 - 1983* ..., k. 19 - 21.

Sprawa obiektowa krypt. Tarcza została natomiast wszczęta w celu zewnętrznej operacyjnej ochrony jednostek i obiektów wojskowych AR[16]. Zakres współpracy z kontrwywiadem AR obejmował: ochronę obiektów radzieckich w miejscu postoju i w czasie przemarszu, wymianę informacji dotyczących obywateli polskich zatrudnionych w garnizonach AR bądź utrzymujących kontakty z ich personelem, organizację działań operacyjno-technicznych w zakresie ochrony kontrwywiadowczej[17].

Jednostki wojskowe AR pozostawały w czynnym zainteresowaniu personelu dyplomatycznego głównie Francji, Belgii, Wielkiej Brytanii, Niemiec i USA. O ilości podejmowanych działań rozpoznawczych ówczesnych państw kapitalistycznych może świadczyć fakt, że mimo początkowych ograniczeń wynikających z wprowadzenia w Polsce stanu wojennego, w roku 1982 stwierdzono 355 faktów penetracji obiektów jednostek wojskowych AR przez zachodnich dyplomatów. *Odbyte przez nich podróże miały charakter zorganizowany, obejmowały najczęściej kilka województw i trwały od jednego do paru dni. Działania te były planowane i koordynowane w ramach współdziałania rezydentur wywiadowczych uplasowanych w placówkach dyplomatycznych państw NATO. Cechami charakterystycznymi podróży penetracyjnych dyplomatów były: większa agresywność, nagminne nie respektowanie przepisów drogowych i poleceń funkcjonariuszy MO, zatrzymywanie się i postoje w strefach chronionych, fotografowanie obiektów wojskowych z wolno poruszających się pojazdów* (...)[18].

Według *Wytycznych w zakresie przedsięwzięć zmierzających do usprawnienia kontrwywiadowczego przeciwdziałania penetracjom obiektów WP i AR dokonywanym przez dyplomatów wojskowych krajów kapitalistycznych* Departamentu II MSW z dnia 22 czerwca 1983 r. uzyskane informacje dotyczące penetracji jednostek wojskowych AR Wydział VI Departamentu II przekazywał właściwemu Wydziałowi II KWMO, Stanowisku Kierowania Biurem „B”[19], Zarządowi III Szefostwa WSW[20] oraz, za pośrednictwem Wydziału II KWMO w Legnicy, kontrwywiadowi PGWAR w Legnicy – jeśli dotyczyły rejonów stacjonowania jednostek AR[21].

SB wykazywało szczególne zainteresowanie osobami zamieszkującymi w pobliżu garnizonów AR i wyjeżdżającymi czasowo na Zachód. Po uzyskaniu informacji z Wydziału Paszportów KWMO (a od 1983 r. WUSW), po złożeniu przez takie osoby

---

[16] *Kontrwywiadowcza charakterystyka do sprawy obiektowej „Tarcza” oraz główne kierunki pracy na odcinku operacyjnej ochrony obiektów Północnej Grupy Wojsk Armii Radzieckiej*. Sprawa obiektowa krypt. Tarcza. Źródło: AIPN, IPN BU 01419/484, k. 7.

[17] Informacja z dnia 14.09.1979 r. dotycząca współdziałania z Wydziałami Specjalnymi KGB w zakresie kontrwywiadowczej ochrony obiektów zlokalizowanych na terenie województwa szczecińskiego, chronionych w ramach sprawy obiektowej krypt. Tarcza. Sprawa obiektowa krypt. Tarcza. Źródło: AIPN Sz, IPN Sz0011/2074, t. 1, k. 105 - 110.

[18] *Informacja o aktualnym stanie rozpoznania zagrożenia wywiadowczego obiektów wojskowych WP i AR oraz główne kierunki działań* kontrwywiadowczych. Źródło: AIPN Ld, IPN Ld 019/42, t. 10, k. 84.

[19] Biuro „B” MSW zajmowało się obserwacją ludzi i miejsc. W 1983 r. Stanowisko Kierowania wchodziło w skład Wydz. XI Biura „B”, a od 1985 r., na skutek reorganizacji, funkcję kierowania wymienionym Biurem przejął Wydz. XV. Źródło: *Aparat bezpieczeństwa w Polsce. Kadra kierownicza, tom III 1975 - - 1990*, P. Piotrowski (red.), Warszawa 2008, IPN, s. 33 - 34; AIPN Ld, IPN Ld 019/42, t. 10, k. 139.

[20] Zarząd III Szefostwa Wojskowej Służby Wewnętrznej zajmował się kontrwywiadem i prowadzeniem ważniejszych rozpracowań operacyjnych oraz analizą. Źródło: B. Kapuściak, *Instrukcje pracy kontrwywiadowczej*..., s. 19.

[21] *Wytyczne w zakresie przedsięwzięć zmierzających do usprawnienia kontrwywiadowczego przeciwdziałania penetracjom obiektów WP i AR dokonywanym przez dyplomatów wojskowych krajów kapitalistycznych*. Źródło: AIPN Ld, IPN Ld 019/42, t. 10, k. 141.

wniosku na wyjazd za granicę, sprawdzano je pod kątem powiązań z osobami wojskowymi i cywilnymi zatrudnionymi w obiektach wojskowych. Z osobami, które uzyskały zgodę na wyjazd, każdorazowo przeprowadzano rozmowę operacyjną, w której trakcie starano się je wyczulić na działania podejmowane przez przedstawicieli obcego wywiadu.

Współpraca między SB a kontrwywiadem Armii Radzieckiej była szczególnie widoczna w podczas ćwiczeń wojskowych AR na poligonach lub przy zabezpieczaniu dróg przemarszu wojsk radzieckich. Dużą uwagę przywiązywano do osób zamieszkujących w pobliżu jednostki wojskowej AR w okresie trwania ćwiczeń wojskowych lub przegrupowania wojsk. W powyższej sytuacji każdorazowo uaktywniano kontrolę osób, wobec których prowadzono sprawy, zapewniano dopływ informacji o zachowaniu cudzoziemców przebywających w pobliżu jednostki wojskowej, zwiększano częstotliwość spotkań z tajnymi współpracownikami, wyczulając ich na osoby interesujące się jednostkami AR. Intensyfikowano pracę operacyjno-rozpoznawczą na terenie hoteli i punktów gastronomicznych zlokalizowanych w okolicach rosyjskich garnizonów. Organizowano punkty zakryte w celu podjęcia obserwacji jednostki wojskowej, dróg dojazdowych do niej oraz osób i pojazdów wykazujących zainteresowanie daną jednostką. Przez cały czas Wydziały II ściśle współpracowały z oficerami kontrwywiadu AR oraz z funkcjonariuszami ruchu drogowego MO i ORMO. Po zakończonych ćwiczeniach wojskowych na poligonie czy po przegrupowaniu wojska Wydziały II przeprowadzały analizę zebranych materiałów i informację w formie meldunku operacyjnego przesyłały do Wydziału VI Departamentu II MSW. Osoby, które przejawiały zainteresowanie ruchami wojsk radzieckich, na bieżąco poddawano kontroli operacyjnej w ramach prowadzonych spraw operacyjnych.

W latach 1985 - 1988 na podstawie uzyskanych informacji agenturalnych została wszczęta przez RUSW w Białogardzie sprawa krypt. Lokator, której figurantka Genowefa Machała była podejrzana o wywiadowcze zainteresowanie jednostkami AR w tym mieście. Machała była zatrudniona w Rejonie Dróg Publicznych w Białogardzie, skąd miała widok na jednostkę AR, a ponadto wyjeżdżała do swojej siostry mieszkającej w RFN. W sprawie tej współdziałano z oficerem kontrwywiadu AR mjr. Byczkowskim, który miał ustalić, czy i ewentualnie jakie kontakty figurantka utrzymywała z personelem jednostki. Przeprowadzono kombinację operacyjną polegającą na zacieśnieniu kontaktów agentki KGB ps. Alesia z figurantką (obie znały się wcześniej). „Alesia" wystąpiła pod legendą osoby oferującej rosyjskie konserwy mięsne i wyroby czekoladowe. Agentka dążyła do częstych kontaktów z Machałą, odwiedzała ją w domu, jednak Machała nie przejawiała zainteresowań jednostkami AR o charakterze wywiadowczym. Prowokowane przez agentkę rozmowy na tematy wojskowe i polityczne spowodowały, że figurantka zaczęła jej unikać. W związku z tym sprawę zakończono[22].

Współpraca między kontrwywiadem wojskowym AR i WUSW polegała także na przesyłaniu informacji dotyczących kradzieży dokonywanych na terenie jednostki wojskowej AR lub poszukiwaniu zbiegłych żołnierzy wojska radzieckiego. Należy tu nadmienić, że zasady postępowania WUSW przy zatrzymywaniu żołnierzy radzieckich lub członków ich rodzin regulowały osobne przepisy, z których wynikało, że żołnierze AR mogli być zatrzymywani tylko w przypadku niezbędnej konieczności. Żołnierza ra-

[22] A IPN Sz, IPN Sz 00105355/DVD.

dzieckiego nie można było na przykład doprowadzać do izby wytrzeźwień. Jeśli dochodziło do osadzenia go w areszcie, należało go umieścić w oddzielnym pomieszczeniu[23]. Ochrona jednostek AR stacjonujących na terenie PRL była tak ważnym zagadnieniem, że oprócz cyklicznych comiesięcznych odpraw w tej sprawie odbywały się również krajowe narady poświęcone współpracy z radzieckim kontrwywiadem. Uczestniczyło w nich kierownictwo Departamentu II MSW, kierownictwo kontrwywiadu PGWAR wraz z oficerami tej służby oraz przedstawiciele KGB. Wypracowane na naradach kierunki współpracy przekazywane były w formie wytycznych do poszczególnych województw. W maju 1982 r. w Legnicy zorganizowana została narada krajowa poświęcona współpracy z kontrwywiadem AR, której przewodniczył Dyrektor Departamentu II MSW gen. bryg. Z. Sarewicz. Wzięli w niej udział przedstawiciele KGB oraz kierownictwo kontrwywiadu PGWAR wraz z oficerami tej służby[24]. Wypracowane tu kierunki współpracy również przekazano w formie wytycznych do zainteresowanych województw[25].

W maju 1985 r. w Warszawie odbyło się spotkanie dotyczące operacyjnej ochrony jednostek wojskowych AR. Jej uczestnikami byli: wiceminister spraw wewnętrznych gen. dyw. Władysław Pożoga, kierownictwo Departamentu II MSW, 16 zastępców szefów WUSW ds. SB (z 15 województw, w których stacjonowały jednostki AR oraz ze Słupska – w województwie tym Armia Radziecka korzystała z portu w Ustce oraz z lotniska i poligonu wojskowego), przedstawiciele Szefostwa Wojewódzkich Spraw Wewnętrznych, przedstawiciele KGB ZSRR do stałych kontaktów z MSW PRL oraz przedstawiciele kontrwywiadu AR z Legnicy i Świdnicy. Celem tej narady miało być: dokonanie oceny stanu zagrożenia wywiadowczego ochranianych jednostek AR, omówienie zainteresowań kierunkami i metodami działalności wrogich wywiadów wobec jednostek AR oraz doskonalenie form i metod działalności SB w operacyjnym zabezpieczaniu jednostek AR[26].

Współpraca transgraniczna

W Polskiej Rzeczpospolitej Ludowej i Związku Radzieckim ochroną granic zajmowały się Wojska Ochrony Pogranicza (dalej: WOP). WOP ZSRR wchodził w skład KGB i był samodzielnym Zarządem. Departament WOP PRL utworzono 27.05.1945 r. Podlegał on Ministerstwu Obrony Narodowej. W 1948 r. na bazie Departamentu WOP utworzono Główny Inspektorat Ochrony Pogranicza (dalej: GIOP). Z dniem 1 stycznia 1949 r. GIOP podporządkowano Ministerstwu Bezpieczeństwa Publicznego, a rok później jednostkę tę przeformowano w Dowództwo WOP. W 1952 r. WOP podlegał

[23] *Zarządzenie nr 9/80 Ministra Spraw Wewnętrznych z dnia 13 marca 1980 r. Postępowanie Milicji Obywatelskiej w razie popełnienia przestępstw lub wykroczeń przez osoby wchodzące w skład wojsk radzieckich czasowo stacjonujących w Polsce lub członków ich rodzin*. Źródło: AIPN Ld, IPN Ld253/2, k. 8.

[24] *Informacja o aktualnym stanie rozpoznania zagrożenia wywiadowczego obiektów wojskowych WP i AR oraz główne kierunki działań* kontrwywiadowczych. Źródło: AIPN Ld, IPN Ld019/42, t. 10, k. 78.

[25] Zalecenia Dyrektora Departamentu II zawarto w piśmie nr ODT-12/090/82 z dnia 16 czerwca 1982 r. dotyczącym narady krajowej w Legnicy w dniu 25 maja 1982 r. (do 15 Wydziałów II, na terenie których stacjonują jednostki AR). Informacja zaczerpnięta z *Wytycznych w zakresie przedsięwzięć zmierzających do usprawnienia kontrwywiadowczego przeciwdziałania penetracjom obiektów WP i AR dokonywanym przez dyplomatów wojskowych krajów kapitalistycznych*, tamże, k. 137.

[26] Projekt programu narady na temat operacyjnej ochrony jednostek wojskowych AR. Źródło: AIPN, IPN BU 01153/1, k. 3 - 5.

dowódcy wojsk wewnętrznych, gen. bryg. Juliuszowi Hibnerowi. Od 1971 r., aż do rozformowania w 1991 r., WOP podlegał Ministerstwu Spraw Wewnętrznych. W 1990 r. Dowództwu WOP podlegało 7 Brygad (Karpacka, Górnośląska, Łużycka, Pomorska, Kaszubska, Podlasko-Mazurska i Bieszczadzka), Batalion Sudecki, Oddział Bałtycki, Graniczna Placówka Kontrolna na Okęciu oraz 3 ośrodki szkolenia[27].

Współpraca transgraniczna SB i KGB polegała na wymianie informacji o: dążeniach, formach i metodach działalności dywersyjnej służb specjalnych krajów zachodnich na płaszczyźnie komunikacji międzynarodowej; konkretnych osobach, firmach i organizacjach wykorzystywanych przez przeciwnika do prowadzenia działalności dywersyjnej przeciwko PRL i ZSRR; sytuacji operacyjnej w miejscach pracy za granicą pracowników transportu obydwu krajów, w tym w organizacjach międzynarodowych (np. w Międzynarodowej Organizacji Lotnictwa Cywilnego – ICAO, Międzynarodowym Związku Kolei i Międzynarodowym Związku Transportu Samochodowego); przygotowywanych akcjach dywersyjnych przeciwko zagranicznym przedstawicielstwom transportowym PRL i ZSRR; interesujących z operacyjnego punktu widzenia marynarzach państw NATO odwiedzających porty PRL i ZSRR, a także o cudzoziemcach przebywających w zagranicznych portach, którzy prowadzili wrogą działalność przeciwko polskim i radzieckim marynarzom oraz o faktach nieprzestrzegania norm zachowania się przez pracowników polskiego transportu na terytorium ZSRR i radzieckiego w Polsce[28].

W październiku 1970 r. KGB planowało przeprowadzić wspólnie z SB przedsięwzięcia operacyjne. Strona polska miała wprowadzić w skład załogi jednego ze statków PRL („Boruta" lub „Rokita") kursujących na trasie Kłajpeda–Francja doświadczonego tajnego współpracownika, który miał przechwycić w portach RFN kontakty z właścicielami miejscowych sklepów obsługujących przemytników, co do których istniały podejrzenia o ich powiązania ze służbami specjalnymi państw zachodnich. Tajny współpracownik SB miał kupować u tych handlarzy towary, a następnie wwozić je do Kłajpedy. W charakterze skupującego artykuły przemytnicze miał być podstawiony agent KGB ps. Bałtia – Rosjanin pochodzenia niemieckiego, muzyk orkiestry wojskowej posiadający dalszych krewnych w RFN i Anglii. Tajny współpracownik SB i agent KGB działaliby jako wspólnicy – przemytnicy. Przemycone towary „Bałtia" miał sprzedawać pracownikowi operacyjnemu KGB. Strona radziecka przypuszczała, że wspomniany kanał przemytu znajdzie się w zainteresowaniu zachodnich służb specjalnych i pojawią się możliwości wykorzystania go w celach kontrwywiadowczych[29].

Obie służby wspólnie realizowały również zadania mające na celu ujawnianie i przerywanie działalności wywiadowczej dyplomatów – pracowników zachodnich wywiadów – podczas ich podróży tranzytowych koleją przez terytoria PRL i ZSRR oraz wykrywanie kanałów przemytu, które przeciwnicy wykorzystywali w działalności dywersyjnej.

---

[27] Z. Jackiewicz, *Wojska Ochrony Pogranicza 1945 - 1991: krótki informator historyczny*, Kętrzyn 1998, Centrum Szkolenia Straży Granicznej, s. 7 - 31.

[28] Plan rozwoju współpracy pomiędzy Departamentem II MSW PRL i IV Zarządem KGB ZSRR na lata 1984 - 1986 zatwierdzony przez ministra spraw wewnętrznych PRL Czesława Kiszczaka i Przewodniczącego KGB ZSRR Wiktora Czebrikowa. Źródło: AIPN, IPN BU0-654/4, k. 1 - 4.

[29] Wymiana korespondencji pomiędzy Departamentem II MSW i KGB ZSRR w 1970 r. Źródło: AIPN, IPN BU 01062/42, t. 38, k. 126 - 128.

W czerwcu 1973 r. KGB planowało przeprowadzić przy pomocy SB przedsięwzięcia dotyczące cudzoziemców, w tym również dyplomatów podróżujących po terytorium ZSRR pociągiem nr 25/26 relacji Warszawa–Bukareszt (i dalej do Warny). Pociąg ten, zgodnie z porozumieniem między ZSRR, PRL i Ludową Republiką Bułgarii, kursował codziennie. W jego skład wchodziły 3 wagony polskie i 7 radzieckich. KGB proponowała stronie polskiej regularną wymianę informacji odnośnie do cudzoziemców, co do których zostaną uzyskane dane o ich przynależności do służb specjalnych, (...) *a także o podjęciu wobec osób w pociągu, w razie konieczności, wspólnych kroków kontrwywiadowczych*. Wymiana informacji miała następować poprzez naczelników rejonowych wydziałów KGB obwodu lwowskiego i przemyskiego oraz Wydziałów II KWMO, telefonicznie lub na spotkaniach osobistych. Na jednym z takich spotkań, we wrześniu 1974 r., uzgodniono, że polscy konduktorzy pociągu nr 25/26, przejeżdżając przez terytorium ZSRR *będą swoje spostrzeżenia dot. pasażerów z kk przekazywać ustnie radzieckiemu kierownikowi pociągu, bądź oficerom służby granicznej ZSRR*. W działaniach miały być wykorzystywane źródła informacji uplasowane w brygadach konduktorskich, a także środki techniki operacyjnej[30].

Koordynowano również przedsięwzięcia dotyczące ochrony tajemnicy i zapewnienia bezpieczeństwa transportów wojskowych w punktach przekraczania granicy państwowej. KGB werbowało do współpracy Polaków, którzy byli zatrudnieni jako pracownicy PKP. Służbę tę interesowały zagadnienia dotyczące m.in. pracowników PKP posiadających dostęp do tajemnicy państwowej i służbowej, osób, z którymi kontaktowali się Rosjanie oraz bezpieczeństwa transportów kolejowych Armii Radzieckiej, w tym okresy i przyczyny postojów.

W trakcie współpracy transgranicznej SB i KGB realizowały przedsięwzięcia w zakresie ujawniania i rozpracowywania pracowników wywiadów państw zachodnich i ich agentów działających pod przykryciem międzynarodowych organizacji transportu i łączności, m.in. Komitetu do spraw Transportu Wewnętrznego Europejskiej Komisji Gospodarczej ONZ, Komitetu Technicznego do spraw Kontenerów, Światowego Związku Pracowników Poczt, firm transportowo-spedycyjnych i morskich m.in. „Maarchshiping" (Kanada), „Frantex" oraz „Helmsing" (RFN)[31].

W 1978 r. KGB planowała podjąć wspólnie z SB działania operacyjne wobec Janusza Łazara, pracownika francuskiej firmy spedycyjno-transportowej „Eteks", utrzymującego kontakty z radziecką firmą „Sovtransavto". J. Łazar okresowo odwiedzał swoich krewnych w PRL. Wspólne działania służb miały doprowadzić do ujawnienia i zdemaskowania współpracy wyżej wymienionego ze służbami specjalnymi Francji[32].

[30] Wymiana korespondencji pomiędzy Departamentem II MSW i KGB ZSRR w 1973 r. Źródło: AIPN, IPN BU 01062/42, t. 48, k. 38 - 45. W materiałach źródłowych brak jest informacji, czy porozumienie dotyczące pociągu nr 25/26 obejmowało również Rumunię.

[31] *Plan rozwoju współpracy pomiędzy Departamentem II MSW PRL i II Głównym Zarządem KGB ZSRR na lata 1978 - 1981* zatwierdzony przez ministra spraw wewnętrznych PRL Stanisława Kowalczyka i Przewodniczącego KGB ZSRR Jurija Andropowa. Źródło: AIPN, 0-654/2, k. 9 - 10.

[32] Wykaz przedsięwzięć operacyjno-agenturalnych dotyczących figurantów pozostających we wspólnym zainteresowaniu Departamentu II MSW PRL i II Głównego Zarządu KGB ZSRR, które były zaplanowane na lata 1978 - 1981, podpisany przez Dyrektora Departamentu II MSW PRL gen. bryg. Władysława Pożogę oraz Szefa II Głównego Zarządu KGB ZSRR gen. dyw. G. F. Grigorienkę. Źródło: AIPN, 0-654/2, k. 27.

Rozpracowywano zarówno pracowników stałych przedstawicielstw zachodnich towarzystw morskich w PRL i ZSRR podejrzanych o przynależność do służb specjalnych, jak również pracowników wywiadu i agentów spośród załóg statków przypływających do obu krajów. W 1978 r. zorganizowano wspólne kompleksowe przedsięwzięcia operacyjno-agenturalne zmierzające do ujawnienia i udokumentowania wrogiej działalności zachodnioniemieckich marynarzy o nazwisku Szulce i Timman ze statku „Helmsing" oraz członków załóg zachodnioniemieckiego armatora „Kargo Liner", którzy w polskich i radzieckich portach zajmowali się zbieraniem informacji wywiadowczych[33].

W latach 1978 - 81 KGB i SB rozpoczęły rozpracowanie właścicieli sklepów „Neptun", „Misca", „Syrena", „Wenus", „Baltoni import-export" i „Gryf" w Kopenhadze, należących do byłych obywateli polskich, którzy wciągali marynarzy polskich i radzieckich w przemyt. Do rozpracowania miała być wykorzystana agentura ulokowana w załogach polskich i radzieckich statków, regularnie zawijających do portu w Kopenhadze[34].

Podczas realizowanych działań baczną uwagę zwracano na interesujących z operacyjnego punktu widzenia marynarzy państw NATO odwiedzających porty PRL i ZSRR, a także na przebywających w zagranicznych portach cudzoziemców, którzy prowadzili wrogą działalność przeciwko polskim i radzieckim marynarzom.

W 1984 r. wspólnie rozpracowywano Rudolfa Schepersa, obywatela RFN, który był II. nawigatorem zachodnioniemieckiego statku „Bremer Horst Bishopp". W czasie pobytów w polskich i radzieckich portach Schepers fotografował radzieckie okręty wojenne i urządzenia portowe[35].

W tym samym roku sojusznicze służby wspólnie przeprowadziły ofensywne przedsięwzięcia operacyjne wobec obywatela RFN o nazwisku Kölne, kadrowego pracownika zachodnioniemieckich służb wywiadowczych, który pracował pod przykryciem w Urzędzie Morskim i ds. Żeglugi w Hamburgu (instytucji wykorzystywanej przez wywiad RFN). Prowadzone działania miały na celu głębsze rozpoznanie stopnia zagrożenia ze strony Kölne i jego współpracowników[36].

W celu sprawniejszej i efektywniejszej współpracy służb konieczne było, o czym wspomiano wyżej, organizowanie spotkań ich przedstawicieli. W kwietniu 1976 r. planowano odbyć robocze spotkanie przedstawicieli KGB i szczecińskiej SB poświęcone omówieniu aktualnej sytuacji operacyjno-politycznej w zakresie kontrwywiadowczego zabezpieczenia międzynarodowego transportu morskiego oraz dalszych wspólnych działań operacyjnych w tym obszarze. O tych planach Dyrektor Departamentu II MSW gen. W. Pożoga poinformował Zastępcę Komendanta Wojewódzkiego MO ds. SB w Szczecinie płk. Z. Baranowskiego. Przygotowując spotkanie, gen. Pożoga powoływał się na plan współpracy między KGB i Departamentem II oraz na uzgodnienia zawarte na spotkaniu w Wilnie we wrześniu 1972 r. (spotkanie to było wspólną konferencją przedstawicieli KGB Litewskiej SSR, MSW PRL i MBP NRD). W szczecińskim spotkaniu udział wzięli: z ramienia KGB – naczelnik Wydziału Morskiego II Zarządu Głównego

[33] Tamże, k. 27 - 28.
[34] Tamże, k. 28.
[35] Wykaz przedsięwzięć dotyczących obiektów wzajemnego zainteresowania Departamentu II MSW PRL i IV Zarządu KGB ZSRR na lata 1984 - 1986. Źródło: AIPN, IPN BU 0-654/4, k. 7.
[36] Tamże, k. 10

KGB ZSRR płk Aleksander Iwanowicz Archipow, naczelnik Zarządu II KGB Litwy płk Antonas Ignatowicz Naras, naczelnik Kłajpedzkiego Wydziału Miejskiego KGB Litwy ppłk Anzelmas Jonowicz Armonas i zastępca naczelnika pionu II KGB Obwodu Leningradzkiego mjr Albert Fiedorowicz Starodubcew. Z ramienia polskiej SB natomiast – płk A. Pudło z Grupy „Wisła" w Leningradzie[37].

Rozpracowywanie i przeciwdziałanie aktywności zachodnich służb specjalnych

Na podstawie analizowanych materiałów źródłowych można wysunąć tezę, że działania podejmowane w latach 1970 - 1990 przez służby specjalne państw zachodnich w stosunku do krajów bloku wschodniego przyczyniły się do zacieśniania współpracy między SB i KGB w zakresie przeciwdziałania i zwalczania aktywności tych służb. Celem wspólnie prowadzonych przedsięwzięć operacyjnych było ujawnianie i rozpracowywanie pracowników wywiadów państw zachodnich prowadzących działalność agenturalną, m.in. dyplomatów, dziennikarzy i handlowców, wykrywanie realizowanych przez nich operacji agenturalnych na terenie PRL i ZSRR oraz realizacja wspólnych przedsięwzięć w zakresie kontroli zachowywania się i działań pracowników służb specjalnych krajów kapitalistycznych w czasie ich podróży z PRL do ZSRR i odwrotnie. Wspólnie organizowano gry kontrwywiadowcze ze służbami specjalnymi państw zachodnich. Zbierano informacje o pracownikach dyplomatycznych tych państw, akredytowanych w PRL i ZSRR, o ich zachowaniu i działalności przed przyjazdem do obu krajów i w czasie przebywania w nich oraz ujawniano ich kontakty z ustalonymi pracownikami wywiadów. Sprawdzano również i rozpracowywano (zgodnie z wzajemnymi prośbami) niektórych obywateli PRL i ZSRR, szczególnie podejrzanych o współpracę z zachodnimi służbami specjalnymi. Wymieniano się także informacjami na temat podejrzanych kontaktów polskich i radzieckich obywateli z pracownikami przedstawicielstw państw zachodnich. Wzajemne możliwości wykorzystywano ponadto do tworzenia warunków operacyjno-technicznego docierania do przedstawicielstw państw zachodnich w PRL i ZSRR oraz do ich rezydentur działających pod przykryciem tych przedstawicielstw (przy zaangażowaniu w miarę potrzeby specjalistów SB i KGB, dzięki którym próbowano uzyskiwać dane o systemach zabezpieczeń wyżej wymienionych placówek, z uwzględnieniem wszelkich wprowadzonych zmian, oraz informacje o aktualnych środkach łączności wywiadowczej stosowanych przez rezydentury placówkowe w ambasadach i konsulatach).

Dużą uwagę przywiązywano do ochrony tajemnicy dotyczącej problematyki politycznej, gospodarczej, wojskowej oraz naukowo-technicznej PRL i ZSRR. W związku z tym sprawdzano i rozpracowywano osoby zatrudnione w przedstawicielstwach banków, firm handlowych, turystycznych i innych w PRL i ZSRR, wobec których nie było danych o ich przynależności do służb specjalnych, a którzy wykorzystywali oficjalne kontakty z polskimi i radzieckimi instytucjami do zbierania informacji szpiegowskich na tematy handlowe, gospodarcze i inne. Ujawniano zagraniczne firmy handlowe, gospodarcze i turystyczne wykorzystywane przez zachodnie służby spe-

[37] Pismo z 12.04.1976 r. adresowane do Zastępcy Komendanta Wojewódzkiego MO ds. SB płk. Z. Baranowskiego i podpisane przez Dyrektora Dep. II MSW gen. bryg. W. Pożogę. W piśmie brak jednak bliższych danych dotyczących spotkania w Wilnie. Źródło: AIPN Sz, IPN Sz 0011/2114.

cjalne w charakterze instytucji przykrycia do działań szpiegowskich przeciwko PRL i ZSRR, które to utrzymywały kontakty z odpowiednimi instytucjami polskimi i radzieckimi. Zapewniano „ochronę" obywateli PRL i ZSRR na międzynarodowych targach, wystawach, konferencjach naukowych oraz wymieniano się informacjami operacyjnymi o przygotowywanych przez zachodnie wywiady wrogich działaniach przeciwko obywatelom obu krajów.

Przedsięwzięcia ofensywne realizowane przez SB i KGB polegały m.in. na tworzeniu warunków zmuszających pracowników rezydentur do działania w okolicznościach kontrolowanych przez jednostki kontrwywiadu PRL i ZSRR. Celem było ewentualne zatrzymanie ich z dowodami winy, przejęcie materiałów szpiegowskich, a także przygotowywanie i realizacja wspólnych przedsięwzięć zmierzających do demaskowania i kompromitacji służb specjalnych krajów demokracji zachodniej.

W 1971 r. KGB przeprowadzało na terenie PRL przedsięwzięcie operacyjne polegające na podesłaniu wywiadowi amerykańskiemu swoich agentów – małżeństwa Katkiewiczów, pracowników Instytutu Chemii Drewna Akademii Nauk Łotewskiej SRR. Katkiewiczowie mieli odwiedzić Warszawę na zaproszenie Zbigniewa Laurowa, pracownika Katedry Użytkowania Lasu. Agenci KGB (…) *przy pomocy Laurowa, lub bez niego, zależnie od okoliczności, odwiedzą „ośrodek kultury" przy ambasadzie USA, gdzie nawiążą kontakt z którymś z pracowników ośrodka, poprzez którego następnie spróbują nawiązać kontakt z przedstawicielem generalnego konsulatu lub ambasady USA*. SB miało udzielić im pomocy, a także sprawdzić Zbigniewa Laurowa. W materiałach źródłowych brak jednak informacji o dalszych przedsięwzięciach realizowanych w tej sprawie[38].

Sprawdzano i rozpracowywano, zgodnie z wzajemnymi prośbami, niektórych obywateli PRL i ZSRR podejrzewanych o kontakty ze służbami specjalnymi państw zachodnich, a także wymieniano się informacjami o podejrzanych kontaktach polskich i radzieckich obywateli z ustalonymi pracownikami przedstawicielstw tych państw.

W celu wykrycia działalności agenturalnej pracowników rezydentur zachodnich wywiadów występujących pod przykryciem, a także ich stałych przedstawicielstw w ZSRR i PRL, przeprowadzano liczne przedsięwzięcia operacyjne polegające m.in. na podsyłaniu im tajnych współpracowników SB i agentów KGB oraz organizowaniu wspólnych gier kontrwywiadowczych. Przykładem takich działań może być wspólne rozpracowywanie Alfreda Blumenfelda.

W 1972 r. Blumenfeld przebywał w Leningradzie jako konsul generalny RFN. Wcześniej był I. sekretarzem ambasady RFN w ZSRR, a w latach 1963 - 1966 zastępcą Szefa Przedstawicielstwa Handlowego RFN w Warszawie. Od 1963 r. w działaniach przeciwko niemu wykorzystywany był tajny współpracownik SB ps. Andrzej. Wspólna operacja SB i KGB polegała na podstawieniu Blumenfeldowi poprzez „Andrzeja" (do werbunku dla niemieckiego wywiadu) agenta KGB ps. Lwow, wywodzącego się spośród radzieckich dziennikarzy. W związku z tym, na prośbę KGB do Moskwy udali się „Andrzej" oraz jego oficer prowadzący – ppłk. A. Karpa, w celu zapoznania się z tym agentem. W 1973 r. KGB informowała SB, że jest zainteresowana dalszym rozwojem kontaktów „Andrzeja" z Blumnefeldem. W następnych miesiącach z kolei

[38] Wymiana korespondencji pomiędzy Departamentem II MSW a KGB ZSRR w 1971 r. Źródło: AIPN, IPN BU 01062/42, t. 36, k. 252 - 253.

SB informowała KGB o spotkaniach mężczyzn. W materiałach źródłowych brak jednak szerszych informacji na ten temat[39].

Ponadto SB i KGB wykorzystywały obywateli ZSRR przebywających na terenie Polski do działań ofensywnych zmierzających do zarekomendowania ich wywiadowi brytyjskiemu za pośrednictwem British Council (instytucja reprezentująca Zjednoczone Królestwo Wielkiej Brytanii i Irlandii Północnej w zakresie współpracy kulturalnej i edukacyjnej). W 1972 r. przeprowadzono wspólną kombinację operacyjną mającą na celu wprowadzenie do British Council agenta KGB ps. Ludmiła za pośrednictwem tajnego współpracownika SB ps. Tulipan. „Ludmiła" była żoną oficera AR i nauczycielką w szkole średniej. W trakcie przeprowadzenia kombinacji dochodziło do bezpośrednich kontaktów Naczelnika Wydziału II w Łodzi kpt. Kazimierza Pjanki („Tulipan" był prowadzony przez ten Wydział) z oficerem operacyjnym KGB Szarowem[40].

W październiku 1973 r. po raz pierwszy odbył się w Związku Radzieckim XXIV Kongres Międzynarodowej Federacji Astronautycznej, na który przybyło około 1500 przedstawicieli światowej nauki i przemysłu. Strona radziecka posiadała materiały operacyjne dotyczące dość licznej grupy osób biorących udział w takich kongresach i jednocześnie realizujących przedsięwzięcia operacyjno-agenturalne[41].

Miesiąc wcześniej (we wrześniu) w Warszawie obradowało Zgromadzenie Generalne Międzynarodowego Towarzystwa Astronomicznego. W związku z tym KGB delegowało na ten okres swoich pracowników operacyjnych do realizacji przedsięwzięć kontrwywiadowczych dotyczących członków delegacji tego Zgromadzenia. Niektóre z przedsięwzięć planowane były wspólnie przez SB i KGB[42].

KGB posiadało agenturę i osoby zaufane, które włączane były w skład delegacji udających się na różnego rodzaju konferencje, m.in. na konferencje Światowego Stowarzyszenia Geofizyków, Światowej Organizacji Meteorologów, Amerykańskiego Instytutu Aeronautyki i Astronautyki oraz Amerykańskiego Stowarzyszenia Lekarzy. W tego typu konferencjach uczestniczyli również polscy naukowcy, dlatego KGB proponowało SB wspólne przedsięwzięcia: (…) *w niektórych wypadkach istnieje możliwość realizacji uzgodnionych posunięć operacyjno-agenturalnych i dokonywania wymiany informacji operacyjnych*[43].

Oprócz wyżej wymienionych przedsięwzięć prowadzonych w stosunku do naukowców, KGB „zabezpieczało" obywateli ZSRR na międzynarodowych targach i wystawach, wysyłając razem z delegacją swoich pracowników. Przykładem może być XV doroczna sesja Komitetu Badań Kosmosu, która odbyła się w RFN. W składzie radzieckiej delegacji na tę sesję miał znajdować się oficer KGB[44].

---

[39] Wymiana korespondencji pomiędzy Departamentem II MSW i KGB ZSRR w latach 1970 - 1973 r. Źródło: AIPN, IPN BU 01062/42, t. 40, k. 141 - 197.

[40] Brak szczegółowych informacji dotyczących kombinacji prowadzonej przeciwko British Council. Źródło: AIPN, IPN BU 01062/42, t. 41, k. 67 - 74.

[41] Wymiana korespondencji pomiędzy Departamentem II MSW i KGB ZSRR w latach 1970 - 1973 r. Źródło: AIPN, IPN BU 01062/42, t. 48, k. 256. Brak szczegółowych informacji dotyczących prowadzonych przedsięwzięć operacyjno-agenturalnych.

[42] Tamże, k. 256. W materiałach brak szczegółów odnośnie do przedsięwzięć operacyjnych dotyczących Zgromadzenia Towarzystwa Astronomicznego.

[43] Tamże, k. 257.

[44] Tamże.

W 1977 r. SB podjęła działania wobec Artura Smitha, radcy ekonomicznego ambasady USA w Warszawie, który w latach 1973 - 1975 przebywał w ambasadzie USA w Moskwie. W czasie pobytu w ZSRR Smith był rozpracowywany przez KGB przy pomocy agenta ps. Ekonomista. W celu kontynuacji tych działań w listopadzie 1978 r. w Warszawie wraz z „Ekonomistą" przebywał oficer KGB. Z tym ostatnim Smith utrzymywał zażyłe kontakty podczas swojego pobytu w Moskwie. Polegały one głównie na (…) *wzajemnych sondażach i przekazywaniu określonych informacji wyprzedzających*. Założeniem kombinacji służb specjalnych było zorientowanie się, czy Smith podejmie ponowny kontakt z „Ekonomistą". W wyniku uzgodnień kierownictwa Wydziału I Departamentu II MSW odbytych w obecności płk. W. Kazmina, prawdopodobnie oficera KGB, postanowiono, że agent skontaktuje się z Amerykaninem w czasie jego pobytu w Warszawie. Gdy do spotkania doszło, Smith scharakteryzował swój pobyt w Polsce oraz zainteresowania wydziału ekonomicznego ambasady USA.

W 1979 r. doszło do jeszcze dwóch spotkań agenta KGB z Arturem Smithem na terenie Polski, podczas których Departament II MSW przeprowadzał czynności kontrolne wobec tego ostatniego. W tym celu SB wykorzystywała tajnych współpracowników ps. Maryla, ps. Continental oraz ps. Tom, którzy dostarczali informacji o kontaktach Amerykanina, jego wyjazdach w teren oraz zainteresowaniach handlowych.

Dużą uwagę w realizowanych samodzielnie lub wspólnie przez obie służby przedsięwzięciach zwracano na ujawnianie i rozpracowywanie pracowników wywiadów państw zachodnich, prowadzących działalność agenturalną wśród przebywających w PRL i ZSRR zagranicznych dziennikarzy zatrudnionych w agencjach prasowych i radiowo-telewizyjnych.

W 1978 r. realizowano wspólne przedsięwzięcia dotyczące rozpracowania Bekherna Ebekharta, korespondenta DPA w Moskwie, podejrzewanego o przynależność do BND. W działaniach tych miała być wykorzystana agentura SB i agentura Grupy „Wisła" w Moskwie[45]. W tym samym roku podjęto działania wobec G. M., które miały być ukierunkowane na ujawnienie faktów świadczących o jego działalności wywiadowczej.

M. urodził się we Francji. W 1954 r. przyjechał wraz z matką do Polski (matka pochodziła z Polski; została wydalona z Francji za przynależność do Francuskiej Partii Komunistycznej). W 1969 r. M. został pozyskany do współpracy z Departamentu II MSW jako TW ps. Radek. W tym samym roku wyjechał na stałe do Francji. W związku z jego wyjazdem za granicę materiały dotyczące jego osoby zostały przekazane do Departamentu I MSW (wywiad cywilny).

M. jednak niechętnie odnosił się do spotkań z funkcjonariuszami, a w 1975 r. odmówił z nimi współpracy. W tym samym roku wyjechał do Moskwy; tu objął stanowisko stałego korespondenta radia francuskiego. W 1975 r. Departament I MSW przesłał do KGB informacje na jego temat oraz wystosował prośbę o pomoc w jego ponownym pozyskaniu do współpracy. W 1977 r. KGB zainteresowało się wspólnym rozpracowaniem M. W materiałach brak jednak informacji o prowadzonych przez SB i KGB działaniach operacyjnych w tej sprawie w latach 1978 - 1980. W aktach znajdujesię jedynie

[45] Wykaz przedsięwzięć operacyjno-agenturalnych wobec figurantów pozostających we wspólnym zainteresowaniu Departamentu II MSW PRL i II Głównego Zarządu KGB ZSRR, jakie były zaplanowane na lata 1978 - 1981, podpisany przez Dyrektora Departamentu II MSW PRL gen. bryg. Władysława Pożogę oraz Szefa II Głównego Zarządu KGB ZSRR gen. dyw. G. F. Grigorienkę. Źródło: AIPN, IPN BU 0-654/2, k. 24 - 25.

zapis z 1980 r. (…) *antypolskie nastawienie i powiązanie z opozycją* (...) *sytuacja taka nie stwarza możliwości pozyskania go do współpracy z nami*[46].

W 1987 r. Wydz. II WUSW w Szczecinie postanowił podjąć działania wobec placówki CIA uplasowanej w ambasadzie USA w Bonn. W tym celu wykorzystano tajnego współpracownika SB ps. A-1, który od 1986 r. wyjeżdżał do RFN do żony i syna. Celem planowanych operacji ofensywnych było zainspirowanie służb USA do werbunku A-1, rozpoznanie form i metod działania tych służb oraz zakresu ich zainteresowania personelem radzieckich obiektów wojskowych na terenie województwa szczecińskiego. Plan działań ofensywnych wobec służb USA zakładał udanie się „A-1" do ambasady USA w Bonn, gdzie miał opowiedzieć o zwerbowaniu go przez oficera AR, który zlecał mu obserwację dyplomatów USA w czasie ich pobytów w szczecińskim hotelu „Neptun" oraz zapamiętywanie obiektów militarnych w RFN. Jako motyw działania „A-1" miał przedstawić niechęć do Rosjan związaną z wydarzeniami historycznymi oraz oszukaniem go przez Rosjanina, z którym zamierzał prowadzić działalność handlową. Kombinację realizowano wspólnie z Wydziałem Specjalnym KGB w Kluczewie. „A-1" nawiązywał kontakt z agentem KGB, zostawiając list w jednostce AR w Szczecinie. Kontakt w drugą stronę nawiązywany był za pomocą kartki pocztowej.

Agentem KGB był Michaił Nikołajewicz Woronkiewicz (lub Woroncow), w wieku około 40 lat. Absolwent Charkowskiego Instytutu Lotniczego. Do jego zadań służbowych należało m.in. wizytowanie jednostek AR. Powyższe informacje dotyczące działalności Rosjanina „A-1" miał przekazać służbom USA. W czasie przeprowadzania kombinacji doszło do kilku bezpośrednich kontaktów „A-1" z ambasadą USA w Bonn oraz do kilku kontaktów telefonicznych. Początkowo dyplomaci USA zlecali podstawionemu agentowi wykonywanie poleceń KGB i informowanie o tym ambasady USA w Bonn, a także zapowiedzieli ewentualny kontakt na terenie Polski. W rezultacie jednak służby amerykańskie przestały interesować się ofertą „A-1" (materiały źródłowe nie podają jednak, czym było to podyktowane)[47].

Odrębną kwestię we współpracy SB i KGB stanowiły służby specjalne Chińskiej Republiki Ludowej oraz Japonii. Wymieniano się informacjami na ich temat oraz podejmowano przedsięwzięcia przeciwko tym służbom w zakresie zwalczania i kontroli operacyjnej ich działalności, prowadzonej z pozycji placówek dyplomatycznych znajdujących się na terenie PRL i ZSRR.

W grudniu 1970 r. KGB wspólnie z SB realizowało przedsięwzięcie operacyjne polegające na podstawieniu pracownikom ambasady ChRL na terenie Polski agenta KGB. Właśnie w związku z tym do niejakiej Wiery Żełubowskiej, zamieszkałej w Białej Podlaskiej, przyjechał jej brat Georgij (Jurij) Kamiński, s. Michała, ur. w 1926 r., agent KGB ps. Juriew. Otrzymał on zadanie odwiedzenia ambasady chińskiej w Warszawie pod pretekstem poszukiwania brata. Postępowanie „Juriewa" było obliczone na ewentualne „podstawienie" go służbom ChRL. SB otrzymało zadanie stworzenia warunków odwiedzenia ambasady przez agenta KGB oraz jego skontrolowania. Polecenia strony radzieckiej były realizowane przy współudziale pracownika KGB z przedstawicielstwa w Warszawie – Winokurowa[48].

[46] AIPN, IPN BU 0189/38.

[47] AIPN Sz, IPN Sz 0079.

[48] W materiałach brak szczegółów dotyczących tego przedsięwzięcia. Źródło: AIPN, IPN BU 01062/42, t. 38, k. 358 - 359.

W 1978 r. przygotowano i zrealizowano działania operacyjne służące wprowadzeniu tajnych współpracowników Grupy „Wisła" ps. Józek, ps. S i ps. E do rozpracowania dyplomatów z ambasady ChRL oraz innych stałych przedstawicielstw Chin w ZSRR, podejrzanych o związki z chińskimi służbami specjalnymi (m.in. asystenta attaché wojskowego ChRL w ZSRR oraz korespondenta agencji „Sinhua" w Moskwie)[49].

W celu sprawniejszej koordynacji przedsięwzięć operacyjnych prowadzonych w stosunku do zachodnich służb specjalnych oraz wymiany doświadczeń SB i KGB przeprowadzały coroczne spotkania robocze w Warszawie i w Moskwie na szczeblu naczelników wydziałów. Przykładem może być spotkanie, które odbyło się w dniach 15 - 18 maja 1989 r. (…) *przebywała w Warszawie delegacja Wydziału XVII II Zarządu Głównego KBP ZSRR w składzie: płk Jużakow Boris Michajłowicz – Naczelnik Wydziału, ppłk Ponomariow Aleksiej Iwanowicz – kierownik sekcji, mjr Christowskij Sergiej Wsiewołodowicz – kierownik sekcji* (...) *Towarzysze radzieccy poinformowali o stosowanych przez CIA i BND nowych elementach w łączności korespondencyjnej, kontenerowej, a także radiowej z wykorzystaniem sztucznych satelitów* (...) *Wydział XVII II Zarządu Głównego KBP ZSRR przekazał stronie polskiej 70 próbek charakterów pisma, którymi sporządzone są „gotowce" oraz kasetę magnetofonową, zawierającą film dotyczący radiowego wyposażenia szpiegowskiego najnowszej generacji, w który wyposażeni są szczególnie cenni agenci CIA*[50].

Szkolenia funkcjonariuszy SB w szkołach związanych ze służbami specjalnymi ZSRR

Zagadnienia dotyczące szkoleń funkcjonariuszy MSW PRL w Wyższej Szkole KGB ZSRR po raz pierwszy zostały poruszone w kwietniu 1972 r. w Moskwie, podczas rozmów Ministra Wiesława Ociepki z kierownictwem KGB. W ich wyniku pierwsza grupa, licząca 10 funkcjonariuszy, została skierowana na roczne przeszkolenie operacyjne w Wyższej Szkole KGB ZSRR w listopadzie 1972 r.[51]. Dopiero rok później, 28 maja 1973 r., podpisane zostało *Zarządzenie Nr 054/73 Ministra Spraw Wewnętrznych* w sprawie zasad kierowania funkcjonariuszy resortu spraw wewnętrznych na studia i kursy w szkołach KGB i Ministerstwa Spraw Wewnętrznych Związku Socjalistycznych Republik Radzieckich, określające zasady rekrutacji do szkół w ZSRR oraz warunki kształcenia i rozliczania kosztów pobytu[52]. Zarządzenie to straciło moc 6 marca 1975 r. Od tej pory obowiązywało *Zarządzenie nr 018/75 Ministra Spraw Wewnętrznych* w sprawie rekrutacji i warunków kształcenia funkcjonariuszy resortu spraw wewnętrznych w wyższych szkołach ZSRR. Pomiędzy wymienionymi dokumentami nie było istotnych różnic[53].

---

[49] Plan rozwoju współpracy pomiędzy Departamentem II MSW PRL i II Zarządem Głównym KGB ZSRR na lata 1978 - 1981, zatwierdzony przez ministra spraw wewnętrznych PRL Stanisława Kowalczyka i Przewodniczącego KGB ZSRR Jurija Andropowa. Źródło: AIPN, IPN BU 0-654/2, k.23.

[50] Raport z dnia 29.06.1989 r. dotyczący rozmów z delegacją Wydziału XVII II Zarządu Głównego KGB ZSRR w dniach 15 - 18 maja 1989 r. Źródło: AIPN, IPN BU 01211/102, k. 186 - 187.

[51] *Wyciąg ze sprawozdania z wizyty Towarzysza Wiesława Ociepki w Moskwie w dniach 11 - 14 kwietnia 1972 r.* Źródło: AIPN, IPN BU 0-637/2, k. 3.

[52] *Zarządzenie Nr 054/73 Ministra Spraw Wewnętrznych z dnia 28 maja 1973 r.* Źródło: AIPN, IPN BU 1225/649, k. 18 - 21.

[53] *Zarządzenie nr 018/75 Ministra Spraw Wewnętrznych z dnia 6 marca 1975 r.* Źródło: AIPN, IPN BU 1254/162, k. 128 - 134.

Wspomniane zarządzenia zawierały kryteria, jakie musiał spełniać funkcjonariusz resortu spraw wewnętrznych PRL chcący odbyć przeszkolenie lub studia w ZSRR. W §1 ust. 2 znajduje się informacja: *Na studia lub przeszkolenie specjalne w ZSRR może być typowany funkcjonariusz, którego cechuje wysoka ideowość* (...) *wyróżnia się w pracy zawodowej, posiada znajomość języka rosyjskiego* (...) *Skierowanie funkcjonariusza na studia lub przeszkolenie* (...) *należy traktować jako szczególne wyróżnienie*[54].

Funkcjonariusze MSW PRL byli kierowani na przeszkolenia specjalne, studia wyższe, studia doktoranckie lub habilitacyjne do Akademii MSW ZSRR, Wyższej Inżynierskiej Szkoły Pożarniczo-Technicznej MSW ZSRR i Wyższej Szkoły KGB. Studia te odbywały się w systemie dziennym lub zaocznym. W przypadku systemu zaocznego funkcjonariusz w czasie całego cyklu nauki kilkanaście razy wyjeżdżał do ZSRR. Z każdego pobytu sporządzał sprawozdania. W czasie tych wyjazdów spotykał się z promotorem pracy, uczęszczał na lektorat języka rosyjskiego, zapoznawał się z literaturą niezbędną do napisania pracy, brał udział w pracach społecznych na uczelni bądź uczestniczył w wycieczkach i spotkaniach z innymi studentami.

Na studia doktoranckie i habilitacyjne byli kierowani funkcjonariusze będący pracownikami naukowo-dydaktycznymi, naukowo-badawczymi albo kandydatami na takich pracowników. Musieli też zajmować wyższe stanowiska kierownicze lub posiadać duże doświadczenie w służbie, wykazywać zainteresowania i uzdolnienia do pracy naukowo-badawczej lub naukowo-dydaktycznej, posiadać co najmniej 5-letni staż pracy w resorcie spraw wewnętrznych i odpowiednie przeszkolenie resortowe. Dodatkowo kandydat na studia habilitacyjne powinien posiadać stopień naukowy doktora oraz przedstawić dorobek naukowy z określonej dziedziny nauki lub dyscypliny naukowej[55].

Na przeszkolenie specjalne można było kierować funkcjonariuszy MO i SB od stanowiska zastępcy naczelnika wydziału (lub równorzędnego) wzwyż, przewidzianych do objęcia wyższych stanowisk służbowych. Jednocześnie warunkiem udziału w takim szkoleniu było posiadanie wykształcenia wyższego, co najmniej 5-letniego stażu pracy w SB (lub zwiadzie WOP) i odpowiedniego przeszkolenia resortowego[56].

Szkoła KGB była informowana przez stronę polską nie później niż na trzy miesiące przed skierowaniem grupy na szkolenie o poziomie wykształcenia ogólnego każdego słuchacza, posiadanym przez niego przygotowaniu do pracy operacyjnej, szczególnie operacyjno-agenturalnej, zajmowanych stanowiskach oraz stopniu znajomości języka rosyjskiego[57]. Opiekę nad funkcjonariuszami przebywającymi na studiach sprawował kierownik Grupy Operacyjnej „Wisła" MSW PRL przy KGB, do którego obowiązków należało udzielanie niezbędnej pomocy związanej z przyjazdem, pobytem i wyjazdem funkcjonariuszy, czuwanie nad ich właściwą postawą w czasie pobytu, rozliczanie funduszy przydzielonych kierownikom poszczególnych grup oraz składanie Dyrektorowi Departamentu Szkolenia i Doskonalenia Zawodowego MSW informacji o problemach związanych z procesem nauczania funkcjonariuszy[58].

---

[54] Tamże, k. 128.

[55] Tamże, k. 130.

[56] Tamże, k. 129.

[57] Pismo z grudnia 1974 r. do Dyrektora Gabinetu Ministra Spraw Wewnętrznych płk. J. Chomętowskiego, przesłane przez Przedstawiciela KGB ZSRR w Warszawie W. Sałowa. Źródło: AIPN, IPN BU 0-637/4, k. 21.

[58] *Zarządzenie nr 018/75 Ministra Spraw Wewnętrznych z dnia 6 marca 1975 r.* Źródło: AIPN, IPN BU 1254/162, k. 132 - 133.

Rekrutację na studia i przeszkolenie specjalne w ZSRR przeprowadzał Departament Kadr; weryfikacji zgłoszonych kandydatów dokonywała natomiast trzyosobowa komisja w składzie: przewodniczący – Dyrektor Departamentu Kadr MSW, członkowie – Dyrektor Departamentu Szkolenia i Doskonalenia Zawodowego MSW i przedstawiciel Komitetu Dzielnicowego PZPR w MSW.

W 1974 r. organy finansowe MSW PRL i KGB ZSRR podpisały protokół o warunkach finansowania i rozliczania kosztów związanych z nauką funkcjonariuszy MSW PRL w zakładach naukowych KGB ZSRR. Zgodnie z tym protokołem KGB ZSRR przyjmowało na studia pracowników MSW na podstawie przyjętego obustronnego porozumienia określającego listę słuchaczy oraz kierunki i okres nauczania. Zakłady naukowe KGB ZSRR miały wypłacać pracownikom MSW PRL przybyłym na studia stypendia w rublach, w wysokości ustalonej przez polskie MSW. Stypendia te miały być, wypłacane począwszy od dnia wjazdu pracownika MSW do ZSRR, do dnia wyjazdu poza jego granice, z wyłączeniem okresu wakacji (letnich i zimowych). Pracownicy MSW PRL byli kwaterowani w internatach zakładów naukowych KGB ZSRR bez członków rodzin. Gdy studia miały trwać dłużej niż jeden rok, można było ubiegać się o zgodę takiego zakładu i Departamentu Kadr na zamieszkanie w ZSRR wraz z rodziną. Wówczas studentowi wypłacano dodatek mieszkaniowy i rodzinny. Uczelnia KGB ZSRR pokrywała koszty przejazdów pracowników PRL z miejsca odbywania studiów do Warszawy (po zakończeniu danego cyklu, w okresie ferii zimowych, w okresie letnim w celu odbycia praktyki oraz w przypadkach wyjazdów związanych z przygotowywaniem pracy naukowej) oraz zapewniała opiekę lekarską. Koszty przejazdów pracowników z Polski do uczelni w ZSRR w każdym przypadku pokrywało MSW PRL. Zwracało też Związkowi Radzieckiemu wszystkie koszty związane z nauczaniem i utrzymaniem swoich pracowników w uczelniach KGB. W skład tych kosztów wchodziło: opłacanie zakwaterowania w internatach, przejazdów, wydatków związanych z opłacaniem profesorów i innego stałego personelu uczelni; finansowanie pomocy naukowych; opłaty za prywatnych nauczycieli czy konsultantów; opieka lekarska oraz wyżywienie[59]. Zwrot kosztów dokonywany był na podstawie art. 3 *Porozumienia między Rządem ZSRR i Rządem PRL o warunkach kształcenia żołnierzy Wojska Polskiego w wojskowych zakładach naukowych ZSRR* z dnia 22 czerwca 1960 r. Zgodnie z tym dokumentem zwrot kosztów następował dwa razy w roku: za I półrocze kalendarzowe – w październiku tego samego roku kalendarzowego i za II półrocze kalendarzowe – w kwietniu następnego roku kalendarzowego[60].

Od 1972 r. do 1980 r. corocznie na szkolenie do KGB ZSRR wyjeżdżała grupa 15 funkcjonariuszy. Od 1982 r. szkolenia te miały cykl 5-miesięczny (grupy 15 osobowe), a w latach 1986 - 1989 trzy razy w roku odbywały się szkolenia 3 - miesięczne. Program nauki obejmował m.in. zagadnienia dotyczące dywersji ideologiczno-politycznej, podstaw pracy kontrwywiadowczej, działalności KGB, działalności kontrwywiadu wojskowego oraz kryminalistyki operacyjnej. W ramach pierwszego bloku zapoznawano się

[59] Protokół podpisany na wiosnę 1974 r. przez Szefa Oddziału Finansów i Planowania przy RM ZSRR P. Zajcewa oraz Dyrektora Departamentu Finansów MSW PRL A. Duszę oraz zatwierdzony przez Zastępcę Przewodniczącego KGB ZSRR A. Małygina i Podsekretarza Stanu MSW PRL M. Milewskiego. Źródło: AIPN, IPN BU 0-1633/1, k. 1 - 7.

[60] *Porozumienie między Rządem ZSRR i Rządem PRL o warunkach kształcenia żołnierzy Wojska Polskiego w wojskowych zakładach naukowych ZSRR z dnia 22 czerwca 1960 r.* Źródło: AIPN, IPN BU 0-637/2, k. 15 - 16.

z tematyką odnośnie do ośrodków dywersyjnych na Zachodzie oraz walki z przeciwnikami ideologicznymi. W przypadku bloku drugiego uczono się organizacji pracy z osobowymi źródłami informacji oraz prowadzenia ewidencji spraw operacyjnych różnych kategorii[61].

Ponadto od 1985 r. przeprowadzany był 2-miesięczny Wyższy Kurs Doskonalenia Kadr KGB ZSRR w Leningradzie z zakresu obserwacji zewnętrznej. Raz w roku 10-osobowa grupa była szkolona w zakresie działalności przeciwnika na terytorium ZSRR i związanych z tym zadań dla służby obserwacji, wykorzystania kryminalistyki w pracy tego pionu, wrogiej działalności legalnych przedstawicielstw państw zachodnich na terytorium ZSRR i taktyki pracy obserwacji. Poruszane były również zagadnienia dotyczące stosowania techniki specjalnej i psychologii przez tę jednostkę. Uczestnicy szkoleń zapoznawani byli poza tym z prawem karnym ZSRR, z podstawami marksizmu-leninizmu oraz uczestniczyli w ćwiczeniach stricte fizycznych i wojskowych. Zajęcia odbywały się w formie wykładu lub seminarium, bez tłumacza[62].

Nie można ustalić dokładnej liczby funkcjonariuszy, którzy w latach 1972 - 1990 studiowali bądź odbyli przeszkolenie na uczelniach związanych z MSW ZSRR i KGB[63]. Na podstawie zidentyfikowanych materiałów źródłowych ich liczbę oszacowano na ponad 600 osób[64].

Zakończenie

Niniejsze opracowanie ukazuje relacje, jakie zachodziły między Departamentami polskiego MSW organami bezpieczeństwa ZSRR w latach 1970 - 1990. Zazębianie się interesów kontrwywiadów obydwu państw, spowodowane sytuacją polityczną, w sposób naturalny doprowadziło do współdziałania między nimi. Kierunki zainteresowań i wspólne realizacje spraw wynikały głównie z potrzeb strony radzieckiej i były im podporządkowane.

Na podstawie analizowanych dokumentów widać jednoznacznie, że koordynacja działań obu służb była systematyczna i standardowa. W prezentowanych materiałach nie ma najmniejszej wzmianki na temat wyjątkowości, czy też szczególnego charakteru ich współpracy.

Dokumenty wskazują jednoznacznie, że strona polska przykładała dużą wagę do współpracy z KGB. Świadczą o tym szczegółowe odpowiedzi na zapytania strony radzieckiej. Także jednostronne meldunki z działań Departamentu II MSW wskazują, iż wymiana informacji odbywała się zgodnie z wcześniejszymi ustaleniami.

Współpraca SB i KGB dotyczyła szerokiego wachlarza działań. Z jednej strony była to kontrwywiadowcza ochrona jednostek Armii Radzieckiej, z drugiej natomiast – działania operacyjne wobec obywateli innych państw oraz zabezpieczanie międzyna-

[61] Szkolenia funkcjonariuszy resortu spraw wewnętrznych PRL w Wyższej Szkole KBP ZSRR w latach 1985 - 1990. Źródło: AIPN, IPN BU 0-637/9, k. 4 - 30.

[62] *Sprawozdanie z przeszkolenia grupy aktywu kierowniczego pionu „B" w Wyższej Szkole Obserwacji w Leningradzie z 11.09.1987 r.* Źródło: AIPN, IPN BU 0-637/10, k. 26 - 27.

[63] Jest to spowodowane brakiem pełnej dokumentacji osób delegowanych na uczelnie ZSRR.

[64] Szacowano na podstawie informacji znajdujących się w pismach Dyrektorów Departamentu Kadr MSW, Departamentu Szkolenia i Doskonalenia Zawodowego MSW i Gabinetu Ministra MSW oraz kierowanych do Przedstawicielstwa KGB ZSRR w Warszawie.

rodowego ruchu granicznego. Do działań operacyjnych należy także zaliczyć kontrolę operacyjną mniejszości narodowych i przeciwdziałanie funkcjonowaniu służb specjalnych przeciwnika. Za przejaw wymiany informacji można natomiast uznać nie tylko różnego rodzaju korespondencję pomiędzy służbami, ale przede wszystkim uczestnictwo strony polskiej w PSED[65]. System ten zapewniał szybką i bieżącą wymianę danych na temat osób, instytucji i organizacji. Środkiem mającym gwarantować i uzupełniać właściwe wykonywanie zadań wynikających z planów współpracy obu służb były działające w Warszawie i Moskwie ich oficjalne przedstawicielstwa. Z kolei współpraca na płaszczyźnie pozaoperacyjnej polegała na organizowaniu szkoleń dla polskich funkcjonariuszy na terenie ZSRR.

Opierając się na analizowanych materiałach, udało się wytypować 600 funkcjonariuszy studiujących i odbywających szkolenia w radzieckich uczelniach. Zidentyfikowano 149 agentów wykorzystywanych we wspólnie prowadzonych przez SB i KGB działaniach operacyjnych.

W zaprezentowanej pracy nie udało się w pełni odtworzyć działalności przedstawicielstwa KGB w Polsce. Nie do końca powiodła się także próba ustalenia danych funkcjonariuszy SB i KGB współpracujących przy realizacji konkretnych spraw operacyjnych. Jest to spowodowane brakiem części materiałów, które zapewne zostały zniszczone przed rokiem 1990.

Niniejszy artykuł stanowi próbę podjęcia tematyki dotyczacej współpracy SB i KGB w latach 1970 - 1990. W żadnym wypadku nie wyczerpuje jednak tego zagadnienia. Pozwala jednie wyznaczyć kierunki dalszego pogłębienia poszczególnych aspektów tej współpracy.

Streszczenie

Niniejszy artykuł stanowi kontynuację opracowania dotyczącego współpracy KGB i SB w latach 1970 - 1990 opublikowanego w poprzednim numerze „Przeglądu Bezpieczeństwa Wewnętrznego". Jego autorzy korzystali z materiałów archiwalnych byłego MSW przechowywanych w Instytucie Pamięci Narodowej.

Jak wynika z treści artykułu, współpraca wyżej wymienionych służb dotyczyła szerokiego zakresu działań. Z jednej strony była to kontrwywiadowcza ochrona jednostek Armii Radzieckiej, z drugiej – działania operacyjne wobec obywateli innych państw oraz zabezpieczanie międzynarodowego ruchu granicznego. Do działań operacyjnych zaliczyć także należy przeciwdziałanie aktywności służb specjalnych krajów demokracji zachodniej. Z kolei współpraca na płaszczyźnie pozaoperacyjnej polegała na organizowaniu dla polskich funkcjonariuszy szkoleń na terenie ZSRR.

Podjęta próba dokonania bilansu współpracy w żadnym wypadku nie wyczerpuje jednak tego tematu. Pozwala jednie wyznaczyć kierunki dalszych prac nad pogłębianiem tego zagadnienia.

[65] PSED – Połączony System Danych Ewidencyjnych o Przeciwniku.

ABSTRACT

This article is a continuation of the paper on the development of cooperation between the Soviet KGB and the Polish Security Service (SB) in the years 1970 - 1990, published in the previous edition of the "International Security Review". The authors used the archives of the former Ministry of Interior stored at the Institute of the National Remembrance (IPN).

As highlighted in the article, the cooperation of KGB and SB related to a wide spectrum of activities such as, counterintelligence protection of Soviet Army and operational activities against citizens of other countries and the security of the international cross border traffic.

Such operational activity includes countering any activity of the Western democracies' intelligence services. The non operational cooperation related to trainings for Polish officers in the Soviet Union.

This article does not fully cover the subject, it just allows to indicate directions for future in depth analysis of the topic.

VII
RECENZJE

Rafał Leśkiewicz

Jens Gieseke, *STASI. Historia 1945 - 1990*, Kraków 2010, Wydawnictwo Uniwersytetu Jagiellońskiego s. 341.

W ciągu ostatnich kilkunastu lat w krajach dawnego bloku wschodniego prowadzono szereg prac badawczych obejmujących swym zakresem działalność komunistycznych organów bezpieczeństwa. Na polskim rynku wydawniczym pojawiła się m.in. książka opisująca historię STASI – niezwykle skutecznego tworu Niemieckiej Republiki Demokratycznej. Jest to swego rodzaju podsumowanie dotychczasowych badań prowadzonych przez Jensa Gieseke – historyka pracującego w Urzędzie Pełnomocnika Federalnego ds. Dokumentów Służby Bezpieczeństwa (BStU), zwanego niegdyś potocznie Urzędem Gaucka, a obecnie bardziej znanego jako *Birthler-Behörde*[1]. Z przedmowy do książki dowiadujemy się, że jej pierwsze niemieckie wydanie opublikowano w 2001 r. Przygotowując wydanie drugie autor zaznaczył, iż poczynione przez niego uzupełnienia dotyczą prezentacji szerszego kontekstu historycznego, bez ograniczania się wyłącznie do omówienia historii STASI jako jednego z narzędzi komunistycznego aparatu represji. Wydanie drugie Gieseke poszerzył o wątki związane z rolą NRD w polityce międzynarodowej oraz umieścił w nim informacje na temat bilansu ofiar komunizmu w wydaniu wschodnioniemieckim.

Fenomen STASI, zdaniem autora, polegał przede wszystkim na tym, że była to najbardziej rozbudowana policja polityczna w krajach Europy Środkowo-Wschodniej. Przez czterdzieści lat funkcjonowania bardzo skutecznie potrafiła ona objąć inwigilacją i kontrolą niemal całe społeczeństwo NRD[2]. Było to możliwe przede wszystkim dzięki dobrej organizacji zarówno aparatu administracyjnego, jak i operacyjnego.

Działalność wschodnioniemieckich komunistycznych służb bezpieczeństwa jest nierozerwalnie związana z historią Niemieckiej Republiki Demokratycznej. Na enerdowski system służb specjalnych składały się dwa resorty: Ministerstwo Spraw Wewnętrznych (*Ministerium des Innern* − MdI) i Ministerstwo Bezpieczeństwa Państwowego (*Ministerium für Staatssicherheit* − MfS). W strukturze MdI znajdowała się Niemiecka Policja Ludowa. MfS z kolei składało się z tajnej policji politycznej (Staatssicherheit – potocznie STASI) i wywiadu (Hauptverwaltung Aufklärung – HVA). Oba resorty funkcjonowały niezależnie od siebie w zasadzie przez cały okres istnienia NRD, z krótką dwuletnią przerwą od lipca 1953 do listopada 1955 r., kiedy to MfS formalnie podlegało MdI. Ogólnie rzecz biorąc, bezpieka zawsze była niezależna od innych struktur państwowych. MfS powołano ustawą z dnia 8 lutego 1950 r. uchwaloną jednogłośnie przez Izbę Ludową. W systemie politycznym NRD nadzór nad ministerstwem bezpieczeństwa sprawowała Niemiecka Socjalistyczna Partia Jedności (*Sozialistische Einheitspartei Deutschlands* − SED).

---

[1] Ustalenia poczynione przez Jensa Gieseke były w Polsce publikowane w okresie kilku ostatnich lat. Zob. dla przykładu: J. Gieseke, *German Democratic Republic*, w: *A handbook of the communist security apparatus in east central Europe 1944 - 1989*, edited by K. Persak i Ł. Kamiński, Warsaw 2005, s. 163 - 219; tenże, *Niemiecka Republika Demokratyczna*, w: *Czekiści. Organy bezpieczeństwa w europejskich krajach bloku sowieckiego 1944 -1989*, red. K. Persak i Ł. Kamiński, s. 325 - 391.

[2] Spośród książek wydanych w języku polskim – zob. E. Matkowska, *System. Obywatel NRD pod nadzorem tajnych służb*, Kraków 2003, ARCANA.

Służba Bezpieczeństwa Państwowego (STASI) uchodziła za jedną z najskuteczniejszych służb specjalnych drugiej połowy XX w. Na czym polegała ta skuteczność i wyjątkowość? Przede wszystkim na tym, że korzystając z nieograniczonych wręcz prerogatyw przydzielonych przez aparat władzy, w zasadzie sprawowała pełną kontrolę nad całym społeczeństwem. Oprócz prewencyjnej inwigilacji obywateli, funkcjonariusze STASI zajmowali się ochroną wschodnioniemieckich dygnitarzy partyjnych, kontrolą ruchu granicznego, handlem bronią i wykradaniem zagranicznych technologii. Jako ciekawostkę warto wspomnieć, że STASI miała nawet swój klub sportowy (FC Dynamo Berlin), który kilkakrotnie zdobył piłkarskie mistrzostwo NRD.

Na czele MfS i jego struktury stali kolejno: Wilhelm Zaisser (1950 - 1953), Ernst Wollweber (1953 - 1957) oraz Erich Mielke (1957 - 1989). Formację tę zlikwidowano w związku z jesiennymi przemianami 1989 r. Najpierw, 18 października, od władzy odsunięto Ericha Honeckera, a jego następcą został Egon Krenz. W kilka tygodni później, na początku listopada, ze stanowiska ustąpił Erich Mielke, który wystąpił również z Biura Politycznego. 7 grudnia 1989 r. Mielkego aresztowano. Nieco wcześniej, 17 listopada, premier Hans Modrow ogłosił przekształcenie MfS w Urząd Bezpieczeństwa Narodowego. Ostatecznie rozwiązywanie wschodnioniemieckiej bezpieki zakończono w marcu 1990 r.

Książka Jensa Gieseke to pasjonująca i ambitna lektura. Autor opisuje organizację i funkcjonowanie STASI w sposób kompleksowy. Publikacja składa się z ośmiu rozdziałów zatytułowanych kolejno: 1. *Dziesięć dni i dziesięć lat*, 2. *Antyfaszyzm – stalinizm – zimna wojna domowa. Źródła i wpływy w latach 1945 – 1956*, 3. *Najbezpieczniejsza NRD świata – siły napędzające rozwój STASI*, 4. *Nieoficjalny Współpracownik – nowy typ donosiciela*, 5. *Inwigilacja obejmująca cały obszar kraju? STASI w społeczeństwie NRD*, 6. Opór – opozycja – prześladowanie, 7. *Wolf i spółka – działania MfS na Zachodzie i za granicą*, 8. *Ostateczny kryzys i upadek 1989/1990*. Uzupełnieniem narracji są zamieszczone na końcu książki wykresy ilustrujące budżet Ministerstwa Bezpieczeństwa Państwowego w latach 1957 - 1989 oraz rozwój kadrowy, począwszy od roku 1950, a kończąc na 1989. Interesujące są również dwa wykresy przedstawiające szczegółową strukturę organizacyjną MfS w 1989 r. wraz z nazwiskami osób, które stały na czele poszczególnych jednostek i komórek Ponadto, książka zawiera rzetelnie opracowany i obszerny wykaz skrótów. Co szczególnie przydatne, obok polskich objaśnień haseł zamieszczono w nim także oryginalne terminy niemieckie.

Recenzowana praca oparta jest na bogatym materiale naukowym. Na końcu każdego rozdziału umieszczono przypisy. Bardzo pomocna, na przykład dla osób pragnących pogłębić wiedzę o działalności STASI, jest również bibliografia opatrzona autorskim komentarzem. Autor jednak w stosunkowo niewielkim tylko stopniu odwołuje się w przypisach do wytworzonych przez STASI dokumentów, które do dziś zachowały się w archiwach BStU i innych.

W publikacji Giesekego nie zamieszczono, niestety, żadnych zdjęć. Wizerunki opisywanych tu osób i obiektów dostępne są oczywiście w innych pracach dotyczących wschodnioniemieckiej bezpieki, ale ich brak w tej konkretnie pracy ewidentnie ją zubaża.

Warto wspomnieć również o języku książki. Jej narracja jest dynamiczna, a użyte sformułowania i terminy należą do tzw. branżowego słownictwa służb specjalnych. Autor jednak nie używa zapożyczeń z tzw. *lingua securitatis* zbyt często, co należy do przyzwyczajeń wielu badaczy zajmujacych się historią komunistycznych służb bezpieczeństwa. Dzięki temu książkę, mimo jej naukowego charakteru, czyta się bardzo dobrze.

Jens Gieseke, syntetycznie opisując działalność STASI, formułuje pytanie o rolę tej formacji w systemie instytucjonalnym państwa socjalistycznego, w którym władza miała charakter monolityczny. W odpowiedzi koncentruje się na opisaniu przede wszystkim mechanizmów, rzadko przywołując konkretne sprawy realizowane przez tę służbę.

Prezentując mechanizmy funkcjonowania obrosłej wręcz legendą agentury STASI, autor podnosi niezwykle istotne w tym aspekcie kwestie ideologii, korzyści osobistych lub strachu. Niewiele natomiast pisze o bardzo powszechnej praktyce pozyskiwania współpracowników na podstawie spreparowanych materiałów kompromitujących. Gieseke w umiejętny sposób przedstawił za to swego rodzaju niemiecki patent na przezwyciężanie pewnych zachowań, czy raczej oporów, związanych z donoszeniem na bliskich, w tym z przekazywaniem informacji o sprawach intymnych. Ciekawy jest także opis mechanizmu tajnej współpracy ze STASI byłych funkcjonariuszy komunistycznej bezpieki i działaczy SED.

W książce w przejrzysty sposób omówiono strukturę organizacyjną wschodnioniemieckiej policji politycznej. Z jej lektury wynika, że w skład enerdowskich tajnych służb wchodziły Centrala (mieszcząca się w Berlinie) oraz Zarządy Rejonowe (14 Rejonów) i Komendy Okręgowe (217 Okręgów). Taki podział związany był z przeprowadzeniem w NRD w 1952 r. reformy administracyjnej, w wyniku której zlikwidowano podział na landy. W okresie przed reformą, tj. w latach 1950 - 1952, funkcjonowało 5 Zarządów w landach i komendy w ponad 100 okręgach[3].

Poza tym omawiana publikacja opisuje mechanizm określany jako „zasada sekcji". Oznacza ona, że wszystkie obszary życia społecznego i politycznego były podporządkowane kontroli organów bezpieczeństwa państwa. Potrzeby powołania niektórych sekcji związane były nie z obszarami zabezpieczenia, ale z ewentualnymi kierunkami ataku „wroga", czyli np. obcego wywiadu (przede wszystkim zachodnioniemieckiego), podziemia politycznego itp. Autor bardzo szczegółowo przedstawił także kontrolę gospodarki i skalę niemalże permanentnej inwigilacji. Dla przykładu, w 1989 r. STASI mogła jednorazowo, np. w Berlinie Wschodnim, podsłuchiwać 20 tys. rozmów telefonicznych. Ponadto aktywnie wykorzystywała zespoły obserwacyjne oraz zakładała podsłuchy w mieszkaniach. W celu uzupełnienia lub aktualizacji danych funkcjonariusze STASI sięgali po dokumenty ubezpieczeniowe, akty zgłoszeń chorób wenerycznych, kartoteki biblioteczne, dane z kartotek szpitalnych itd.[4] .

Jak wspomniano na wstępie, historia wschodnioniemieckiej bezpieki opisana została w szerszym kontekście funkcjonującego systemu komunistycznego (wraz z jego specyfiką) we Wschodnich Niemczech. Z tego też powodu w książce znalazło się miejsce na zaprezentowanie i krótką charakterystykę działalności niemieckiej opozycji demokratycznej. Gieseke zwrócił uwagę na różnice mentalne i ideologiczne między śro-

[3] Warto wspomnieć o ciekawej książce historyka z BstU − Christiana Halbrocka − zatytułowanej *Mielkes Revier. Stadtraum und Alltag rund um die MfS – Zentrale in Berlin – Lichtenberg*, Berlin 2010. Jest to przewodnik po Centrali MfS. Autor opisał w niej funkcjonowanie Centrali Ministerstwa Bezpieczeństwa Państwowego w Berlinie wskazując, że było to swego rodzaju miasto w mieście, żyjące własnym życiem i przestrzegające własnych zasad. To tu podejmowano najważniejsze decyzje związane z działalnością aparatu bezpieczeństwa.

[4] Mechanizm inwigilacji obywateli w znakomity sposób ilustruje film fabularny pt. *Życie na podsłuchu* (*Das Leben der Anderen)* w reżyserii Floriana Heneckela von Donnersmareka (Niemcy 2005/2006).

dowiskiem opozycji w NRD i w innych państwach tzw. bloku wschodniego, w tym także w Polsce. Interesujący, choć wydaje się, że za mało rozwinięty, jest wątek dotyczący kontaktów opozycjonistów wschodnioniemieckich ze środowiskami tzw. zachodnioniemieckiej „Nowej Lewicy". Przywołując dane statystyczne, autor podał, że wiosną 1989 r. STASI zarejestrowała 2,5 tys. osób wśród aktywnych działaczy opozycji, z czego 600 uznała za przywódców, a ok. 60 za wrogów socjalizmu.

W książce poruszony jest również wątek dotyczący ucieczek mieszkańców NRD do RFN, przede wszystkim przez najsłynniejszy fragment granicy znajdujący się w Berlinie. Statystyki przywołane przez autora są szokujące. Otóż, przed wybudowaniem słynnego muru na Zachód uciekło ok. 3 mln obywateli NRD, po jego zbudowaniu zaś, w latach 1961 - 1989, nieco ponad 650 tys.

Niezwykle interesujący jest także fragment poświęcony mechanizmowi prowadzenia postępowań karnych, ukazuje bowiem genezę i ewolucję machiny komunistycznego terroru oraz „szczególną" współpracę niemieckiej bezpieki z organami wymiaru sprawiedliwości. Najpierw omówiono pierwsze lata funkcjonowania radzieckich obozów specjalnych, w których z różnych przyczyn zmarło blisko 63 tys. osób. Okazuje się, że do 1955 r. sowieckie trybunały wojskowe wydały co najmniej 1963 wyroki śmierci na niemieckich cywilów, z czego co najmniej 1201 wyroków zostało wykonanych, a w 616 przypadkach karę śmierci zamieniono na dożywotnie więzienie. Od lat 60. XX wieku oficjalnie orzekane kary śmierci należały do rzadkości. Trzy ostatnie wyroki wykonano na oficerach MfS. Autor przedstawił również problematykę dotyczącą mordów politycznych. Jednak prawdopodobnie z powodu braku istotnych dokumentów źródłowych temat ten został wyłącznie zasygnalizowany.

Zdecydowanie za mało miejsca poświęcono w omawianej publikacji działalności Zarządu Głównego Wywiadu (*Hauptverwaltung Aufklärung* – HVA). Z uwagi na charakter działań oraz zakres działalności poza granicami NRD jednostka ta bez wątpienia była uważana za szczególnie ważną w rozbudowanym systemie organów bezpieczeństwa. Na podstawie przeprowadzonych badań Gieseke ustalił, że poza granicami komunistycznych Niemiec, pod koniec ich istnienia, w działaniach MfS uczestniczyło 9 - 10 tys. funkcjonariuszy bezpieki. Przy czym, największą grupę wśród nich stanowili funkcjonariusze HVA, w tym z podległych mu wydziałów w zarządach rejonowych. Autor doliczył do tego prawie 5 tys. funkcjonariuszy z komend okręgowych oraz ponad 2 tys. osób pełniących służbę w jednostkach wywiadu radiowego i kontrwywiadu.

W książce skoncentrowano się na uogólnieniach; prezentując działania wywiadu, w zasadzie nie przywołano żadnych konkretnych przykładów. Wiadomo chociażby, że działania służb specjalnych NRD skupiały się wokół planowania operacji specjalnych w Afryce. Niestety, z książki Giesekego nie można się zbyt wiele na ten temat dowiedzieć. Autor nie dokonał nawet krótkiej syntezy, zadowalając nas jedynie przywołaniem ogólników i kilku faktów[5].

[5] W języku polskim ukazała się książka autorstwa Maskusa Wolfa i Anne McElvoy pt. *Człowiek bez twarzy. Autobiografia szefa STASI* (Warszawa 1998) dotycząca działań HVA. Jak wskazuje tytuł oraz nazwisko współautora, powinna to być autobiografia szefa wschodnioniemieckiego wywiadu – Markusa Wolfa, który kierował HVA w latach 1952 - 1986. W rzeczywistości jednak, mimo że znalazło się tu wiele interesujacych informacji na temat działań wywiadu enerdowskiego na całym świecie, jest to praca o charakterze popularnym.

W publikacji przedstawiono także szereg działań STASI w sektorach związanych z gospodarką narodową. Omówiono tu m.in. funkcjonowanie wywiadu gospodarczego i technologicznego, wskazując na te obszary, które w odczuciu władz komunistycznych Niemiec były szczególnie istotne z operacyjnego punktu widzenia. Owo ukierunkowanie działań pośrednio wynikało z aktualnych zapotrzebowań. I tak, w latach 60. XX wieku wywiad wschodnioniemiecki interesowały np. procedury dotyczące produkcji włókien syntetycznych, w latach 80. zaś – energia i mikroelektronika.

Mało miejsca poświęcono w publikacji samemu momentowi likwidacji Ministerstwa Bezpieczeństwa Państwowego. Co prawda rozdział ósmy zatytułowany *Ostateczny kryzys i upadek 1989/1990* obejmuje ponad 20 stron, jednak więcej miejsca poświęca się w nim opisowi upadku NRD niż przekształceniu organów bezpieczeństwa w służby specjalne. Ciekawy jest podrozdział zatytułowany *STASI jako dziedzictwo*. Polski czytelnik odnajdzie w nim wiele analogii do sytuacji, która przed dwudziestoma laty występowała także w naszym kraju (chociażby w kwestii problemu dokumentów bezpieki czy roli funkcjonariuszy służb komunistycznych w demokratycznym społeczeństwie), ale i różnic. To, czego na pewno brakuje w omawianej książce, to porównania dotyczące poszczególnych sfer działalności STASI do jej instytucjonalnych odpowiedników w innych krajach Europy Środkowo-Wschodniej. Autor nie odniósł się do tego, co typowe i specyficzne dla działań komunistycznych organów bezpieczeństwa, tj. w zasadzie nie poruszył wątku współpracy STASI z innymi służbami z krajów bloku wschodniego; nie dokonał również zestawień dotyczących problematyki i ilości spraw prowadzonych przez tę służbę, zarówno jeśli chodzi o kierunki działań, jak i stosowane metody pracy operacyjnej. Są to bardzo istotne zagadnienia, bez ich omówienia historia STASI na pewno nie jest pełna.

Konkludując należy stwierdzić, że do rąk czytelników trafiła publikacja przygotowana rzetelnie i ujęta syntetycznie. Mimo mankamentów, które zostały wykazane i omówione powyżej, na pewno warto po nią sięgnąć. Na rynku wydawniczym ukazuje się dość dużo pozycji na temat historii służb specjalnych państw demokratycznych oraz tych funkcjonujących w krajach tzw. demokracji ludowej. Wśród nich dominują prace popularno-naukowe lub popularne, w których główny nacisk kładziony jest na opis tajnych operacji, często w stylu sensacyjnym. Zwykle brakuje w nich analiz opartych na autentycznych źródłach. Z kolei prace naukowe często są nadmiernie naszpikowane materiałem faktograficznym, brakuje w nich uogólnień. W przypadku książki Jensa Gieseke mamy do czynienia z wartościowym opracowaniem naukowym, po które może sięgnąć każdy, kogo interesuje historia NRD lub działalność komunistycznych policji państwowych.

Krzysztof Izak

Anat Berko, *Droga do raju. Świat wewnętrzny zamachowców samobójców,* Zakrzewo–Poznań 2010, Replika s. 308.

Książka Anat Berko jest czwartą z kolei pozycją na polskim rynku wprowadzającą czytelników w świat zamachowców-samobójców i ideę męczeńskiej śmierci. Trzy poprzednie to: *Narzeczone Allaha* Julii Jusik (Videograf II, 2006), opowiadająca o czeczeńskich terrorystkach-samobójczyniach, *Idea szahadatu w kulturze Iranu* Sylwii Surdykowskiej (Wydawnictwa UW, 2006), omawiająca ideę i kult męczeństwa w szyizmie oraz *Męczeństwo w islamie* Davida Cooka (Wydawnictwo UJ, 2009), przedstawiające płaszczyznę kulturową, doktrynalną i historyczną islamu oraz analizujące zjawisko męczeństwa.

Pierwsze wydanie *Drogi do raju*... ukazało się w 2004 r. w języku hebrajskim. Trzy lata później w USA i Wielkiej Brytanii pojawił się jej angielski przekład. W 2010 r. książkę wydano w języku polskim.

W swej publikacji Anat Berko w sposób niezwykle profesjonalny poszerza wiedzę na temat zamachowców-samobójców, skupiając się głównie na terrorystach palestyńskich. Autorka (ekspert od spraw terroryzmu w randze podpułkownika) przez 25 lat służyła w izraelskich siłach zbrojnych i jednostce antyterrorystycznej, walcząc z Hezbollahem i palestyńskimi organizacjami terrorystycznymi. Po odejściu ze służby zajęła się pracą badawczą dotyczącą terroryzmu. Dysertację doktorską, obronioną w 2003 r. na Wydziale Kryminologii Uniwersytetu Bar-Ilan w Ramat Gan w Izraelu, poświęciła porównaniu motywacji, którymi kierują się w swych działaniach palestyńscy terroryści i pospolici przestępcy, w tym zabójcy. Na podstawie tych badań sformułowała m.in. wniosek, że terroryści, w odróżnieniu od pospolitych przestępców, posiadają osąd moralny społeczeństwa, w stosunku do którego stosują przemoc.

Obecnie Berko jest pracownikiem naukowym Instytutu Polityki Międzynarodowej ds. Walki z Terroryzmem w Herzliya (Izrael) i Uniwersytetu George'a Washingtona w Waszyngtonie. Kontynuuje również badania na zlecenie izraelskiej i amerykańskiej Rady Bezpieczeństwa Narodowego, prowadzi wykłady na wielu zachodnich uczelniach oraz wygłasza odczyty na temat terroryzmu dla FBI i dowództwa NATO.

Droga do raju … powstała niejako „na marginesie" wspomnianej dysertacji Berko. Autorka podczas zbierania materiałów do tej pracy odbyła szereg spotkań z osadzonymi w izraelskich więzieniach zamachowcami-samobójcami, którzy albo zostali ujęci przed dokonaniem zamachów lub zrezygnowali z ich przeprowadzenia w ostatniej chwili, albo przygotowywali i koordynowali zaplanowane akcje. Istotną grupę rozmówców Berko stanowiły kobiety, dzięki którym mogła zanalizować dokonywanie samobójczych ataków, patrząc ich oczami.

Publikacja składa się z 15 rozdziałów. Tytuł każdego z nich jest charakterystycznym, emocjonalnie zabarwionym zdaniem wypowiedzianym przez osoby różnej płci i w różnym wieku. Każda z tych wypowiedzi może stanowić swego rodzaju motto. Skazani, zarówno kobiety, jak i mężczyźni, z którymi spotykała się Berko, nie byli na ogół skuwani w kajdanki, choć strażnicy przestrzegali ją, że osoby, skazane na wielokrotne dożywocie, mogą zachować się różnie. Autorka jednak nie czuła się specjalnie zagrożona. Można sądzić, że z racji pełnionej wcześniej służby musiała poznać sztuki walki, choć w książce ani słowem o tym nie wspomina.

Berko w żadnym wypadku nie usprawiedliwia swoich rozmówców. Zapoznaje nas jedynie z ich odczuciami i stara się zrozumieć rzeczywiste przyczyny, które popchnęły tych ludzi ku „męczeństwu". Jednocześnie próbuje nakreślić portrety psychologiczne niedoszłych zamachowców i zrozumieć ich motywację. Okazuje się, że powody, dla których osoby te zamierzały zostać *szahidami* (męczennikami za sprawę Allaha), są różne, choć można ustalić ich pewne cechy wspólne: zemstę z powodu śmierci lub aresztowania bliskiej osoby, postępowanie w ślad za kimś, kto dał przykład swym męczeństwem, nienawiść do Izraela z powodu złego traktowania Palestyńczyków przez żołnierzy tego kraju, walkę o niepodległość Palestyny, a w przypadku kobiet – zmycie z siebie hańby i ratowanie honoru rodziny. Okazuje się, że wiara w rajskie życie po męczeńskiej śmierci plasuje się u tych osób często na drugiej lub nawet dalszej pozycji. Tak więc religijna motywacja „islamikadze", wbrew powszechnemu mniemaniu, wcale nie jest najważniejsza, choć niewątpliwie nadal pozostaje ważnym czynnikiem.

Berko krok po kroku przedstawia także okoliczności, które sprawiają, że muzułmanie (niektórzy zresztą niezbyt religijnie radykalni, ani nawet zbyt religijni) chcą odebrać sobie życie, decydując się na samobójczy atak bombowy.

Szczególną grupę osób biorących udział w męczeńskich operacjach stanowią ich organizatorzy, często zajmujący się także werbunkiem zamachowców-samobójców. To im autorka poświęciła pierwsze rozdziały. Według relacji jednego z nich, organizacje terrorystyczne werbują do przeprowadzania zamachów osoby zepchnięte na margines społeczny, które, w ich własnym mniemaniu, mogłyby zaskarbić sobie poważanie właśnie poprzez męczeńską śmierć (nawiasem mówiąc, na takim marginesie żyje obecnie większość Palestyńczyków w Strefie Gazy). Idealnymi kandydatami są więc osoby mające niską samoocenę, nie potrafiące odnaleźć się w społeczeństwie i otaczającej je rzeczywistości, w związku z czym odczuwają rozgoryczenie i gniew. Okazuje się jednak, że o ile w latach 1993 - 1996 (tj. po zawarciu porozumienia izraelsko-palestyńskiego) można było sporządzić pewien portret typowego zamachowca-samobójcy, o tyle trudno tego dokonać w przypadku zamachowców drugiej intifady z lat 2000 - 2006 (intifada Al-Aksa).

Z lektury *Drogi do raju*… można dowiedzieć się, że wcześniejsze zamachy przeprowadzali w większości ludzie młodzi, niewykształceni i nie posiadający rodzin. W ostatniej dekadzie było nieco inaczej. Tak ważnej roli, jak dotychczas, nie odgrywał już także ekstremizm religijny. Organizatorzy zamachów i zamachowcy nie byli fanatykami religijnymi. Niektórzy nawet stawali się bardziej religijni dopiero w izraelskich więzieniach, pod wpływem współwięźniów. Nie zmienia to jednak faktu, że w większości wypadków indoktrynacja religijna pozostaje integralną częścią procesu przygotowania zamachowca-samobójcy do przeprowadzenia ataku.

Berko wykazuje, że zamachowcy-samobójcy często kierują się pragnieniem pomszczenia śmierci krewnych albo nienawiścią do Izraela. Innym bodźcem jest obietnica nagrody pieniężnej wypłacanej rodzinie *szahida* po dokonaniu zamachu. Autorka ustala jednak, że wielu zamachowców, którzy dokonywali ataków, nie miało problemów finansowych i żyło na średnim poziomie w porównaniu z pozostałymi Palestyńczykami. Ponadto większość z nich nie doświadczyła zaburzeń emocjonalnych, których skutkiem byłaby niezdolność do odróżniania rzeczywistości od wyobrażeń.

W omawianej publikacji czytamy, że zamachowiec-samobójca nie uważa ludzi, których zabija, za ofiary, w związku z czym ludzkie uczucia nie odgrywają u niego żadnej roli. Dzieje się tak dlatego, że ci, którzy wysyłają żywe bomby z „samobójczą misją" demonizują wrogów (na przykład Żydów) na wszelkie możliwe sposoby. Nazywają ich „zabójcami proroków", „krwiopijcami", „potomkami małp i świń", „wrogami

Allaha" itp. Takie określenia w odniesieniu do Żydów występują na przykład w publikacjach wydawanych przez Hamas, w kazaniach, podręcznikach, a nawet w pismach dla dzieci. Organizatorzy zamachów dążą do tego, aby samobójcy nie myśleli o sobie; starają się wykorzenić u nich emocje i myśli dotyczące nawet najbliższych. Próbują także dehumanizować przyszłe ofiary w ich umysłach. Potencjalni zamachowcy poddawani są procesowi emocjonalnemu, który powoduje u nich neutralizację ocen moralnych. Jeśli jednak jakiś impuls spowoduje przerwanie takiego stanu, przypominającego trans, może zrodzić się szansa na oprzytomnienie zamachowca i odstąpienie przez niego od zbrodniczych zamiarów. Tym odczuciom często jednak przeciwstawia się strach przed zleceniodawcą.

Przykładem rezygnacji z „samobójczej misji" było zachowanie jednej z rozmówczyń Berko, która dotarła do celu przeprowadzenia zamachu, ale zauważywszy kobietę z dzieckiem i przypomniawszy sobie dzieci w swojej rodzinie, zaniechała ataku. Organizator niedoszłej operacji był bardzo rozgniewany. Stwierdził: (…) *wielu ludziom zależało na tym ataku, więc spieprzenie* (sic!) *nie wchodzi w grę*.

Organizatorów zamachów z organizacji Hamas, Palestyński Islamski Dżihad i Brygady Męczenników Al-Aksy uważa się za osoby przestrzegające podstawowych zasad moralnych, często budzące podziw, gdyż uchodzą za bojowników. Osoby te stają się wzorem dla wielu młodych muzułmanów. Należy zaznaczyć, że dojrzewanie mężczyzny w społeczeństwie arabskim przebiega w zgodzie z zasadami społecznymi, religijnymi i kulturowymi. Wielka hipokryzja organizatorów zamachów polega na tym, że nigdy nie posłaliby na śmierć własnych dzieci, nawet z najbardziej szlachetnych pobudek.

Osobny rozdział autorka poświeciła rozmowie z szejkiem Ahmedem Yassinem, założycielem, szefem i głównym ideologiem Hamasu. Rozmowę tę przeprowadziła w grudniu 1996 r. w więzieniu, w którym odbywał on karę dożywotniego pozbawienia wolności[2]. W spotkaniu towarzyszył jej mąż, badacz islamu. Rozmowa dotyczyła m.in. sensu dżihadu i motywacji szahidów. Wypowiedzi szejka przesycone były religijnością, odwołaniami do *Koranu* i hadisów[3] oraz metaforami, niekiedy bardzo skrajnymi, a dla nas, wychowanych w innej kulturze – często wręcz śmiesznymi. Yassin przede wszystkim podkreślał, że dla żarliwego muzułmanina świat doczesny pozbawiony jest wartości, tak więc wielu bojowników Allaha wybiera śmierć, która jest dla nich przyjemna, i męczeństwo, które nie jest brzemieniem, lecz rzeczą dobrą i upragnioną. Zwracał uwagę, że mudżahedin musi prowadzić dżihad dla Allaha, a nie dla własnej sprawy. Jego celem nie może być chęć zostania przywódcą czy zdobycia poważania. Szahidem natomiast, według niego, nie może być ktoś, kto wprawdzie odważnie broni swej rodziny lub plemienia, ale zapomina o urzeczywistnieniu słów Allaha. Yassin pochwala dokonywanie samobójczych ataków przez osoby podejrzewane o kolaborację z Izraelem oraz przez kobiety, które chcą oddalić od siebie kompromitujące podejrzenia i ratować

[2] W 1989 r. szejk Ahmed Yassin został skazany na dożywocie, ale w 1997 r. władze Izraela zmuszone były go uwolnić, wymieniając go po podjętej przez Mossad nieudanej próbie zabicia Chaleda Meszala, szefa Biura Politycznego Hamasu w Syrii, na dwóch izraelskich agentów. Po uwolnieniu Yassin nadal kierował organizacją. Izrael oskarżał go o organizowanie ataków terrorystycznych. Yassin zginął 22.03.2004 r. w wyniku eksplozji pocisku rakietowego wystrzelonego z izraelskiego helikoptera.

[3] Hadis – opowieść przytaczająca wypowiedź proroka Mahometa, jego czyn lub milczącą aprobatę. Każdy hadis składa się z tekstu i łańcucha przekazicieli. Hadisy tworzą sunnę (Tradycję) – najważniejsze po *Koranie* źródło muzułmańskiego prawa szariatu.

honor rodziny poprzez zmazanie własnej hańby.

Zasadniczą część książki stanowią rozmowy przeprowadzone z palestyńskimi więźniarkami, które zdecydowały się na przeprowadzenie samobójczego ataku. Dla większości z nich indoktrynacja religijna była jedynie dodatkowym czynnikiem ich motywacji. Jedna z tych kobiet chciała zostać samobójczynią, aby zemścić się na ojcu, który nie wyraził zgody na jej wymarzone małżeństwo.

Dla niektórych młodych dziewczyn, jak wynika z lektury książki, początkiem nieszczęścia staje się internet. Organizacje ekstremistyczne korzystają z sieci, aby manipulować młodymi, niedoświadczonymi arabskimi kobietami, chcącymi nawiązać kontakt ze światem zewnętrznym. Następnie je wykorzystują. Ich członkowie nawiązują z nimi romantyczne znajomości, które często muszą być ukrywane przez nie przed rodziną (nie zapominajmy, że jest to kultura i moralność arabska, a zachowanie nie musi mieć związku z religijną żarliwością).

Znajomości nawiązane na czatach przez Arabów żyjących w Izraelu i mieszkających w Autonomii Palestyńskiej poszerzają kontakty i wiedzę o tym, co dzieje się po obu stronach. Dochodzi do znajomości i romansów na odległość. Niekiedy następują potajemne spotkania. Wówczas pojawia się strach przed rodziną lub groźba szantażu ze strony partnera, który w wielu wypadkach okazuje się być członkiem organizacji terrorystycznej. Zdarza się dokonywanie gwałtów na arabskich kobietach w celu zmuszenia ich do przeprowadzenia samobójczych operacji.

Z relacji niektórych rozmówczyń Anat Berko wynika, że zamachy przeprowadzają także kobiety, które często są w ciąży, choć nie wyszły za mąż, albo kobiety mające reputację angażujących się w kontakty seksualne bez ślubu. Żyją one w wielkim stresie, grozi im bowiem śmierć ze strony męskich krewnych, którzy chcą bronić honoru rodziny. Samobójczy zamach jest w takich ptrzypadkach honorowym, poważanym wyjściem z trudnej sytuacji zarówno dla takich kobiet, jak i ich rodzin.

Niektóre kobiety zmuszane są do przeprowadzania zamachów przez mężów i członków Hamasu w związku z tym, że podejrzewane są o romanse. W tego rodzaju sytuacjach wielokrotnie wystarcza jedynie drobna szkalująca pogłoska. Przypuszczalnie dlatego Hamas, który na ogół jest przeciwnikiem zamachów bombowych przeprowadzanych przez kobiety, poparł jedną z tego typu akcji.

Jedna z rozmówczyń Berko przyznała, że chciała popełnić samobójstwo, ponieważ jej mąż dopuszczał się w stosunku do niej gwałtów i przemocy. Samobójczy zamach bombowy miał jej przynieść oczyszczenie, a jej rodzinie zapewnić poważanie i pieniądze. Ale też wiele kobiet, które z różnych powodów się nie wysadziły, twierdziło, że zasadniczą motywacją ich działania była chęć uczestniczenia w narodowościowej walce zbrojnej i religia.

Do 2006 r. Palestynki dokonały 10 ataków samobójczych. Pierwsza z nich wysadziła się w Jerozolimie w styczniu 2002 r. W wieku 16 lat wyszła za mąż za swego kuzyna. Była w nim zakochana. Jednak przez 9 lat nie mogła zajść w ciążę. Mąż się z nią rozwiódł i ożenił ponownie. Z drugą żoną miał dzieci. Jest bardzo prawdopodobne, że samobójczyni zdecydowała się na ten krok, gdyż czuła się niezrealizowana jako kobieta i matka.

Autorka pisze, że ponad dwadzieścia kobiet aresztowano, gdy udawały się na miejsce zaplanowanego zamachu lub podczas przygotowań do niego. Świadczy to o dość dobrym rozpoznaniu komórek organizujących zamachy przez izraelskie służby. Kobiety te, nadmienia Berko, w większości nie ukończyły trzydziestego roku życia, nie były mężatkami i ukończyły przynajmniej szkołę średnią. Większość z nich, wbrew

obiegowym informacjom podawanym w naszych mediach i literaturze, należała do organizacji Fatah, ale były wśród nich także członkinie Ludowego Frontu Wyzwolenia Palestyny oraz Palestyńskiego Islamskiego Dżihadu. Tylko dwie kobiety, które wysadziły się w Gazie, należały do Hamasu.

Między wierszami głównego wątku książki możemy przeczytać o życiu organizatorów zamachów (zwłaszcza niedoszłych szahidek) w izraelskich zakładach karnych. Często wyrażają oni opinię, że dopiero, gdy znaleźli się w więzieniu i poznali swoich wrogów – Żydów – zaczęli uważać ich za ludzi. Spotkanie z innymi więźniami spowodowało u nich odczuwanie bliskości z nimi i dostrzeganie człowieczeństwa u innych ludzi.

Palestyńczycy osadzeni w izraelskich więzieniach obchodzą wszystkie uroczystości. Przywiązują też duże znaczenie do rocznic, którym niekiedy przypisują magiczną moc. Wiele dat ma dla nich znaczenie szczególne, na przykład 15 maja to Dzień Katastrofy (tego dnia 1948 r. ustanowiono państwo Izrael), a 30 marca to Dzień Ziemi (tego dnia po raz pierwszy przeprowadzono wysiedlenie Palestyńczyków, aby budować osiedla żydowskie). Jest także wiele dni ustanowionych przez ugrupowania ekstremistyczne jako Dni Gniewu.

Lektura książki pozwala nam zapoznać się ze zwyczajami panującymi w izraelskich więzieniach. Czytamy tu, że osadzeni mają prawo korespondencyjnie uczyć się i studiować, a skazane kobiety – wychowywać dzieci do ukończenia przez nie drugiego roku życia (podany jest fakt, że jedna z terrorystek urodziła w więzieniu dziecko). Zaskakiwać może, że w więzieniach panuje całkowita dowolność ubioru. Niektóre więźniarki na przykład noszą tradycyjne stroje muzułmańskie, inne natomiast – wprost przeciwnie – bluzki lub koszulki z krótkimi rękawami i obcisłe dżinsy. Wiele z nich swą urodę podkreśla makijażem, niekiedy bardzo wyzywającym.

Nie brak jednak i ciemnych stron. Wyraźnie rysują się prowadzące do konfliktów różnice między członkiniami i zwolenniczkami różnych palestyńskich ugrupowań. Mimo, iż władze więzienne rozdzielają skonfliktowane strony piętrami, niekiedy dochodzi do sytuacji drastycznych (na przykład oblanie wrzącą margaryną zwolenniczki ugrupowań fundamentalistycznych przez protagonistkę świeckiego Tanzimu[4]).

Drogę do raju… Anat Berko, pomimo skromnego wydania, czyta się dobrze. Książka ma jednak pewną wadę: autorce nie udało się uniknąć powtórzeń. Często wraca do rozmów, które opisała kilka rozdziałów wcześniej. Czytelnikowi nieobeznanemu z poruszaną tu tematyką na pewno pomocny będzie słowniczek terminów arabskich umieszczony na końcu książki, a profesjonaliści zajmujący się badaniem terroryzmu i jego zwalczaniem mogą poszerzyć wiedzę o literaturę zawartą w bibliografii (niestety, wymienione są tu w większości trudno dostępne wydawnictwa amerykańskie i izraelskie, choć niektóre z nich, jak opracowania Bruce'a Hoffmana i Marca Sagemana zostały już przetłumaczone na język polski).

Książka Anat Berko jest godna polecenia zwłaszcza funkcjonariuszom służb odpowiedzialnych za walkę z terroryzmem oraz pracownikom naukowym zajmującym się badaniem tego zjawiska. Publikacją powinni być zainteresowanie również oficerowie śledczy, gdyż zawiera ona cenny materiał poznawczy dotyczący sposobu prowadzenia rozmów i wnikania do wnętrza człowieka.

[4] Tanzim – radykalna frakcja al-Fatah, która wyodrębniła się w 1995 r. po zawarciu porozumień pokojowych w Oslo. Podczas intifady Al-Aksa członkowie Tanzimu zaczęli cieszyć się dużą popularnością dzięki udziałowi w walkach ulicznych z Izraelczykami. Do Tanzimu należą również palestyńscy chrześcijanie.

Jerzy Stańczyk

Stanisław Koziej, *Między piekłem a rajem: szare bezpieczeństwo na progu XXI wieku*, Toruń 2006, Adam Marszałek, s. 332.

Problematyka bezpieczeństwa narodowego i międzynarodowego stała się obecnie niezwykle nośna. W ostatnim czasie niezwykle popularyzowana jest przez media i uznawana za jedno z najważniejszych zagadnień dotyczących życia społecznego. Upowszechnianiu zagadnień związanych z tego typu bezpieczeństwem nieczęsto jednak towarzyszy należycie wysoki poziom dyskursu. Tymczasem zagadnienia z zakresu bezpieczeństwa stanowią złożony i trudny problem, wymagający od autora wypowiedzi dużej wiedzy. Dlatego już na wstępie można z przyjemnością stwierdzić, że recenzowana książka to głos niezwykle pożądany we wspomnianej debacie, gdyż nazwisko jej autora gwarantuje wysoki profesjonalizm w traktowaniu przedmiotowego tematu i płynącą z doświadczenia refleksję na temat poruszanych problemów.

Celem publikacji, w intencji jej autora, było określenie istoty i charakteru współczesnych wyzwań i zagrożeń dla szeroko rozumianego bezpieczeństwa narodowego i międzynarodowego, przedstawienie podstawowych zasad i sposobów reagowania kryzysowego i obronnego, w tym skutecznego funkcjonowania organów administracji i podmiotów gospodarczych w sytuacjach nadzwyczajnych. Co to w praktyce oznacza? Otóż – dostarczenie wiedzy i pobudzenie świadomości w celu skutecznego radzenia sobie z różnorodnymi problemami z zakresu bezpieczeństwa, a więc m.in. ze sprawnym funkcjonowaniem państwa w różnych sytuacjach kryzysowych, przewidywaniem i zapobieganiem konfliktom, a także organizowaniem skutecznego reagowania kryzysowego.

Książka składa się ze wstępu, ośmiu rozdziałów, zakończenia i bibliografii. W jej strukturze dostrzega się, choć nieformalnie, trzy części. Dwa pierwsze rozdziały (*Podstawy bezpieczeństwa* i *Współczesne środowisko bezpieczeństwa*) poświęcone są istocie i ewolucji najważniejszych kategorii z dziedziny bezpieczeństwa narodowego i międzynarodowego oraz zmianom charakteru współczesnego środowiska bezpieczeństwa. Założeniem autora było pragmatyczne, a nie przeteoretyzowane, podejście do problemu. Kolejne trzy rozdziały (*Strategia i polityka bezpieczeństwa mocarstw globalnych*, *Strategia i polityka bezpieczeństwa organizacji międzynarodowych* oraz *Międzynarodowe kampanie i operacje bezpieczeństwa*) dotyczą problematyki bezpieczeństwa międzynarodowego. Rozpatrywane są tu przede wszystkim treści koncepcji strategicznych i praktyczne ich urzeczywistnianie w kampaniach bezpieczeństwa. Trzy ostatnie rozdziały (*Ewolucja bezpieczeństwa narodowego Rzeczypospolitej Polskiej w końcu XX wieku, Strategia i polityka bezpieczeństwa narodowego Rzeczypospolitej Polskiej w warunkach członkostwa w NATO* i *Kierowanie bezpieczeństwem narodowym*) odnoszą się do spraw krajowych – ukazują ewolucję sposobów zapewniania bezpieczeństwa naszemu krajowi oraz formułują postulaty dotyczące transformacji bezpieczeństwa.

Całość stanowi obszerną, wielowątkową monografię, bazującą na reprezentatywnej literaturze przedmiotu, dokumentach i materiałach prasowych. Już od pierwszych stron uwagę zwraca krytyczne spojrzenie autora na przedstawiane kwestie, poparte jego wiedzą i doświadczeniem. To niewątpliwy atut wyróżniający tę publikację na tle innych wydawnictw podejmujących problematykę bezpieczeństwa. Przez całość monografii przewijają się takie zasadnicze pojęcia, jak: interesy i cele dotyczące bezpieczeństwa, szanse na bezpieczeństwo ogólne, wyzwania i zagrożenia bezpieczeństwa, w tym

kryzysy i konflikty, koncepcje strategiczne i operacyjne w zakresie bezpieczeństwa oraz systemy bezpieczeństwa narodowego i międzynarodowego. W charakterystykach współczesnego środowiska bezpieczeństwa uwaga skierowana zostaje głównie na terroryzm międzynarodowy i proliferację broni masowego rażenia.

W podejściu pragmatycznym, jak to sam na wstępie podkreślił autor, bezpieczeństwo określone zostaje w sposób dynamiczny jako taka dziedzina aktywności danego podmiotu, która *zmierza do zapewnienia możliwości przetrwania, rozwoju i swobody realizacji własnych interesów w konkretnych warunkach, poprzez wykorzystywanie okoliczności sprzyjających (szans), podejmowanie wyzwań, redukowanie ryzyka oraz przeciwdziałanie (zapobieganie i przeciwstawianie się) wszelkiego rodzaju zagrożeniom dla podmiotu i jego interesów*[1]. Autor opowiada się przy tym za nadrzędnością strategii nad polityką przy kierowaniu państwem czy inną organizacją, czyli czynników generalnych i długofalowych nad bieżącą polityką. Skupiając uwagę na działaniach strategicznych, dalsze swe rozważania opiera na wyróżnieniu trzech rodzajów tych działań, tj. działań prewencyjno-stabilizacyjnych, reagowania kryzysowego i obronnych (wojennych). W jego pragmatycznym podejściu bezpieczeństwo zawsze występuje w kontekście społecznym, w którym ujawniają się sprzeczności na tle różnic interesów. To powoduje uciekanie się do przemocy. W konsekwencji: *Stosowanie przemocy i przeciwstawianie się przemocy jest zatem główną treścią kryzysów i konfliktów społecznych, a tym samym główną treścią bezpieczeństwa*[2]. I właśnie tym zagadnieniom poświęcona jest recenzowana książka.

Odnosząc się do nowych warunków prowadzenia działań zbrojnych, autor omawia m.in. kwestie prymatu jakości nad ilością, asymetryczności zagrożeń i działań oraz wiążącego się z tym problemu tzw. walki sieciowej oraz operacji zintegrowanych, cywilno-wojskowych. W jego opinii, terrorystyczne ataki na Stany Zjednoczone z 11 września 2001 r. stanowią koniec ery specjalizacji w sferze bezpieczeństwa. Ponieważ w zintegrowany sposób należy wykorzystać cały potencjał i wysiłki ludzi dla przeciwstawiania się tym nowym zagrożeniom, *Niejako wracamy do pierwotnej sytuacji, gdy wojny prowadziły całe społeczności, a nie tylko ich wyodrębnione, wyspecjalizowane struktury. Wracamy na nowo do najdawniejszej, klasycznej teorii wojen. To jest ostateczne zwycięstwo Sun-Tzu nad Clausewitzem*[3]. To zintegrowane podejście do spraw bezpieczeństwa stanowi zasadniczy wątek publikacji.

Przyszłe konsekwencje dla środowiska bezpieczeństwa autor upatruje w dwóch wielkich rewolucjach: informacyjnej i geopolitycznej (globalizacja, rozpad świata dwubiegunowego). Bezpieczeństwo także podlega globalizacji. Mówimy przecież o bezpieczeństwie globalnym, na co zresztą zwracano uwagę wraz z wybuchami wojen światowych. Globalizacja zmienia środowisko bezpieczeństwa, sprzyjając m.in. uaktywnieniu się (erupcji) terroryzmu międzynarodowego. W pragmatycznej konstatacji autora, przyjętej na potrzeby tej książki, istotą terroryzmu jest (…) *ostentacyjne i maksymalistyczne (masowe, totalne, nieograniczone), celowe (tj. świadomie zamierzone) atakowanie niewinnych, postronnych (cywilnych) osób i dóbr publicznych (otoczenia) dla pośredniego (asymetrycznego, poprzez opinię publiczną) oddziaływania na rzeczywistego przeciwnika politycznego lub ideologicznego*[4]. W warunkach globalizacji

[1] S. Koziej, *Między piekłem a rajem: szare bezpieczeństwo na progu XXI wieku*, Toruń 2006, Adam Marszałek, s. 7.
[2] Tamże, s. 17.
[3] Tamże, s. 23.

organizacje i grupy terrorystyczne zaczęły stawać się samodzielnymi graczami strategicznymi na arenie międzynarodowej, co stawia je przed nowymi wyzwaniami i zagrożeniami. Dodatkowym niebezpieczeństwem jest łączenie terroryzmu z przestępczością zorganizowaną, czy groźba posłużenia się przez terrorystów bronią masowego rażenia. Globalna sieć terrorystyczna zyskuje przy tym cechy swoistego mocarstwa światowego. Jak więc zauważa autor, jakościowe zmiany środowiska bezpieczeństwa na progu XXI wieku powodują, że: *Do opisu stanu bezpieczeństwa nie wystarczają już dzisiaj klasyczne kategorie pokoju i wojny. Kończy się klarowny wybór między rajem pokoju i piekłem wojny. Ludzkość musi potrafić radzić sobie ciągle w środowisku pośrednim między rajem i piekłem. Bezpieczeństwo tutaj nie jest czymś albo czarnym, albo białym. Jest to po prostu bezpieczeństwo szare*[5].

Przedstawiając strategie i polityki bezpieczeństwa mocarstw globalnych, autor skupia uwagę na Stanach Zjednoczonych, Federacji Rosyjskiej, a także (choć w dużo mniejszym stopniu) na Chinach i Indiach. Wnikliwie analizowane są tu dokumenty ważne z punktu widzenia polityki bezpieczeństwa tych państw. Dokonywane są niezbędne wyjaśnienia, dopowiadane komentarze i formułowane uwagi krytyczne. Omawiane rozwiązania odnoszone są przy tym do polskiej rzeczywistości, co pozwala na formułowanie istotnych postulatów w tym zakresie. Przykładem jest choćby, w nawiązaniu do amerykańskiej strategii obrony narodowej, następujący osąd: *Konia z rzędem temu, kto wytłumaczy naszą logikę strategiczną. Najpierw prezydent określa generalne zadania strategiczne, w tym także zadania sił zbrojnych, a potem bezpośrednio ustala, w jaki sposób siły zbrojne mają wykonać te zadania. Oznacza to ni mniej ni więcej, że w kolejnym cyklu sam będzie się przed sobą rozliczał z wykonawstwa zadań wojskowych w dziedzinie bezpieczeństwa narodowego. Nic pozytywnego z takiej logiki wyniknąć nie może*[6]. Autorowi podoba się wyraźne wyróżnienie dwóch nurtów w strategii amerykańskiej: operacyjnego (działania bieżące przy współczesnych wyzwaniach) i transformacyjnego (przygotowania do przyszłych wyzwań). Traktuje je jako dwie strony tej samej praktyki strategicznej. I śmiało formułuje następujący pogląd: *Myślę, że tego typu podejście jest na tyle logiczne i uzasadnione, że powinniśmy go wykorzystać także w konstruowaniu układu własnych strategii. Proponowałbym wręcz wyróżnianie dwóch działów, czy też dwóch dziedzin koncepcji strategicznych: strategii operacyjnej (strategii działania) i strategii transformacyjnej (strategii rozwoju)*[7]. Wyjaśnić tu należy, że autor ma świadomość kontrowersji, jakie mogą budzić terminy strategia operacyjna czy operacja strategiczna (według tradycyjnego rozumienia rozróżniano bowiem następującą triadę pojęć składających się na szczeble sztuki wojennej: strategię, sztukę operacyjną i taktykę)[8]. Jednakże opowiada się za współczesną amerykańską koncepcją pojęciową, która pojawia się także w pracach polskich autorów[9].

W omawianej publikacji zestawiona i przeanalizowana jest również strategia i polityka bezpieczeństwa takich organizacji międzynarodowych, jak: ONZ, OBWE, NATO i Unia Europejska (UE). Zwłaszcza tym dwóm ostatnim poświęcono, co zrozumiałe, dużo uwagi. Charakteryzując nowe wyzwania wobec NATO na początku XXI wieku, autor jednoznacznie opowiada się za potrzebą wypracowania nowej koncepcji strategicznej

[4] Tamże, s. 31.
[5] Tamże, s. 43.
[6] Tamże, s. 71.
[7] Tamże, s. 72.
[8] F. Skibiński, *Rozważania o sztuce wojennej,* Warszawa 1972, Wojskowy Instytut Historyczny.
[9] M. Wiatr, *Między strategią a taktyką*, Toruń 2002, Adam Marszałek.

tego Sojuszu. Słuszne wydaje się jego założenie, że: *Punktem wyjścia polskiej refleksji o sojuszniczych potrzebach w dziedzinie bezpieczeństwa i celach strategicznych musi być konstatacja interesów (racji stanu) NATO jako całości w świetle polskich interesów narodowych*[10]. Wyróżniając dwa zasadnicze kierunki strategicznego zainteresowania NATO (według tradycyjnego kryterium przestrzenno-strategicznego: północny/wschodni i południowy), S. Koziej dodaje jeszcze trzeci – kierunek globalny (związany głównie z rozprzestrzenianiem się zagrożeń terrorystycznych i broni masowego rażenia). Założenia operacyjne przyszłej strategii Sojuszu odnosi natomiast do dwóch podstawowych koncepcji: prewencyjno-stabilizacyjnej oraz reagowania kryzysowego i obronnego. Jednocześnie zwraca uwagę na potrzebę stworzenia nowej jakościowo kategorii sił (obok sił interwencyjnych i reagowania) w postaci sił stabilizacyjnych i rekonstrukcyjnych służących pokojowej odbudowie.

Autor nie jest przekonany co do realnych możliwości ustanowienia skutecznych struktur militarnych w ramach Unii Europejskiej. Pisze wręcz o „papierowym" charakterze tych inicjatyw. Trudno byłoby obalić jego pogląd, że: *Tę papierowość potwierdza powszechny zamiar unijnych członków NATO wyznaczania do dyspozycji Unii Europejskiej tych sił, które już są przeznaczone do NATO. Tak też postępuje Polska. (...) Od takiego manewru nie przybywa żadnych zdolności obronnych. Co najwyżej mogą być osłabione przez nadmierne komplikowanie sposobu ich wykorzystania*[11]. W konsekwencji rodzą się niebezpieczeństwa dla skuteczności obrony europejskiej. Jedyne rozwiązanie tego problemu autor widziałby w doprowadzeniu do takiej sytuacji, w której wszystkie państwa UE będą jednocześnie członkami NATO. Wówczas Europejska Tożsamość w Dziedzinie Bezpieczeństwa i Obrony w ramach NATO pokryłaby się z Europejską Polityką Bezpieczeństwa i Obrony UE. W konsekwencji w NATO funkcjonowałyby dwa podmioty: Unia Europejska i Stany Zjednoczone.

Wiele miejsca w publikacji poświęcono również uwagom i komentarzom do strategii bezpieczeństwa Unii Europejskiej z 2003 r. W opinii autora, błędem było zainicjowanie wówczas Europejskiej Polityki Bezpieczeństwa i Obrony bez jednoczesnego określenia strategii: *Polityka bez strategii nie może być skuteczna; mało – nie może być racjonalnie realizowana*[12]. Właśnie w tym upatrywać można słabości i niepowodzenia polityki europejskiej w tym zakresie. Zupełnie inaczej, tj. racjonalnie, zachowały się Stany Zjednoczone, reagując na nowe wyzwania i zagrożenia dla bezpieczeństwa. Natomiast: *Europejczycy patrzyli na nowe problemy tylko, albo głównie, w kontekście bieżących, doraźnych (politycznych) celów i rezultatów. Ignorowali podejście strategiczne*[13]. Ponadto, jak twierdzi S. Koziej, europejska strategia bezpieczeństwa nie jest kompletna, gdyż nie określa, jakie są interesy i strategiczne cele jej podmiotu oraz jakie zasoby (siły i środki) należy wydzielić do realizacji przyszłej koncepcji działania. Autor zwraca też uwagę, że to, co w tej strategii prezentowane jest jako cele strategiczne, w istocie jest zestawem celów operacyjnych. Jednocześnie podkreśla zauważalną tendencję do zbliżania się tego kształtującego się strategicznego podejścia europejskiego w sprawach bezpieczeństwa do obowiązującej strategii amerykańskiej i zgadza się, by Unię Europejską definiować jako podmiot bezpieczeństwa o charakterze globalnym. W erze globalizacji jest to zasadne, a tego właśnie długo brakowało także w odniesieniu do NATO.

[10] S. Koziej, *Między piekłem a rajem*..., s. 121.
[11] Tamże, s. 146.
[12] Tamże, s. 157.
[13] Tamże.

Wśród omawianych międzynarodowych kampanii i operacji dotyczących bezpieczeństwa znalazły się kampanie bałkańska i afgańska oraz kryzys iracki. Przy ich ocenie S. Koziej postuluje potrzebę wypracowania globalnej strategii dla tego typu przedsięwzięć, którą określa jako strategię wyprzedzania zagrożeń. Jest to nawiązanie do amerykańskiej strategii działań prewencyjnych i uprzedzających, na której opiera się przeciwdziałanie terroryzmowi i rozprzestrzenianiu się broni masowego rażenia. Nie jest to jednak bezkrytyczne przyjmowanie wzorców amerykańskich. W publikacji wiele miejsca poświęca się również analizie słabości tego typu rozwiązań.

Postulowaną strategią, według założeń, miałyby się posługiwać także organizacje międzynarodowe, wyprzedzając sytuacje kryzysowe. W opinii autora strategia ta, mająca logiczne i operacyjne uzasadnienie, powinna stać się strategią całej społeczności międzynarodowej. Jednocześnie *pozostawienie wyboru na poziomie strategii narodowych mogłoby w sumie doprowadzić do stanu swego rodzaju anarchii strategicznej, w którym to każde państwo wedle własnego uznania przyznawałoby sobie prawo do akcji prewencyjnych*[14].

W omawianej publikacji szeroko ukazana została ewolucja bezpieczeństwa narodowego Polski na przełomie wieków. Dokonano tu przeglądu doktryn i strategii polityczno-wojskowych obowiązujących od roku 1990 do 2003 i uzupełniono je postulatami dotyczącymi kierowania bezpieczeństwem narodowym. Z przemyśleń autora wynika konieczność przeprowadzenia poważnej debaty strategicznej (i powstania instytucji ją organizującej), długofalowego myślenia o bezpieczeństwie oraz stworzenia zintegrowanego (cywilno-wojskowego i ponadresortowego) systemu bezpieczeństwa państwa. Jest to rezultat dostrzegania zacierania się granic między niektórymi strategicznymi instytucjami, w których kompetencjach leży zapewnianie bezpieczeństwa. Niezbędna staje się powszechność, profesjonalizacja i konsolidacja podejmowanych działań w celu jak najlepszego realizowania interesów narodowych. Jednocześnie dotychczasowa koncepcja obrony terytorialnej wymaga przekształcenia w szerszą koncepcję dotyczącą powszechnego bezpieczeństwa terytorialnego.

Omawiana książka jest zasobnym źródłem wiedzy o najważniejszych problemach związanych z bezpieczeństwem narodowym i międzynarodowym w warunkach globalizacji. Obrazuje złożoność współczesnego środowiska bezpieczeństwa i jego ewolucję, jak również wskazuje na jakościowo nowe wyzwania i zagrożenia wymagające nowych rozwiązań strategicznych. Jednocześnie zachęca do wyzbycia się obiekcji wobec strategii wyprzedzających i postuluje tworzenie zintegrowanych systemów bezpieczeństwa – zarówno w wymiarze narodowym, jak i globalnym.

Logiczna struktura, bogata baza faktograficzna i bibliograficzna, załączone materiały poglądowe w postaci diagramów, a także przystępny styl wypowiedzi są niewątpliwymi atutami recenzowanej publikacji. Widoczne jest także duże zaangażowanie emocjonalne autora, przejawiające się m.in. w odważnej krytyce dotychczasowych rozwiązań w zakresie zapewniania bezpieczeństwa, w formułowaniu konkretnych sądów czy wniosków dla Polski.

W książce tej pada wiele pytań. Nie na wszystkie z nich znajdziemy bezpośrednie i wyczerpujące odpowiedzi. Jednak wyczulenie czytelnika na złożoność problematyki bezpieczeństwa oraz koncepcje autora dotyczące nowoczesnego podejścia do tego zagadnienia w wysokim stopniu zasługują na zainteresowanie się omawianym wydawnictwem.

[14] Tamże, s. 203.

VIII
WYDARZENIA

Kamila Sacewicz

Propozycje poprawy skuteczności reagowania na sytuacje kryzysowe o charakterze terrorystycznym[1]

W dniach 22 - 23 listopada 2010 r. w Józefowie oraz Emowie koło Warszawy[2] zostało przeprowadzone sztabowe ćwiczenie antyterrorystyczne na wypadek ataku z użyciem broni chemicznej (TTEx-01 OPCW), zrealizowane w ramach *Decyzji Rady Europejskiej ws. wsparcia działań OPCW w zakresie wprowadzania w życie strategii UE przeciwko rozprzestrzenianiu broni masowego rażenia* (nr 2009/569/CFSP) z 27 lipca 2009 r. Inicjatorem przedsięwzięcia była Organizacja ds. Zakazu Broni Chemicznej (OPCW), a organizatorami Rządowe Centrum Bezpieczeństwa, Ministerstwo Spraw Zagranicznych oraz Agencja Bezpieczeństwa Wewnętrznego.

Do udziału w ćwiczeniu zaproszono 150 uczestników z 27 państw członkowskich OPCW, reprezentantów 16 organizacji międzynarodowych i pozarządowych, właściwe rzeczowo organa administracji rządowej i samorządowej RP oraz przedstawicieli przemysłu chemicznego.

Celem ćwiczenia była weryfikacja procedur zarządzania kryzysowego na poziomie lokalnym, narodowym i międzynarodowym na podstawie fikcyjnego scenariusza ćwiczenia opracowanego przez konsultantów OPCW. Aktywny udział ABW pozwolił na koordynację tych elementów ćwiczenia, które były związane z realizacją ustawowych zadań służb specjalnych.

Scenariusz zakładał atak terrorystyczny na zakład chemiczny ulokowany w gęsto zaludnionym rejonie, w którego wyniku zniszczeniu ulega zbiornik zawierający 20 ton chloru. Na skutek powyższego dochodzi do wycieku toksycznej substancji w pobliżu ruchliwej drogi krajowej, którą w tym czasie przejeżdżają uczestnicy międzynarodowej imprezy masowej. W konsekwencji zachodzi konieczność hospitalizacji poszkodowanych oraz ewakuacji okolicznych mieszkańców. Atak terrorystyczny poprzedzają intensywne działania służb odpowiedzialnych za przeciwdziałanie i zwalczanie terroryzmu. Służby te są obecne także podczas akcji ratunkowej.

Należy zaznaczyć, że imprezie towarzyszył szereg spotkań planistycznych oraz spotkanie podsumowujące, przeznaczone dla podmiotów krajowych. Przedmiotowe spotkania stanowiły zasadniczy element całości przedsięwzięcia. Powyższe wypływało z faktu, że sztabowy charakter ćwiczenia był odzwierciedleniem prac wykonywanych w okresie poprzedzającym realizację imprezy, w związku z czym przebieg ćwiczenia pozostawał niezakłócony.

Przygotowania obejmujące określenie roli poszczególnych aktorów w przygotowanym przez konsultantów OPCW scenariuszu zdarzeń, który wymagał odniesienia się do właściwości rzeczowej poszczególnych graczy i tym samym narzucał koniecz-

[1] Opracowano na podstawie dokumentacji własnej ABW, materiałów RCB oraz raportów międzynarodowego konsultanta ds. rozbrojenia, przekazanych przez OPCW.

[2] Ćwiczenie odbyło się w obiekcie konferencyjnym hotelu Holiday Inn w Józefowie oraz w Centralnym Ośrodku Szkolenia ABW w Emowie.

ność bliższego zrozumienia ich zakresów kompetencyjnych i wskazania realnych możliwości operacyjnych, a ponadto precyzował zasady współpracy ukierunkowanej na zwalczenie zagrożenia, wydają się być najważniejszym etapem ćwiczenia. Tym samym wyraźnie uwidocznione zostało szczególne znaczenie jego sztabowego charakteru, który umożliwia podniesienie jakości działań odpowiednich służb i organów administracji bez konieczności ponoszenia wysokich nakładów finansowych towarzyszących realnym ćwiczeniom.

Do celów ćwiczenia i jednocześnie wyników spotkań towarzyszących, tożsamych z dotychczasowymi wysiłkami ABW w zakresie przeciwdziałania zagrożeniom związanym z nieuprawnionym użyciem broni chemicznej i zwalczania ich, należy zaliczyć umiejętności w zakresie:

- przeciwdziałania zamachom na instalacje chemiczne poprzez analizę, ewaluację i identyfikację ewentualnych luk prawnych i proceduralnych, skuteczne wdrażanie oraz skrupulatne egzekwowanie, zgodnie z rzeczową właściwością Agencji, stosownych krajowych i międzynarodowych regulacji w przedmiotowym zakresie,
- prowadzenia skutecznej, wielostronnej współpracy ze służbami specjalnymi oraz organami ochrony porządku publicznego państw członków OPCW oraz aktywnego wspierania działań zmierzających do wskazania i rozpowszechniania praktycznych mechanizmów zwalczania zagrożenia zamachami chemicznymi,
- poszerzania działań prewencyjnych w celu ograniczenia dostępu terrorystów do materiałów mogących posłużyć do produkcji broni chemicznej, przeciwdziałania transferom technologii oraz pozyskiwaniu wiedzy teoretycznej i praktycznej, która mogłaby zostać użyta do rozwoju i produkcji broni chemicznej,
- dalszego pogłębiania współpracy w obrębie OPCW oraz ulepszania praktyk i narzędzi służących realizacji celów Organizacji.

Należy zaznaczyć, że zarówno ćwiczenie, jak i towarzyszące mu spotkania, wskazały wyraźnie, że istnieje potrzeba zintegrowanego podejścia do zagrożeń związanych z nieuprawnionym użyciem broni ABC, oraz że krajowe plany reagowania powinny umożliwiać skuteczną reakcję na całe spektrum takich zagrożeń.

W następstwie ćwiczenia Agencja Bezpieczeństwa Wewnętrznego oraz Rządowe Centrum Bezpieczeństwa zorganizowały spotkanie podsumowujące, przeznaczone dla właściwych rzeczowo podmiotów krajowych oraz przedstawicieli przemysłu, w którego wyniku udało się wypracować szereg rekomendacji odnośnie do zidentyfikowanych przeszkód prawnych i proceduralnych mogących w znacznym stopniu utrudnić, a nawet udaremnić, skuteczną reakcję na zdarzenie kryzysowe opisane w scenariuszu.

Wnioski ABW w przedmiotowym zakresie są następujące:

- Do niewątpliwych zalet ćwiczenia należy zaliczyć jego sztabowy charakter, pozwalający w znacznym stopniu zredukować koszty przedsięwzięcia oraz ograniczenia występujące w przypadku realizacji działań rzeczywistych wynikających z angażowania ludzi i zasobów materiałowych. Jednocześnie należy zaznaczyć, że przeprowadzenie tego typu szkolenia skutkuje brakiem możliwości sprawdzenia niezawodności personelu i sprzętu w sytuacji rzeczywistej. Z uwagi na powyższe, w przyszłości warto rozważyć możliwość włączenia do takich ćwiczeń elementów, które badałyby przedmiotowy zakres. Trzeba podkreślić, że doświadczenia wyniesione z TTEx-01 OPCW wyraźnie wskazują na znaczący potencjał ćwiczeń sztabowych, który może być wykorzystywany w celu pogłębiania współpracy pomiędzy ich uczestnikami, przy jednoczesnym dążeniu do poprawy skuteczności własnych działań i koordynacji dalszych prac. W konsekwencji ćwiczenia sztabowe należy uznać za cenne narzę-

dzie mogące służyć podniesieniu jakości działań administracji publicznej.

- Ewaluacja obowiązujących procedur wskazała na potrzebę pogłębionej koordynacji zarządzania kryzysowego pomiędzy właściwymi rzeczowo instytucjami RP oraz partnerami międzynarodowymi. Szczególnie ważne w tym kontekście będzie podniesienie świadomości odnośnie do charakteru działań odpowiednich organów administracji w sytuacji kryzysowej oraz regulacji, na których podstawie podejmują one działania. Gotowość państwa do skutecznej reakcji na zamach z użyciem toksycznych chemikaliów przemysłowych wymaga prawidłowej oceny zagrożenia, określenia i scharakteryzowania celów wysokiego ryzyka oraz przeglądu krytycznych punktów infrastruktury. Ostatecznie plany zarządzania kryzysowego winny uwzględniać stan prawny RP, delegację ustawową poszczególnych organów administracji oraz ich rzeczywiste możliwości operacyjne, zakres wsparcia gwarantowany przez partnerów międzynarodowych, rozmieszczenie zakładów przemysłowych oraz stan ich zabezpieczenia, gęstość zaludnienia czy istniejącą infrastrukturę. Ważne będzie ponadto ustanowienie pełnej kompatybilności użytkowanych systemów komunikacji oraz spójnego sposobu określania rozmiarów skażenia chemicznego, usprawnienie współdziałania służb w miejscu akcji oraz nawiązanie stałej współpracy z sektorem przemysłowym w celu bezpośredniej wymiany informacji o możliwym zagrożeniu i jego skali.
- Poprawa procedur reagowania kryzysowego nie może odbywać się w izolacji, stąd ważny będzie przegląd bilateralnych, regionalnych i międzynarodowych systemów powiadamiania oraz wsparcia, jak też ewentualne dostosowanie porozumień i umów do umożliwienia udzielenia i uzyskania pomocy w sytuacjach nadzwyczajnych w skali ponadnarodowej. Dodatkowym atutem podjętych przez państwo wysiłków w zakresie podniesienia zdolności reagowania na zamach z użyciem toksycznych chemikaliów będzie ułatwienie i poprawa wzajemnej współpracy zarówno pomiędzy członkami OPCW, jak i między wyżej wymienioną Organizacją ds. Zakazu Broni Chemicznej a sygnatariuszami Konwencji CWC.
- Z uwagi na złożoność problematyki oraz zazębiające się krajowe i międzynarodowe akty prawne, a ponadto często zbieżne kompetencje szeregu organów aktywnych na arenie krajowej, a szerzej także w obrębie OPCW, zasadnym wydaje się utworzenie centralnej bazy wiedzy skupiającej w sposób usystematyzowany wszelkie informacje odnośnie do powyższego. RCB zadeklarowało wolę prowadzenia bazy danych, w której będą gromadzone wnioski i doświadczenia podmiotów krajowych z przeprowadzanych w przyszłości ćwiczeń sztabowych. Wydaje się, że warto rozważyć włączenie do zasobów tego typu bazy aktualnego opracowania na temat schematu działań administracji państwowej w wypadku zagrożenia zamachem przy użyciu broni chemicznej, w szczególności w kontekście zarządzania kryzysowego.
- Ze względu na fakt, że znajdujące się na terenie RP zakłady chemiczne mogą stać się celem ataków lub wypadków mogących prowadzić do uwolnienia toksycznych chemikaliów do środowiska oraz kradzieży lub nabycia tych chemikaliów przez potencjalne grupy ryzyka, szczególnie istotne jest poszerzanie świadomości w tym zakresie i działalność edukacyjna skierowana do decydentów politycznych, przedstawicieli przemysłu chemicznego, ośrodków akademicko-naukowych, a także mediów i opinii publicznej. W związku z powyższym, cenną inicjatywą może być wdrożenie odpowiednich programów szkoleniowych przybliżających przedmiotową problematykę, a także odwołujących się do najlepszych praktyk bezpieczeństwa chemicznego, umiejętności wczesnego rozpoznawania zagrożenia i sposobów reagowania pod-

czas zdarzenia kryzysowego. Z uwagi na szeroko zakrojoną działalność szkoleniową Centralnego Ośrodka Szkolenia ABW w Emowie, jego możliwości dydaktyczne, profesjonalną kadrę, nowoczesne sale konferencyjne oraz zainicjowaną w ostatnim czasie przez COS współpracę z partnerami zagranicznymi warto rozważyć możliwość przeprowadzenia takich szkoleń przez wyżej wymieniony Ośrodek. Współpraca międzynarodowa w tym zakresie mogłaby objąć cykl wykładów wygłaszanych przez ekspertów zaprzyjaźnionych służb specjalnych i organów ochrony porządku publicznego, którzy przybliżyliby obowiązujące na ich terytorium procedury zarządzania kryzysowego i przyjęte strategie komunikacji kryzysowej.

- Mając na uwadze, że zarządzanie kryzysowe w przypadkach podobnych do opisanych w scenariuszu wymaga specjalistycznej wiedzy z zakresu chemii, ważnym elementem jego planowania, a tym samym skutecznego przeciwdziałania zagrożeniu, musi pozostawać ścisła współpraca z ekspertami w tej dziedzinie, w tym z ekspertami zewnętrznymi. W takiej sytuacji warto rozważyć stworzenie platformy współpracy pomiędzy światem akademickim i laboratoriami ABW, OPCW i państw w niej zrzeszonych. Powyższe może w szerszej perspektywie wydatnie wesprzeć wysiłki państwa ukierunkowane na usuwanie skutków zamachu terrorystycznego z użyciem broni chemicznej, a w węższej doprowadzić do udoskonalenia istniejących procedur w zakresie reagowania na wypadki w zakładach przemysłowych lub klęski żywiołowe skutkujące uwolnieniem toksycznych substancji do środowiska. Platforma mogłaby równocześnie służyć do wypracowania kompleksowych rozwiązań, które pozwoliłyby na równoczesne usuwanie skutków zamachu, dokonywanie oględzin i zabezpieczanie śladów w taki sposób, by wysiłki żadnego z zaangażowanych organów nie zostały przypadkowo udaremnione.
- Uregulowania zdają się wymagać również zasady współpracy z mediami. Opracowanie kompleksowej strategii informowania opinii publicznej może bowiem mieć niebagatelne znaczenie dla skuteczności zarządzania kryzysowego. Szczególnie ważna będzie tu dbałość o bieżącą współpracę z mediami, która w sytuacji kryzysowej umożliwi przygotowanie relacji wspierających wysiłki administracji. Dalszym krokiem będzie podniesienie poziomu współpracy ze środkami masowego przekazu osób bezpośrednio zaangażowanych w prowadzenie akcji w miejscu zdarzenia. Dodatkowym atutem przedmiotowych przedsięwzięć o charakterze długofalowym byłoby zwiększenie zaufania społecznego, jako że organy, które potrafią znaleźć dogodne płaszczyzny dialogu z mediami, mogą być odbierane jako partnerzy nowocześni, bliscy społeczeństwu i dbający o jego interesy. W tym kontekście warto rozważyć przyjęcie w obustronnych kontaktach formuły wykraczającej poza ramy tradycyjnego komunikatu prasowego (na rzecz np. wywiadu z szefem urzędu), co dawałoby możliwość uwrażliwiania społeczeństwa na zagrożenia dla bezpieczeństwa państwa, w tym na zagrożenie ewentualnym zamachem terrorystycznym na zakład chemiczny i, co ważniejsze, informowania społeczeństwa o zasadach zachowywania się w sytuacji kryzysowej jeszcze przed jej wystąpieniem.
- Część uczestników ćwiczenia postulowała potrzebę przeprowadzania przyszłych ćwiczeń wyłącznie w języku polskim, motywując to niskim poziomem znajomości języków obcych wśród przedstawicieli polskiej administracji. Argument ten zdaje się być zasadny w odniesieniu do sporej części urzędników państwowych, w związku z czym wskazane wyżej oczekiwania są w pewnej mierze zrozumiałe. Wydaje się jednak, że podjęcie decyzji o przeprowadzaniu przyszłych ćwiczeń wyłącznie w języku polskim byłoby nietrafione z kilku przyczyn. Po pierwsze, skuteczna realizacja ćwicze-

nia pokazała, że właściwe rzeczowo organy administracji RP oraz sektor przemysłu chemicznego dysponują personelem, który może brać udział w tego rodzaju przedsięwzięciach. Po drugie, w przypadku zdarzenia kryzysowego o charakterze transgranicznym, jak to opisane w scenariuszu, organy te zmuszone będą do pracy w języku obcym, najpewniej angielskim, a ćwiczenie musi odzwierciedlać sytuację rzeczywistą. Podobnie nietrafiona wydaje się idea utworzenia centralnej jednostki tłumaczeniowej dla wszystkich służb zaangażowanych w procedurę reagowania na zdarzenie kryzysowe, co miałoby na celu eliminację rozbieżności w tłumaczeniach, które mogłyby stać się podstawą różnic interpretacyjnych i skutkować nieskoordynowanymi działaniami administracji. Niemniej jednak, w przypadku poprawnego przekładu dokumentów użycie synonimów przez tłumaczy poszczególnych służb jedynie powierzchownie wpłynie na treść dokumentu, nie zmieniając jego meritum.

Podsumowując należy podkreślić, że sztabowe ćwiczenie antyterrorystyczne TTEx-01 OPCW umożliwiło pogłębioną analizę obowiązujących procedur reagowania kryzysowego oraz wydatnie przyczyniło się do poprawy koordynacji współpracy pomiędzy właściwymi rzeczowo organami administracji RP. Mając na uwadze podjęte w wyniku ćwiczenia działania na rzecz usunięcia zidentyfikowanych przeszkód prawnych i proceduralnych, które mogłyby w znacznym stopniu utrudnić, a nawet udaremnić skuteczną reakcję na zamach terrorystyczny z użyciem broni chemicznej, należy zaznaczyć, że jego wartość ma charakter długofalowy. Sztabowe ćwiczenia antyterrorystyczne pozostają więc ważnym i skutecznym narzędziem weryfikacji, oceny oraz szkolenia krajowych zasobów reagowania na zdarzenie kryzysowe.

Zdj. 1. Otwarcie ćwiczenia – sesja ministerialna.

Zdj. 2. Od lewej: Z-ca Dyrektora RCB płk Dariusz Góralski, Szef Obrony Przed Bronią Masowego Rażenia gen. bryg. Ryszard Frydrych, Z-ca Szefa ABW płk Paweł Białek i Z-ca Dyrektora Departamentu Polityki Bezpieczeństwa MSZ Marek Szczygieł.

Zdj. 3. Drugi dzień ćwiczenia w COS ABW w Emowie. Od lewej: Lech Starostin – konsultant OPCW (za mównicą), Lesław Górniak – konsultant OPCW, Krzysztof Paturej – Dyrektor Biura ds. Projektów Specjalnych Sekretariatu Technicznego OPCW, mjr Marcin Siuda – Z-ca Dyrektora Centrum Analiz ABW, Katarzyna Madej – Samodzielny Wydział Szkoleń i Ćwiczeń RCB.

Piotr Potejko
Ilona Idzikowska

Międzynarodowy Warsztat Ekspercki pt. *Antyterrorystyczna polityka informacyjna – najlepsze praktyki i wyzwania,* Emów 2011

W dniach 7 - 8 kwietnia 2011 r. w Centralnym Ośrodku Szkolenia Agencji Bezpieczeństwa Wewnętrznego w Emowie odbył się międzynarodowy warsztat ekspercki nt. *Antyterrorystyczna polityka informacyjna – najlepsze praktyki i wyzwania*.

Organizatorami spotkania byli: Szef Agencji Bezpieczeństwa Wewnętrznego gen. bryg. Krzysztof Bondaryk oraz Podsekretarz Stanu w Ministerstwie Spraw Wewnętrznych i Administracji Adam Rapacki. W warsztacie ponadto udział wzięli Zastępca Szefa ABW płk Paweł Białek oraz Podsekretarz Stanu w Ministerstwie Sprawiedliwości Piotr Kluz.

Do wymiany doświadczeń zaproszeni zostali eksperci z państw Grupy G6[1] i Stanów Zjednoczonych, przedstawiciele placówek dyplomatycznych tych państw[2], reprezentanci pionów prasowych służb i instytucji wchodzących w skład polskiego systemu antyterrorystycznego oraz członkowie Zespołu Zadaniowego – Stałej Grupy Eksperckiej działającej przy Międzyresortowym Zespole ds. Zagrożeń Terrorystycznych[3]. O udział w dyskusji poproszono również dziennikarzy oraz reprezentantów Centrum Badania Opinii Społecznej, środowisk naukowych i organizacji pozarządowych.

Moderatorami warsztatów byli:
- Zastępca Dyrektora Departamentu Analiz i Nadzoru MSWiA – Agata Furgała,
- Zastępca Dyrektora Departamentu Unii Europejskiej i Współpracy Międzynarodowej MSWiA – Anna Tulej,
- Zastępca Dyrektora Centrum Antyterrorystycznego ABW – Paweł Chomentowski,
- Zastępca Naczelnika Wydziału III Centrum Antyterrorystycznego ABW – Damian Szlachter,
- Dyrektor COS ABW w Emowie ppłk dr Piotr Potejko.

Obrady otworzył Szef ABW gen. bryg. Krzysztof Bondaryk, który po przywitaniu gości wyraził opinię, iż spotkania w tym gremium powinny doprowadzić do zdiagnozowania najważniejszych wyzwań w zakresie antyterrorystycznej polityki informacyjnej oraz zainspirować szeroką wymianę doświadczeń, istotnych z punktu widzenia bezpieczeństwa wewnętrznego państwa. W swojej wypowiedzi wskazał również na rolę Agencji w zakresie kreowania antyterrorystycznej polityki informacyjnej, szcze-

[1] Grupa sześciu największych państw UE, w której skład wchodzą: Francja, Hiszpania Niemcy, Wielka Brytania, Włochy oraz Polska.

[2] Przedstawiciele placówek dyplomatycznych: Francji – Cohade Pascal i Lora Joanna, Hiszpanii – Correa-Cruz Raul, Niemiec – Guterl Roger, Wielkiej Brytanii – Moody Tim.

[3] Przedstawiciele: Kancelarii Prezesa Rady Ministrów, MSWiA, Ministerstwa Sprawiedliwości, Ministerstwa Spraw Zagranicznych, Ministerstwa Obrony Narodowej, Ministerstwa Finansów, Rządowego Centrum Bezpieczeństwa, Centralnego Biura Antykorupcyjnego, Biura Bezpieczeństwa Narodowego, Policji, Straży Granicznej, Państwowej Straży Pożarnej, Służby Wywiadu Wojskowego oraz Biura Ochrony Rządu.

gólnie przez Centrum Antyterrorystyczne i Departament Przeciwdziałania Terroryzmowi ABW, czego przykładem było przeprowadzenie międzynarodowych ćwiczeń pod nazwą *OFFSIDE 2010*.

Podsekretarz stanu w MSWiA, Adam Rapacki, zwrócił uwagę na zintegrowane podejście administracji rządowej do kwestii zagrożeń terrorystycznych, rekomendowane przez Międzyresortowy Zespół ds. Zagrożeń Terrorystycznych, oraz wskazał na cztery fazy reakcji służb na tego typu zagrożenia, tj. na zapobieganie tym zagrożeniom, ochronę ludności i obiektów, ściganie sprawców aktów terrorystycznych i reagowanie w przypadku otrzymania informacji o zagrożeniu. Minister podkreślił, iż w zależności od wystąpienia konkretnej fazy powinno następować odpowiednie działanie właściwych służb. Wskazał także na niebezpieczeństwo związane ze zbyt szybkim podawaniem przez media do publicznej wiadomości informacji wrażliwych, co może być wykorzystywane przez terrorystów, a jednocześnie powodować panikę wśród społeczeństwa.

Podsekretarz stanu w Ministerstwie Sprawiedliwości, Piotr Kluz, potwierdził wagę i znaczenie antyterrorystycznej polityki informacyjnej oraz przedstawił strukturę resortu sprawiedliwości i jego działania, które mogą mieć istotny wpływ na zwalczanie terroryzmu. Podkreślił przy tym rolę sądów, w których finalizowane są sprawy wszczynane na podstawie dokumentacji operacyjnej.

Po wystąpieniach przedstawicieli kierownictwa służb i instytucji głos zabrał Oscar Jaime, Dyrektor ds. Naukowych w Gabinecie Studiów nad Bezpieczeństwem Wewnętrznym Ministerstwa Spraw Wewnętrznych Królestwa Hiszpanii, które aktualnie sprawuje prezydencję w Grupie G6. Podziękował on stronie polskiej za organizację warsztatu oraz zwrócił uwagę na istotne zagrożenie, jakim jest możliwość wykorzystywania mediów przez terrorystów, m.in. do działań propagandowych.

Następnie Pani Barbara Badora z Centrum Badani Opinii Społecznej przedstawiła diagnozę oczekiwań społecznych wobec instytucji państwowych w zakresie informowania obywateli o ewentualnych zgrożeniach i komunikowania się z nimi w celu zapobiegania zagrożeniom terrorystycznym i reagowania na nie. Przedmiotowa diagnoza jest wynikiem badania przeprowadzonego przez CBOS we współpracy z Wyższą Szkołą Policji w Szczytnie na liczącej 899 osób grupie dorosłych obywateli RP.

Kolejnym wystąpieniem była prezentacja prof. dr hab. Ewy Stasiak-Jazukiewicz z Wydziału Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego[4] dotycząca badania opinii przedstawicieli środowisk dziennikarskich nt. mechanizmów oraz odpowiedzialności za proces przekazywania informacji obywatelom w sytuacji zagrożenia. Prezentowane badanie było przeprowadzone metodą indywidualnego wywiadu pogłębionego (IDI) i objęło dwunastu przedstawicieli środowiska mediów, w tym przedstawicieli najważniejszych polskich dzienników i tygodników, Polskiej Agencji Prasowej oraz Informacyjnej Agencji Radiowej Polskiego Radia.

W ramach obrad warsztaty podzielono na następujące sesje tematyczne:

1. *Spójna antyterrorystyczna polityka informacyjna państwa jako gwarancja skuteczności w zapobieganiu i reagowaniu na zagrożenia terrorystyczne,*
2. *Organy państwa a media – przykłady współpracy w zakresie informowania o zagrożeniach terrorystycznych,*

[4] Agencja Bezpieczeństwa Wewnętrznego i Wydział Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego prowadzą współpracę w ramach porozumienia podpisanego w 2008 r.

3. Profilaktyka antyterrorystyczna – możliwości współpracy ze światem nauki i organizacjami pozarządowymi.

W pierwszej sesji tematycznej Dyrektor Departamentu Analiz i Nadzoru MSWiA, Jacek Zalewski, oraz Naczelnik Wydziału Przeciwdziałania Zagrożeniom Terrorystycznym i Przestępczości Zorganizowanej DAiN MSWiA, Mariusz Cichomski, przedstawili rolę ministra spraw wewnętrznych i administracji w procesie komunikowania się ze społeczeństwem odnośnie do zagrożeń terrorystycznych oraz w kształtowaniu postaw i budowaniu świadomości obywateli dotyczącej natury tych zagrożeń.

Następnie przedstawiciele Agencji Bezpieczeństwa Wewnętrznego – Rzecznik Prasowy ABW, ppłk Katarzyna Koniecpolska-Wróblewska, oraz Dyrektor Centrum Antyterrorystycznego ABW, płk Zbigniew Muszyński – przedstawili prezentację na temat działań ABW w zakresie kreowania polityki informacyjnej dotyczącej zagrożeń terrorystycznych. Podczas prezentacji wskazano na inicjatywy ABW dotyczące informowania społeczeństwa o wyżej wymienionych zagadnieniach, tj. na:

– opublikowany *Raport roczny* stanowiący jawne sprawozdanie z działalności ABW,
– uruchomiony przez Agencję portal internetowy www.antyterroryzm.gov.pl,
– strony internetowe założone przez ABW w ramach ochrony cyberprzestrzeni, których zadaniem jest uświadamianie społeczeństwu potencjalnych zagrożeń związanych z wykorzystaniem internetu i zapoznanie z metodami zabezpieczania się przed nimi (www.cert.gov.pl; www.surfujbezpiecznie.pl).

Jako element zwiększania świadomości społecznej w zakresie zagrożeń terrorystycznych wskazano również zorganizowane w październiku 2010 r. ćwiczenia antyterrorystyczne *OFFSIDE 2010*. Podczas warsztatu zaprezentowano film z realizacji tych ćwiczeń. Jednym z etapów projektu było zorganizowanie czterech seminariów regionalnych poświeconych zapobieganiu zagrożeniom terrorystycznym dla imprez masowych, po których organizowane były briefingi dla mediów. Przedstawiciele ABW podkreślili, iż jednym z zasadniczych elementów zapewnienia bezpieczeństwa podczas zbliżających się Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012 jest właśnie wypracowanie jednolitej strategii informowania na temat ewentualnych zagrożeń terrorystycznych. Przyjęcie takiej strategii pozwalałoby bowiem na uniknięcie potencjalnej paniki i umożliwiłoby służbom odpowiedzialnym za bezpieczeństwo efektywne przeciwdziałanie zagrożeniom.

W tej części spotkania głos zabrał także redaktor Adam Szostkiewicz, zwracając uwagę na to, że w kontekście dyskusji nad antyterrorystyczną polityką informacyjną państwa należy uwzględniać również kulturę danej społeczności. Zaznaczył przy tym, że w Polsce nadal dominuje nieufność wobec instytucji państwowych.

Oficer łącznikowy przy Prezydencji w Radzie UE z ramienia Departamentu Bezpieczeństwa Wewnętrznego Stanów Zjednoczonych, Lauren Nelly Beyer, przedstawiła doświadczenia USA w antyterrorystycznej edukacji społeczeństwa oraz w procesie komunikowania się struktur państwowych z obywatelami w sytuacji zagrożenia terrorystycznego. W szczególności zwróciła uwagę na wdrażaną aktualnie w Stanach Zjednoczonych zamianę pięciostopniowej skali uwzględniającej konkretną kolorystykę poziomów zagrożenia terrorystycznego na system opisowy.

Vincenzo Di Peso, przedstawiciel Centralnej Służby Antyterrorystycznej w Ministerstwie Spraw Wewnętrznych Republiki Włoskiej, zaprezentował doświadczenia Włoch w zakresie antyterrorystycznej polityki informacyjnej, sposób porozumiewania się w sytuacjach zagrożenia w obrębie włoskiego resortu spraw wewnętrznych na poziomie centralnym i lokalnym, jak również wskazał na funkcjonowanie biur prasowych

Ministerstwa Spraw Wewnętrznych, departamentu stanowiącego odpowiednik polskiej Komendy Głównej Policji oraz jednostek organizacyjnych Policji w terenie, jako podmiotów właściwych do komunikacji zewnętrznej resortu.

Następnie głos zabrał ponownie Oscar Jaime, który przedstawił doświadczenia Hiszpanii dotyczące polityki informacyjnej na temat terroryzmu. Zwrócił m.in. uwagę na konieczność kompleksowego podchodzenia do tego zagadnienia w sytuacjach kryzysowych, takich jak chociażby zamachy w Madrycie. Wskazał również na kwestie wrażliwości na tragedię oraz na problem zagadnień politycznych, które w tego rodzaju sytuacjach mogą być forsowane przez władze. W jego opinii, ważne jest również możliwie szybkie informowanie rodzin ofiar o zaistniałym zdarzeniu, aby stosowne informacje docierały do nich, zanim zostaną upublicznione w mediach. Do mediów powinny być przekazywane wyłącznie sprawdzone i potwierdzone wiadomości, które, w opinii Jaime-'a, należy aktualizować nie częściej niż co 2 - 3 godziny, aby nie wprowadzać chaosu.

Ostatnią prezentacją tej sesji tematycznej było wystąpienie insp. Krzysztofa Hajdasa, przedstawiciela Wydziału Prasowego Komendy Głównej Policji, który omówił zasady obsługi medialnej na miejscu zdarzenia kryminalnego oraz praktyczne przykłady współpracy służb i instytucji odpowiedzialnych za kontakty z mediami w sytuacji zagrożenia. Inspektor Hajdas zwrócił m.in. uwagę na to, że w czasach tzw. dziennikarstwa społecznego dziennikarze często otrzymują od obywateli informacje szybciej niż np. rzecznicy służb, którzy w przypadku zaistnienia danego zdarzenia powinni z ramienia właściwych do tego instytucji oficjalnie informować o nim społeczeństwo.

Kolejną sesję tematyczną zatytułowaną *Organy państwa a media – przykłady współpracy w zakresie informowania o zagrożeniach terrorystycznych* rozpoczęły prof. dr hab. Ewa Stasiak-Jazukiewicz i dr Marta Jas-Koziarkiewicz z Wydziału Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego, prezentując wybrane przykłady relacjonowania przez media sytuacji kryzysowych (np. zamachu terrorystycznego lub nieudanej próby jego przeprowadzenia). W ramach przeprowadzonego przez UW badania dokonano ilościowej i jakościowej analizy przekazów medialnych dotyczących następujących przypadków:
– (w Hiszpanii) zamachu w Madrycie z 11 marca 2004 r.,
– (w Wielkiej Brytanii) zamachu w londyńskim metrze z 21 lipca 2005 r.,
– (w Polsce) związanego z porwaniem polskiego geologa w Pakistanie w 2009 r.

W tej samej sesji tematycznej wystąpił przedstawiciel Wielkiej Brytanii John Toker, Dyrektor ds. Komunikacji dla Bezpieczeństwa i Wywiadu, przedstawiając brytyjskie doświadczenia w zakresie polityki medialnej dotyczącej zagrożeń terrorystycznych, w szczególności związane ze wspomnianym wyżej zamachem w londyńskim metrze oraz z działalnością utworzonego wówczas systemu wymiany informacji za pośrednictwem Centrum Koordynacji Informacji. Jednocześnie podkreślił konieczność współpracy z mediami w tego rodzaju sytuacjach. Dotychczas współpraca ta w przypadku Wielkiej Brytanii polegała na:
– wydawaniu oświadczeń dla prasy,
– regularnym zwoływaniu konferencji prasowych,
– organizowaniu tzw. wywiadów jeden na jednego ze wskazanymi rzecznikami,
– organizowaniu pomieszczeń lub obiektów dla przedstawicieli mediów,
– publikowaniu zdjęć i ilustracji związanych z zamachem,
– bieżącym przekazywaniu informacji za pośrednictwem poczty e-mail i stron internetowych,
– organizowaniu briefingów prasowych, tzw. *off the record*,

– służeniu przedstawicielom mediów radą.

W efekcie służbom brytyjskim udało się w relacjach z mediami stworzyć atmosferę zrozumienia i zaufania, czego przykładem były przypadki dobrowolnej rezygnacji dziennikarzy z podawania do publicznej wiadomości niektórych informacji wrażliwych.

Krzysztof Liedel, Zastępca Dyrektora Departamentu Bezpieczeństwa Pozamilitarnego Biura Bezpieczeństwa Narodowego zaprezentował natomiast wyniki programu badawczego Collegium Civitas pn. *Model wykorzystania środków masowego przekazu w przeciwdziałaniu i walce z terroryzmem w warunkach RP*. Zaakcentował przede wszystkim potrzebę właściwego doboru ekspertów, którzy wypowiadają się w mediach, oraz wskazał na fakt, iż zwykle eksperci ci odnoszą się tylko do roszczeń politycznych stojących u podstaw zamachu, natomiast nie dają wskazówek, jak należałoby się zachować w przypadku tego typu zagrożenia. Takie wskazówski mogłyby wpłynąć na kształtowanie pożądanych postaw społecznych.

Anna Marszałek, redaktor „Dziennika Gazety Prawnej", zaangażowała uczestników spotkania w dyskusję na temat współpracy polskich mediów z organami państwa w sytuacji ataku terrorystycznego poprzez symulację fikcyjnego ataku na jedną ze stacji telewizyjnych, podczas którego doszłoby do zatrzymania dziennikarzy w charakterze zakładników. W dyskusję aktywnie włączyli się rzecznicy służb, w tym m.in. Policji i Centralnego Biura Antykorupcyjnego, a także obecni na spotkaniu dziennikarze.

Następnie Roman Osica z Radia RMF FM przedstawił oczekiwania, jakie mogą mieć media w stosunku do instytucji i służb państwowych odpowiedzialnych za bezpieczeństwo państwa w sytuacji, gdy przyjdzie im relacjonować zdarzenie kryzysowe, np. atak terrorystyczny.

Pierwszy dzień warsztatu zakończył podinsp. Andrzej Borowiak, Rzecznik Komendanta Wojewódzkiego Policji w Poznaniu, który również przedstawił analizę przypadków relacjonowania ataków terrorystycznych w mediach i ich wpływ na działania Policji.

W kolejnym dniu warsztatów odbyła się trzecia i ostatnia z zaplanowanych sesji tematycznych nt. *Profilaktyka antyterrorystyczna – możliwości współpracy ze światem nauki i organizacjami pozarządowymi*.

Zastępca Naczelnika CAT ABW, Damian Szlachter, omówił w wystąpieniu wprowadzającym tematykę radykalizacji wybranych grup społecznych w RP oraz przykłady przeciwdziałania rozwojowi tego zjawiska w Holandii. W ramach zaprezentowanego badania ocenie poddano 534 osoby, w tym m.in. uchodźców czeczeńskich wyznania muzułmańskiego, uchodźców będących wyznawcami innych religii, osoby bezwyznaniowe, polskich muzułmanów (w większości Tatarów), Polaków innych wyznań oraz cudzoziemskich studentów różnych wyznań. W ramach prezentacji przedstawiono związki pomiędzy fundamentalizmem religijnym i aprobatą przemocy religijnej i politycznej u wyżej wymienionych grup społecznych i narodowych.

Prof. dr hab. E. Stasiak-Jazukiewicz zaprezentowała zadania i działania organizacji pozarządowych w Polsce przygotowane na wypadek wystąpienia sytuacji krytycznych oraz rolę tych organizacji w systemie informowania społeczeństwa o tego typu zdarzeniach. W swoim wystąpieniu wskazała, iż organizacje pozarządowe działające na rzecz edukacji w zakresie bezpieczeństwa i porządku publicznego mogłyby być wykorzystywane do działań profilaktyczno-edukacyjnych, a w przypadku wystąpienia sytuacji kryzysowej dodatkowo angażowane do działań zapobiegających ewentualnemu chaosowi oraz do ochrony ludności cywilnej.

W dalszej części spotkania omówiono rolę wyższych uczelni w procesie kształtowania pożądanych postaw społecznych, które ujawniają się w sytuacji zagrożenia bezpieczeństwa, w szczególności związanej z terroryzmem.

Do kwestii edukacji antyterrorystycznej, jej aktualnego stanu oraz perspektyw rozwoju odniosła się prof. dr hab. Jadwiga Stawnicka z Uniwersytetu Śląskiego w Katowicach, która zwróciła uwagę na funkcjonujące na tym uniwersytecie kierunki studiów podyplomowych z zakresu chociażby negocjacji w sytuacji kryzysowej. Ponadto poruszyła problem psychospołecznych aspektów terroryzmu, a w szczególności możliwości neutralizacji działań terrorystów poprzez język używany w komunikatach na ich temat.

Z kolei prof. dr hab. Ewa Gruza z Wydziału Prawa i Administracji UW zwróciła uwagę na prowadzone przez tę uczelnię podyplomowe studia z zakresu problematyki przestępczości zorganizowanej i terroryzmu. Studia te są realizowane przy wsparciu merytorycznym i dydaktycznym funkcjonariuszy ABW.

Zastępca Dyrektora CAT ABW, Paweł Chomentowski, podsumowując obrady, zaznaczył między innymi potrzebę międzyinstytucjalnego podejścia do kwestii antyterrorystycznej polityki informacyjnej. Jednocześnie podkreślił niezwykle istotną rolę bieżącej współpracy pomiędzy instytucjami i służbami państwowymi a środowiskiem dziennikarzy, przybierającej m.in. formę spotkań podobnych do niniejszych warsztatów. Dodatkowo wskazał na istotne problemy dotyczące omawianej podczas warsztatów problematyki, w tym na:

– kwestię potrzeby przeprowadzania ćwiczeń antyterrorystycznych z zaangażowaniem społeczeństwa,
– problem dziennikarskiej autocenzury w przypadkach, w których publikacja danej informacji mogłaby stanowić zagrożenie dla bezpieczeństwa,
– potrzebę szkolenia szefów redakcji w zakresie zagrożeń związanych z ewentualnym wykorzystaniem przez terrorystów mediów oraz konieczność prowadzenia antyterrorystycznej polityki informacyjnej, na którą wskazali w ramach dyskusji sami przedstawiciele ŚMP.

Wnioski ogólne, które pojawiały się podczas dyskusji kończącej, dotyczyły potrzeby bieżącej współpracy służb i instytucji polskiego systemu antyterrorystycznego z mediami, w celu stworzenia atmosfery wzajemnego zrozumienia i zaufania. Mogłoby to w konsekwencji sprzyjać kształtowaniu u dziennikarzy postawy autocenzury mającej istotne znaczenie w przypadkach, gdy publikacja danej informacji mogłaby stanowić zagrożenie dla bezpieczeństwa ogólnego. Podkreślono również potrzebę budowania sieci współpracy z mediami jeszcze przed wystąpieniem zdarzenia o charakterze terrorystycznym.

W wypowiedziach przedstawicieli mediów pojawiały się propozycje rozważenia organizacji szkoleń dla dziennikarzy oraz dla szefów redakcji z zakresu: niwelowania propagandowego oddziaływania terrorystów, podnoszenia świadomości społecznej na temat zagrożenia terrorystycznego, budowania społecznego zaufania do organów bezpieczeństwa i porządku publicznego, informowania na temat ryzyka wystąpienia zagrożenia dla bezpieczeństwa publicznego oraz propagowania zasad bezpieczeństwa w życiu codziennym.

Zdj. 1. Od lewej: Szef ABW gen. bryg. Krzysztof Bondaryk, podsekretarz stanu w MSWiA min. Adam Rapacki, podsekretarz stanu w Ministerstwie Sprawiedliwości min. Piotr Kluz.

Zdj. 2. Odlewej:RzecznikprasowyABWppłkKatarzynaKoniecpolska-Wróblewska, Dyrektor Centrum Antyterrorystycznego ABW płk Zbigniew Muszyński, Dyrektor Centralnego Ośrodka Szkolenia ABW ppłk Piotr Potejko, Z-ca Dyrektora Departamentu Analiz i Nadzoru MSWiA Agata Furgała, Z-ca Dyrektora Centrum Antyterrorystycznego ABW kpt. Paweł Chomentowski.

Piotr Durbajło

Porozumienie ABW–NATO

12 kwietnia 2011 r. Szef Agencji Bezpieczeństwa Wewnętrznego gen. bryg. Krzysztof Bondaryk oraz Asystent Sekretarza Generalnego NATO ds. Nowych Wyzwań dla Bezpieczeństwa, ambasador Gabor Iklody podpisali w Kwaterze Głównej NATO porozumienie dotyczące współpracy w zakresie cyberobrony. Porozumienie pomiędzy Krajową Władzą Bezpieczeństwa RP a NATO (*Cyber Defence Management Authority* – CDMA) wskazuje między innymi podmioty i osoby odpowiedzialne po obu stronach za realizację zadań w obszarze *Cyber Defence*, zarówno na poziomie polityczno-koordynacyjnym, jak i techniczno-operacyjnym. Inicjatywa ta usprawni bieżącą współpracę przy zwalczaniu cyberzagrożeń, między innymi poprzez wzajemną wymianę informacji, doświadczeń i dobrych praktyk związanych z reagowaniem na incydenty dotyczące bezpieczeństwa teleinformatycznego. Wyżej wymienione porozumienie reguluje również kwestie związane z ewentualnym wysłaniem przez NATO zespołów szybkiego reagowania w przypadku wystąpienia na terytorium RP ataków cybernetycznych na dużą skalę.

Efektem porozumienia pomiędzy ABW a NATO jest ustanowienie przodującej roli CERT.GOV.PL w zakresie cyberbezpieczeństwa nie tylko w Polsce, ale i u sojuszników NATO leżących w naszym obszarze geopolitycznym. W efekcie doprowadzi to do powstania wspólnej polityki działań, powodującej wzrost bezpieczeństwa i na terytorium konkretnego kraju, i na całym obszarze cyberprzestrzeni. Ambasador Iklody zwrócił się z propozycją, aby to właśnie Polska była centrum kompetencyjnym w sferze cyberbezpieczeństwa dla Europy Środkowo-Wschodniej.

12.04.2011 r. Podpisanie przez Szefa Agencji Bezpieczeństwa Wewnętrznego gen. bryg. Krzysztofa Bondaryka i Asystenta Sekretarza Generalnego NATO ds. Nowych Wyzwań dla Bezpieczeństwa, ambasadora Gabora Iklodya porozumienia dotyczącego współpracy w zakresie cyberobrony.

Marek Szczur-Sadowski

Uroczystość wręczenia Odznaki Honorowej im. gen. Stefana Roweckiego „Grota”

W dniu 6 maja w siedzibie ABW w Warszawie odbyła się uroczysta odprawa z okazji Święta Narodowego Trzeciego Maja. W trakcie uroczystości, oprócz dorocznych awansów na wyższe stopnie oficerskie i odznaczeń państwowych dla funkcjonariuszy, Szef ABW gen. bryg. Krzysztof Bondaryk po raz pierwszy wręczył osobom zasłużonym dla ochrony bezpieczeństwa wewnętrznego państwa i porządku konstytucyjnego Odznaki Honorowe imienia gen. Stefana Roweckiego „Grota”. W akcie wręczania Szefowi ABW towarzyszyła najbliższa żyjąca w kraju krewna Generała, Jego bratanica, Pani prof. Krystyna Rowecka-Trzebicka. *Postanowieniem nr 1/2011 Szefa ABW z dnia 6 kwietnia* Odznaką uhonorowani zostali Szefowie UOP i ABW:

1. Krzysztof Jan Kozłowski
2. Andrzej Stanisław Milczanowski
3. Jerzy Konieczny
4. Piotr Naimski
5. Gromosław Czempiński
6. Jerzy Marian Nóżka
7. Andrzej Kapkowski
8. Zbigniew Włodzimierz Nowek
9. Andrzej Barcikowski
10. Jerzy Mario Kiciński
11. Tomasz Klimek.

Jednocześnie na podstawie wyżej wymienionego *Postanowienia* Odznakę pośmiertnie przyznano:

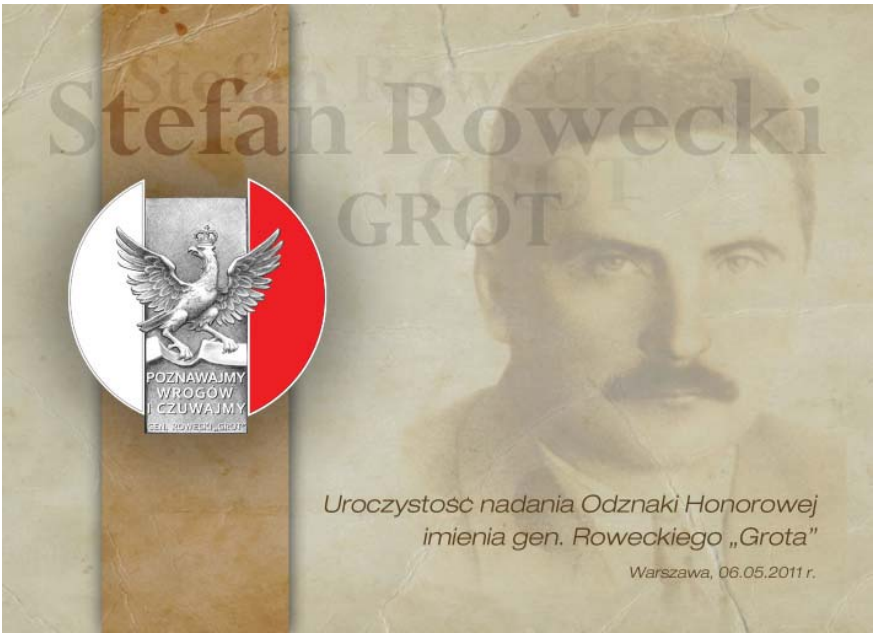
1. Czesławowi Justynowi Cywińskiemu, byłemu Prezesowi Zarządu Głównego Światowego Związku Żołnierzy Armii Krajowej,
2. ks. Tadeuszowi Stefanowi Płoskiemu, byłemu biskupowi polowemu WP,
3. Jerzemu Marianowi Zimowskiemu, wiceministrowi spraw wewnętrznych RP w rządzie T. Mazowieckiego.

Pomysł ustanowienia Odznaki narodził się w trakcie obchodów 20-lecia służb specjalnych suwerennej RP, kiedy to Szef ABW, gen. K. Bondaryk, wyszedł z inicjatywą wyróżniania osób szczególnie zasłużonych dla ochrony bezpieczeństwa państwa specjalną państwową odznaką branżową z przywołaniem w jej nazwie osoby patronującego już Centralnemu Ośrodkowi Szkolenia ABW w Emowie Generała Stefana Roweckiego „Grota”.

W dniu 29 kwietnia 2010 r. ideę ustanowienia Odznaki zaakceptowała Pani prof. Krystyna Rowecka-Trzebicka, a w ślad za Nią Światowy Związek Żołnierzy Armii Krajowej, Klub Kawalerów Orderu Wojennego Virtuti Militari, Instytut im. gen. Stefana „Grota” Roweckiego, a także Rada Konsultacyjna przy COS ABW w Emowie.

Po uzyskaniu we wrześniu 2010 r. zgody Prezesa Rady Ministrów RP Donalda Tuska na podjęcie prac legislacyjnych dotyczących ustanowienia wyżej wymienionego odznaczenia, projekt rozporządzenia w przedmiotowej sprawie skierowano do uzgodnień międzyresortowych. W marcu 2011 r. projekt ten został pozytywnie zaopiniowa-

ny przez: Komisję Heraldyczną, Sejmową Komisję do Spraw Służb Specjalnych oraz Kolegium do Spraw Służb Specjalnych. 1 kwietnia 2011 r. zgodę na ustalenie wzoru i sposobu noszenia Odznaki wyraził Prezydent RP, a 5 kwietnia Premier Donald Tusk podpisał rozporządzenie Rady Ministrów RP w sprawie jej ustanowienia. W tym samym dniu powyższe rozporządzenie zostało opublikowane w Dzienniku Ustaw RP. W jego myśl: (…) § 1.2. *Odznaka jest zaszczytnym, honorowym wyróżnieniem za zasługi położone dla ochrony bezpieczeństwa wewnętrznego państwa i porządku konstytucyjnego.* § 2.1. *Odznaka może być nadana funkcjonariuszom oraz pracownikom Agencji Bezpieczeństwa Wewnętrznego za szczególne osiągnięcia w służbie lub pracy na rzecz ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego* (…) § 2.2. *Odznaka może być nadawana także innym osobom za działanie na rzecz ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego.* (…) § 3.2. *Odznaka może być nadana pośmiertnie* (…) § 7.2. *Odznakę nadaje się z okazji dnia 11 listopada Narodowego Święta Niepodległości lub z okazji dnia 6 kwietnia Święta Agencji Bezpieczeństwa Wewnętrznego.*



Zdj. 1. Wręczenie Odznaki Honorowej Nr 1 pierwszemu Szefowi UOP, Krzysztofowi Kozłowskiemu przez prof. Krystynę Rowecką-Trzebicką (bratanicę gen. Stefana Roweckiego „Grota") i Szefa Agencji Bezpieczeństwa Wewnętrznego gen. bryg. Krzysztofa Bondaryka.

Zdj. 2. Wręczenie Odznaki Honorowej Nr 2 drugiemu Szefowi UOP, Andrzejowi Milczanowskiemu przez prof. Krystynę Rowecką-Trzebicką.

Zdj. 3. Wręczenie Pani Annie Cywińskiej-Kowalewskiej Odznaki Honorowej, pośmiertnie przyznanej Jej Ojcu – Prezesowi Zarządu Głównego Światowego Związku Żołnierzy AK płk. Czesławowi Cywińskiemu.

Zdj. 4. Wręczenie Pani Kazimierze Płoskiej Odznaki Honorowej, pośmiertnie przyznanej Jej Synowi biskupowi polowemu Wojska Polskiego gen. broni Tadeuszowi Płoskiemu.

Agnieszka Zabielska
Michał Wizor

Realizacja przez Agencję Bezpieczeństwa Wewnętrznego projektu pt. *Działania Antyterrorystyczne podczas Międzynarodowych Imprez Sportowych. Rola Narodowych Centrów Antyterrorystycznych*

I. Wstęp

Na podstawie podpisanej 2 czerwca 2010 r. przez Szefa Agencji Bezpieczeństwa Wewnętrznego umowy ABW realizowała projekt pt. *Działania Antyterrorystyczne podczas Międzynarodowych Imprez Sportowych. Rola Narodowych Centrów Antyterrorystycznych*. Przedsięwzięcie to współfinansowane było przez Unię Europejską ze środków Komisji Europejskiej – Dyrekcji Generalnej Spraw Wewnętrznych, w ramach Programu Ramowego Unii Europejskiej na lata 2007 - 2013 *Bezpieczeństwo i ochrona wolności*, w ramach programu *Zapobieganie, Gotowość i Zarządzanie Skutkami Działań Terrorystycznych i innymi rodzajami ryzyka dla bezpieczeństwa w 2009* (CIPS 2009 II).

Agencja Bezpieczeństwa Wewnętrznego po raz pierwszy podjęła starania o przyznanie środków finansowych z funduszy unijnych na realizację swoich projektów. Wniosek Szefa ABW, złożony 1 września 2009 r. do Dyrekcji Generalnej Komisji Europejskiej ds. Sprawiedliwości, Wolności i Bezpieczeństwa, uzyskał w konkursie największą liczbę punktów.

II. Podstawowe założenia projektu

Wśród podstawowych celów wyżej wymienionego projektu należ wymienić wspólne wypracowanie i wdrażanie procedur, instrukcji postępowania oraz trybu reagowania na sytuacje kryzysowe powodowane zamachem terrorystycznym, poprzez zwiększanie skuteczności podejmowanych działań oraz usprawnianie mechanizmów komunikacji wewnętrznej i międzyinstytucjonalnej w wymiarze krajowym i międzynarodowym. W zakres przedsięwzięć wyżej wymienionego projektu weszła analiza rozwiązań prawno-instytucjonalnych dotyczących procedur bezpieczeństwa, ewaluacja procedur, instrukcji powstępowania oraz trybu reagowania na zagrożenia terrorystyczne, seminarium międzynarodowe i konferencja, a także ćwiczenia antyterrorystyczne zakładające wystąpienie zagrożenia podczas międzynarodowej masowej imprezy sportowej.

Uczestnikami ćwiczeń były służby i instytucje zaangażowane w ochronę antyterrorystyczną RP, instytucje ochrony porządku publicznego, służby miejskie oraz porządkowe. Pozwoliło to na realizację założeń scenariusza oraz na przećwiczenie procedur reagowania wszystkich uczestników systemu antyterrorystycznego.

W ćwiczenia zaangażowani byli również partnerzy zagraniczni, których obecność pozwoliła na wymianę doświadczeń. Szczególnie istotna była obecność służby niemieckiej i brytyjskiej, tj. służb państw w przeszłości zaangażowanych w organizację międzynarodowych imprez masowych, oraz obserwatora ćwiczeń – ukraińskiej SBU – służby kraju współorganizatora mistrzostw UEFA EURO 2012.

III. Realizacja projektu

Projekt realizowany był w trzech etapach:

1. *Etap pierwszy – międzynarodowe ćwiczenia antyterrorystyczne i seminarium*

W dniach 11 - 13 maja 2010 r. ABW zorganizowała w Warszawie międzynarodowe ćwiczenia antyterrorystyczne o kryptonimie *OFFSIDE 2010*. Ich uczestnikami oprócz ABW byli: Ministerstwo Spraw Wewnętrznych i Administracji, Komenda Główna Policji, Komenda Główna Straży Granicznej, Rządowe Centrum Bezpieczeństwa, Biuro Ochrony Rządu oraz Komenda Główna Państwowej Straży Pożarnej. Ponadto w działaniach uczestniczyli: Mazowiecki Urząd Wojewódzki, Urząd m.st. Warszawy, Warszawska Straż Miejska i Straż Ochrony Kolei. Partnerami zagranicznymi ćwiczeń byli: Urząd Ochrony Konstytucji (BfV, Niemcy), Rumuńska Służba Kontrwywiadu (SRI, Rumunia) i Departament Bezpieczeństwa Państwowego (VSD, Litwa). Do udziału w ćwiczeniach w roli obserwatorów zaproszeni zostali również przedstawiciele: Centralnej Dyrekcji Wywiadu Wewnętrznego (DCRI, Francja), Służby Bezpieczeństwa Ukrainy (SBU, Ukraina), FBI (USA), policji słowackiej, policji austriackiej i Europolu.

W trakcie seminarium został przedstawiony i omówiony plan dokonania ataku terrorystycznego podczas międzynarodowej imprezy sportowej oraz przeprowadzone zostały ćwiczenia. Następnie ćwiczenia te zostały podsumowane i zaprezentowano wstępne wnioski z ich przebiegu.

Wnioski z ćwiczeń

Podstawowym założeniem przyjętym przez organizatorów projektu było sprawdzenie w praktyce funkcjonowania obiegu informacji między podmiotami systemu antyterrorystycznego RP. Weryfikacji poddane zostały procedury działania w sytuacji zagrożenia terrorystycznego oraz praktyczny wymiar współpracy w ramach utworzonego sztabu kryzysowego.

Realizacja ćwiczenia *OFFSIDE 2010* i określone na ich podstawie słabe i silne strony koordynacji ochrony antyterrorystycznej w Polsce stanowiły podstawę do sformułowania szeregu wniosków.

Za podstawowy warunek skutecznego obiegu informacji uznano konieczność precyzyjnego zdefiniowania zadań oraz weryfikację procedur współdziałania operacyjno-rozpoznawczego. Optymalizacja podziału kompetencji oraz sprawnie funkcjonujące procedury pozwalają bowiem na skrócenie i przyspieszenie procesu decyzyjnego, umożliwiając dopasowanie działań do dynamiki zdarzeń.

W przypadku organizacji sztabu terenowego oraz podejmowania działań na miejscu zdarzenia o charakterze terrorystycznym, elementem niezbędnym jest zintegrowanie dowodzenia oraz jasne określenie zakresu kompetencji służb i instytucji operujących w danym miejscu. Pozwoli to uniknąć zarówno dublowania się kompetencji i realizowanych czynności, jak i tworzenia „białych plam odpowiedzialności" (*responsibility gaps*), kiedy to dany obszar nie zostaje zabezpieczony przez żadną z zaangażowanych służb.

Aby osiągnąć optymalny poziom skoordynowania działań oraz zapewnić prawidłowy stopień poinformowania zaangażowanych podmiotów, niezbędnym jest wypra-

cowanie w najbliższej przyszłości jednolitego systemu łączności, kompatybilnego dla wszystkich uczestników systemu antyterrorystycznego w Polsce. W szczególności dotyczy to ujednolicenia i zintegrowania środków łączności opartych na technologiach analogowych i cyfrowych, które w chwili obecnej wzajemnie nie współpracują. Powyższe zagadnienie dotyczy zarówno służb porządku publicznego, jak i służb specjalnych.

Wnioski płynące ze zrealizowanych ćwiczeń oraz dobre praktyki, z racji profilu przeprowadzonych działań oraz wysokiego stopnia realizmu scenariusza, posłużą do podniesienia poziomu bezpieczeństwa w trakcie polskiej prezydencji w Unii Europejskiej w 2011 r. oraz podczas Mistrzostw Europy w Piłce Nożnej UEFA EURO 2012.

2. *Etap drugi – seminaria regionalne*

Istotnym elementem projektu, mającym na celu rozpowszechnienie doświadczeń zdobytych podczas ćwiczeń *OFFSIDE 2010*, był cykl seminariów regionalnych z zakresu bezpieczeństwa wewnętrznego i zarządzania kryzysowego przeznaczonych dla przedstawicieli administracji publicznej w miastach-gospodarzach turnieju EURO 2012. Odbyły się one przy współudziale Urzędów Wojewódzkich, które logistycznie wsparły to przedsięwzięcie.

Seminaria odbyły się w marcu we Wrocławiu, w Gdańsku, Poznaniu i w Warszawie. Łącznie uczestniczyło w nich ok. 400 przedstawicieli administracji rządowej i samorządowej, służb specjalnych i służb ochrony porządku publicznego. Wystąpiło ok. 50 prelegentów – specjalistów i ekspertów z zakresu bezpieczeństwa imprez masowych, bezpieczeństwa wewnętrznego i zarządzania kryzysowego. Przedsięwzięcie spotkało się z dużym zainteresowaniem mediów. W organizowanych podczas seminariów briefingach wzięło udział łącznie 75 przedstawicieli lokalnej prasy i rozgłośni radiowych.

W zamierzeniu realizatorów projektu wiedza zdobyta w toku współpracy służb i instytucji i zweryfikowana w praktyce podczas ćwiczeń stanowi podstawę skutecznej prewencji antyterrorystycznej. Wnioski płynące z przedsięwzięcia są istotne, w szczególności w kontekście zbliżającej się bezprecedensowej w skali kraju imprezy masowej, jaką będzie EURO 2012. Narzędziem służącym propagowaniu tej wiedzy, zdobytych doświadczeń, rekomendacji i dobrych praktyk stały się seminaria regionalne .

W zakres prezentowanych podczas seminariów treści weszły podstawowe informacje dotyczące struktury polskiego systemu ochrony antyterrorystycznej, zarówno na poziomie decyzyjnym, wykonawczym, jak i koordynacyjnym, realizowanym przez CAT ABW. Innym zagadnieniem poruszonym podczas seminariów było omówienie aktualnego stanu zagrożeń terrorystycznych w RP, ze szczególnym uwzględnieniem potencjalnego ryzyka związanego z terroryzmem wymierzonym w imprezy masowe. Jednocześnie wiele miejsca poświęcono przybliżeniu zasad funkcjonowania procedur przeciwdziałania zagrożeniom terrorystycznym w ramach innych podmiotów, m.in. Straży Granicznej, Policji czy Straży Ochrony Kolei. Osobną kwestią stanowiącą ważny składnik prezentowanej podczas spotkań wiedzy, były zagadnienia związane z ochroną infrastruktury krytycznej oraz szeroko pojętym zarządzaniem kryzysowym, w tym uwzględniającym aspekty ochrony ludności podczas masowych imprez sportowych.

Wśród najczęściej wymienianych przez uczestników seminariów wniosków była konieczność stworzenia platformy wymiany informacji z przedstawicielami podmio-

tów i instytucji uczestniczących w systemie antyterrorystycznej ochrony RP na szczeblu terenowym. Ponadto uczestnicy zwracali uwagę na możliwość wykorzystania CAT ABW w działaniach związanych z zagrożeniem terrorystycznym na poziomie zarówno krajowym, jak i lokalnym. Szeroko dyskutowanym zagadnieniem była również potrzeba wypracowania polityki informacyjnej oraz kontaktów ze społeczeństwem.

3. *Etap trzeci – międzynarodowa konferencja*

Elementem systematyzującym i upubliczniającym całość zdobytych doświadczeń i informacji, a zarazem podsumowaniem unijnego projektu, była międzynarodowa konferencja, która odbyła się w dniach 25 - 26 maja 2011 r. Było to oficjalne spotkanie przedstawicieli polskich służb i instytucji odpowiedzialnych za bezpieczeństwo państwa i porządek publiczny z partnerami zagranicznymi z Europejskiego Urzędu Policji (EUROPOL-u) Litwy, Rumunii, Niemiec, Ukrainy, Węgier i Grecji.

Zorganizowanie konferencji w kilka miesięcy po przeprowadzeniu ćwiczeń *OFFSIDE 2010*, stanowiących główny element projektu, pozwoliła organizatorom i partnerom na kompleksowe i dogłębne przeanalizowanie dorobku informacyjnego powstałego w tym czasie. W rezultacie, spotkanie konferencyjne na szczeblu *heads of units* stało się formalną platformą, na której zaprezentowane zostały finalne efekty całości projektu.

IV. Podsumowanie

Stojące przed Polską wyzwania najbliższych kilkunastu miesięcy, a przede wszystkim przewodnictwo naszego kraju w Radzie Unii Europejskiej w drugiej połowie 2011 r. oraz Mistrzostwa Europy w Piłce Nożnej UEFA EURO 2012, które zostaną zorganizowane latem 2012 r., stanowią ważny impuls do praktycznej weryfikacji i ewaluacji procedur współdziałania służb i instytucji zaangażowanych w przeciwdziałanie i zwalczanie terroryzmu. Realizowany przez ABW projekt unijny, w tym w szczególności ćwiczenia *OFFSIDE 2010* dowiodły, że głównym elementem skutecznego funkcjonowania systemu antyterrorystycznego jest efektywna współpraca wszystkich zaangażowanych podmiotów. Zastosowanie scenariusza ćwiczeń opartego na realnych założeniach, połączone z usystematyzowaniem pozyskanej wiedzy i doświadczeń, pozwoliło na wypracowanie katalogu wniosków i rekomendacji oraz na ich wdrożenie, które jest kolejnym etapem projektu przyczyniającym się do zwiększenia poziomu bezpieczeństwa naszego kraju.

Podkreślenia wymaga fakt, iż zrealizowane przez ABW przedsięwzięcie pozwoliło także na ukazanie silnych stron podmiotów zaangażowanych w działania antyterrorystyczne, takich jak wysoki poziom wyszkolenia, umiejętność wdrażania różnorodnej i specjalistycznej wiedzy oraz duże zaangażowanie uczestników. Wykorzystanie tych cech wraz z ich wsparciem poprzez wprowadzenie wypracowanych rekomendacji pozwoli w sposób maksymalnie efektywny zmierzyć się ze stojącymi przed naszym krajem wyzwaniami.

Zdj. 1. Funkcjonariusze ABW podczas ćwiczeń *OFFSIDE 2010*.

Zdj. 2. Funkcjonariusze ABW podczas ćwiczeń *OFFSIDE 2010*.

Zdj. 3. Mazowiecki Urząd Wojewódzki – Warszawa, 29.03.2011 r. Seminarium poświęcone projektowi ABW pt. *Działania antyterrorystyczne podczas międzynarodowych imprez sportowych. Rola Narodowych Centrów Antyterrorystycznych*.
Konferencja prasowa Z-cy Szefa ABW płk. Pawła Białka.

Zdj. 4. Konferencja międzynarodowa pt. *Działania antyterrorystyczne podczas międzynarodowych imprez sportowych. Rola Narodowych Centrów Antyterrorystycznych*. Warszawa, 25 - 26.05.2011 r.
Przemawia Szef ABW gen. bryg. Krzysztof Bondaryk.

O autorach

About the Authors

Brunon Czabok, płk, Zastępca Dyrektora Departamentu Zabezpieczenia Technicznego Agencji Bezpieczeństwa Wewnętrznego.
Piotr Durbajło, kpt., Zastępca Dyrektora Departamentu Bezpieczeństwa Teleinformatycznego Agencji Bezpieczeństwa Wewnętrznego.
Fabiana Fetke, kpt., Zastępca Dyrektora Departamentu Kontrwywiadu Agencji Bezpieczeństwa Wewnętrznego.
Wojciech Filipkowski, dr, Wydział Prawa Uniwersytetu w Białymstoku.
Jacek Gawryszewski, ppłk, Agencja Bezpieczeństwa Wewnętrznego.
Mirosław Grabowiecki, kpt., Dyrektor Gabinetu Szefa Agencji Bezpieczeństwa Wewnętrznego.
Piotr Herman, kpt., Agencja Bezpieczeństwa Wewnętrznego.
Ilona Idzikowska, Ministerstwo Spraw Wewnetrznych i Administracji.
Krzysztof Izak, mjr, Agencja Bezpieczeństwa Wewnętrznego.
Artur Jasiński, dr inż. arch., Wydział Architektury i Sztuk Pięknych Krakowskiej Akademii im. Andrzeja Frycz Modrzewskiego.
Krzysztof Jurczuk, mjr, Agencja Bezpieczeństwa Wewnętrznego.
Jacek Kędzierski, ppłk, Agencja Bezpieczeństwa Wewnętrznego.
Rafał Leśkiewicz, dr, p.o. Dyrektora Biura Udostępniania i Archiwizacji Dokumentów IPN.
Ryszard Lonca, ppłk WP w stanie spoczynku.
Jacek Mąka, płk, Zastępca Szefa Agencji Bezpieczeństwa Wewnętrznego.
Michał Młotek, kpr., Agencja Bezpieczeństwa Wewnętrznego.
Kazimierz Mordaszewski, płk, Dyrektor Biura Prawnego Agencji Bezpieczeństwa Wewnętrznego.
Robert Osek, ppłk, Dyrektor Biura Ewidencji i Archiwum Agencja Bezpieczeństwa Wewnętrznego.
Antoni Podolski, b. Wiceminister Spraw Wewnętrznych i Administracji, b. Dyrektor Rządowego Centrum Bezpieczeństwa.
Piotr Potejko, dr, ppłk, Dyrektor Centralnego Ośrodka Szkolenia Agencji Bezpieczeństwa Wewnętrznego w Emowie.
Kamila Sacewicz, por., Agencja Bezpieczeństwa Wewnętrznego.
Marcin Siedlarz, st. kpr., Agencja Bezpieczeństwa Wewnętrznego.
Jerzy Stańczyk, dr, Uniwersytet Przyrodniczo-Humanistyczny w Siedlcach.
Alfred Staszak, dr, Prokurator Okręgowy w Zielonej Górze.
Włodzimierz Suleja, prof. dr hab., Dolnośląska Szkoła Wyższa we Wrocławiu.
Marek Szczur-Sadowski, ppłk, Agencja Bezpieczeństwa Wewnętrznego.
Aleksandra Tucholska-Lenart, dr, ppłk w stanie spoczynku, Polskie Towarzystwo Kryminalistyczne.
Maria Wągrowska, Wiceprezes Zarządu Stowarzyszenia Euro-Atlantyckiego, Doradca Dyrektora Rządowego Centrum Bezpieczeństwa.
Michał Wizor, st. kpr., Agencja Bezpieczeństwa Wewnętrznego.
Katarzyna Wojtaszyn, kpt., Agencja Bezpieczeństwa Wewnętrznego.
Agnieszka Zabielska, por., Agencja Bezpieczeństwa Wewnętrznego.