Nr 2 (2) 2010

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

ISSN 2080-1335

AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO

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

PRZEGLĄD BEZPIECZEŃSTWA WEWNĘTRZNEGO

Recenzja naukowa prof. dr hab. Brunon Hołyst

WARSZAWA 2 (2) 2010

INTERNAL SECURITY REVIEW

Reviewer Prof. dr hab. Brunon Hołyst

WARSZAWA 2 (2) 2010

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
tel. (+48) 22 58 58 667
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

Contests

Piotr Potejko
Piotr Tchorzewski

Od Redakcji

Szanowni Państwo,

przedstawiamy drugi numer „Przeglądu Bezpieczeństwa Wewnętrznego", zawierający studia i analizy wybranych aspektów szeroko rozumianego zagadnienia terroryzmu. Recenzji naukowej dokonał prof. dr hab. Brunon Hołyst, wybitny przedstawiciel polskiej nauki, specjalizujący się w takich dziedzinach, jak: kryminalistyka, kryminologia, profilaktyka społeczna, suicydologia, wiktymologia i terroryzm.

Zbiór tekstów zamieszczonych w tym numerze „Przeglądu" jest wyrazem interdyscyplinarnego ujmowania problematyki terroryzmu. Autorzy przedstawiają oblicza tego zjawiska, posługując się pojęciami i metodami analizy stosowanymi przez różne dyscypliny nauk humanistycznych i technicznych. Na szczególną uwagę zasługują opracowania dotyczące: analizy zamachów terrorystycznych (Wojciech Filipkowski i Ryszard Lonca), terroryzmu morskiego (Piotr Mickiewicz), zagrożeń bezpieczeństwa w ujęciu kryminologicznym (Katarzyna Laskowska) oraz ochrony infrastruktury krytycznej RP wobec zagrożeń asymetrycznych (Tomasz Szewczyk i Maciej Pyznar).

Czasopismo skierowane jest do jednostek administracji państwowej, w których kompetencjach leży zapewnienie bezpieczeństwa oraz do pracowników naukowych i studentów, zajmujących się bezpieczeństwem.

„Przegląd" został opracowany na podstawie materiałów jawnych, a opinie zawarte w artykułach są wyłącznie opiniami ich autorów.

Zasady redakcyjne dostepne są na stronie www.abw.gov.pl.

Foreword

Issue no. 2 of "Internal Security Review" includes research and analyses referring to the chosen aspects of the broadly recognised problem of terrorism. Scientific review has been prepared by Professor Brunon Hołyst, a distinguished representative of the Polish world of scholarship, an expert on such fields of science as criminal investigation techniques, criminology, social prophylaxis, suicidology, victimology and terrorism.

Articles selected for this issue of "Internal Security Review" exemplify the interdisciplinary attitude towards the problem of terrorism. The authors present different aspects of terrorism using the terms and analysis methods applied by different fields of science, such as humanities and technical sciences. We particularly recommend articles concerning: analysis of terrorist attempts (by Wojciech Filipkowski and Ryszard Lonca), marine terrorism (by Piotr Mickiewicz), threats to security from the criminological point of view (by Katarzyna Laskowska) and protection of critical infrastructure of the Republic of Poland vs. asymmetrical threats (by Tomasz Szewczyk i Maciej Pyznar).

The present publication is directed to government administration, particularly dealing with ensuring security, as well as to researchers and students analysing the issue of security.

We notify that "Internal Security Review" has been prepared on the basis of unclassified materials and all opinions given in the articles published in the present issue are solely the opinions of their authors.

I.
TERRORYZM

Wojciech Filipkowski
Ryszard Lonca

Analiza zamachów samobójczych w aspekcie kryminologicznym i prawnym. Cz. I

I. Zagadnienia wprowadzające

W opracowaniu podjęto próbę przedstawienia terrorystycznych zamachów samobójczych rozumianych jako zagrożenia, przed którymi praktycznie nie można się uchronić ani obronić[1)]. Aktualnym przykładem tego zjawiska jest samobójczy atak dokonany 30 grudnia 2009 r. w najważniejszej bazie CIA oraz w centrum jej dowodzenia w Afganistanie. Sprawcą okazał się afgański informator wywiadu amerykańskiego, prawdopodobnie przewerbowany przez Talibów, który zdołał wejść do sali odpraw i tam zdetonować ładunek wybuchowy wśród przyjmujących go oficerów CIA. W eksplozji zginęło siedmiu oficerów, w tym pomagający im oficer jordańskiego wywiadu. Zamach ten uznano za jeden z najpoważniejszych ciosów zadanych amerykańskiemu środowisku wywiadowczemu. Po tym i innych spektakularnych atakach samobójczych, dokonanych pod koniec 2009 r. w Afganistanie i Pakistanie, eksperci ds. walki z terroryzmem uznali, że samobójczy zamach bombowy jest „śmielszą i bardziej skuteczną operacją zakończoną sukcesem" niż zamach uliczny. Poza tym stwierdzili, że taka forma ataku zwiększa wśród różnego rodzaju ekstremistów islamskich poszanowanie dla organizacji, która zdołała go przeprowadzić[2)].

Ostatni i poprzednie ataki samobójcze dowiodły, że przeciwdziałanie terroryzmowi samobójczemu jest szczególnym wyzwaniem dla służb odpowiedzialnych za jego zwalczanie z racji nie tylko groźnych i natychmiastowych skutków materialnych dla poszkodowanych i propagandowych dla sprawców, ale też z powodu wybuchu ewentualnej paniki w zbiorowości ludzkiej, którą może wywołać nawet fałszywy sygnał o obecności terrorysty-samobójcy. Plotka o obecności terrorysty-samobójcy rozpowszechniona 30 sierpnia 2005 r. wśród tysięcy szyickich pielgrzymów przekraczających most w Bagdadzie spowodowała panikę, a w jej wyniku śmierć co najmniej 800 Irakijczyków[3)].

[1)] Do 30 grudnia 2009 r. jako przykład podawano spektakularny atak samobójczy dokonany 12 kwietnia 2007 r. w irackim parlamencie przez ochroniarza jednego z sunnickich deputowanych w tzw. Zielonej Strefie, (obszarze najbardziej chronionym w Iraku przez siły amerykańskie). Sprawca zdetonował nasobny pas z materiałem wybuchowym w porze lunchu. Zamachowiec-samobójca zabił osiem osób, w tym trzech parlamentarzystów. Zob. R. Kostrzyński, *Eksplozja w irackim parlamencie*, „Rzeczpospolita" z dnia 12.04.2007.

[2)] Informacje przekazane przez CNN w dniu 4.01.2010. i powielone przez serwisy internetowe pt.: *Kłótnia o straszny cios zadany Ameryce*, Onet.pl w dniu 5.01.2010.

[3)] Por. *Tysiąc ofiar tragedii w Bagdadzie*, „Gazeta Wyborcza" z dnia 1.09.2007. http://wyborcza.pl/1,75248,2895118.html. W 2007 r. pracownicy firmy ochroniarskiej Blackwater, konwojując ulicami Bagdadu VIP-a ulegli panice na widok domniemanego terrorysty-samobójcy jadącego samochodem i otworzyli niekontrolowany ogień. Skutkowało to zabiciem 17 przypadkowych Irakijczyków. Podobny przypadek miał miejsce w listopadzie 2007 r. podczas wizyty 18 afgańskich parlamentarzystów w cukrowni w Baghlanie (Afganistan). Ochrona delegacji otworzyła ogień do domniemanego terrorysty-samobójcy, w wyniku czego zginęło co najmniej 40 osób, a około 120 zostało rannych. Wśród ofiar śmiertelnych było sześciu afgańskich deputowanych ochranianych przez siły afgańskie.

Z punktu widzenia kryminologii i prawa karnego terroryzm samobójczy jest zjawiskiem zorganizowanym. Terrorysta czuje się zobowiązany wobec grupy, swojego społecznego systemu i wspólnego losu. Z tej przyczyny tematem rozważań jest m.in. relacja między samobójcami, a grupą o charakterze terrorystycznym. Grupa stosująca terroryzm samobójczy jest, w przeciwieństwie do jego tradycyjnej odmiany, głęboko motywowana i to na różne sposoby. Z tego względu stanowi szczególny rodzaj zagrożenia w kontekście trudności w identyfikowaniu potencjalnych sprawców i podejmowaniu działań o charakterze prewencyjnym. Należy podkreślić, że terroryzm samobójczy wywołuje u atakowanych społeczności nie tylko poczucie wysokiego zagrożenia, ale też stan bezsilności władz. Coraz częściej staje się również metodą stosowaną w konfliktach militarnych, religijnych i politycznych, po którą sięgają strony najbardziej upokorzone i zdesperowane ponoszonymi klęskami.

Istotnym utrudnieniem dla autorów tej pracy jest brak rzetelnych i wiarygodnych materiałów źródłowych, na podstawie których można by było przeprowadzić niezbędne analizy i sformułować obiektywne wnioski. Podmioty władzy państwowej często przekazują opinii publicznej takie informacje dotyczące terroryzmu, które służą socjotechnice i pozwalają manipulować mediami, a za ich pośrednictwem społecznościami. Jest to także element wojny psychologicznej z samymi terrorystami. Manipulowana jest w dodatku nie tylko opinia publiczna, ale i politycy, a nawet wymiar sprawiedliwości. Retoryka socjotechniki ma zakodować w ich świadomości, że źródła rządowe publikują jedynie prawdziwe informacje, które są potem bezkrytycznie wykorzystywane w ocenach i analizach. Manipulacje takie polegają na tym, że politycy, media, naukowcy itp. otrzymują od służb zwalczających terroryzm spreparowane informacje o terrorystach lub zagrożeniach terrorystycznych[4]. Tego typu wiadomości są następnie publikowane jako tzw. przecieki informacji tajnych. Pozwala to przedstawicielom władz państwowych powoływać się następnie na te – celowo wcześniej ujawnione – dane i potwierdzać ich prawdziwość. W efekcie otrzymujemy najczęściej zniekształcony pogląd na wszystkie aspekty terroryzmu, w tym samobójczego. Dla odcięcia mediów od dostępu do informacji na temat ataków terrorystycznych, głównie samobójczych, służby amerykańskie stworzyły, m.in. w Iraku i Afganistanie, specjalne bariery formalno-prawne[5]. Ujawnianie przez podmioty państwowe nieprawdziwych i zmanipulowanych informacji o terroryzmie sprawia, że powstają też fałszywe bazy wiedzy o tym przedmiocie, wykorzystywane potem do pisania przez ośrodki naukowe lub organizacje pozarządowe ocen i analiz, czy też formułowania wniosków i prognozowania zagrożeń. Takie dokumenty stworzone na zmanipulowanej bazie informacyjnej służą potem często jako argumenty do zmian systemu prawa, ograniczania swobód i praw obywatelskich, a tak-

[4] Ofiarą takiej manipulacji i insynuacji w kwestii powiązań Saddama Husajna z Al-Kaidą stał się nawet Georg Tenet, szef Centralnej Agencji Wywiadowczej w latach 1997-2004, który sam dostarczył administracji amerykańskiej rzekomo niepodważalnych dowodów dotyczących zagrożenia terrorystycznego USA ze strony reżimu irackiego.

[5] Proamerykański rząd iracki specjalnym rozporządzeniem z 13 maja 2007 r. zakazał wszystkim dziennikarzom pracującym w Iraku dostępu do miejsc zamachów (szczególnie samobójczych) przez godzinę od momentu ich zaistnienia. Zakaz ten ma na celu ograniczenie nadawania przez media „niepożądanych informacji", stwarzających warunki do manipulowania nimi. Wiadomość tę podał w Internecie amerykański Komitet Ochrony Dziennikarzy (CPJ) i wezwał do zniesienia nałożonych restrykcji. W liście CPJ napisano: *To dziennikarze, a nie rządy powinni decydować, czy historia jest zbyt niebezpieczna do opisania*. Zob. informacja zamieszczona w portalu Onet.pl. w dniu 22.05.2007 r.

że realizacji określonych celów w polityce wewnętrznej i zewnętrznej państwa[6]. Manipulację faktami stosują też organizacje terrorystyczne.

Pomimo tych trudności eksperci i naukowcy sformułowali szereg teorii i prognoz na temat zagrożeń terrorystycznych, które zostały uwzględnione w tej pracy. Pewnym rodzajem trudności w prowadzeniu rozważań na temat aspektów terroryzmu samobójczego są braki w wiedzy naukowej i faktograficznej o zamachowcach z powodu samej natury śmierci samobójczej.

II. Geneza i ewolucja terroryzmu samobójczego

Ścisły związek między samobójstwem i terroryzmem współczesnym istnieje od ponad 30 lat[7]. Jest to rezultat ciągłego poszukiwania przez organizacje terrorystyczne najbardziej efektywnych metod atakowania przeciwnika. Taką metodą jest właśnie terroryzm samobójczy[8].

W literaturze przedmiotu przyjmuje się, że współczesny samobójczy terroryzm islamski zaistniał 11 listopada 1982 r. w Libanie. Zastosowano go wówczas jako asymetryczny środek walki przeciwko agresji Izraela na ten kraj[9]. W tym dniu (święto narodowe Libanu) 17-letni Ahmad Kassir wjechał samochodem z materiałami wybuchowymi w ośmiopiętrowy budynek izraelskich władz okupacyjnych w Tyrze. W zamachu

---

[6] Przykładem takiego manipulowania był rozpoczęty w maju 2007 r. w Miami proces José Padilly. Prokurator generalny USA, John Ashcroft, na konferencji w dniu 2002 r. informował, że J. Padilla, który należał do latynoskiego gangu z Chicago, a potem przeszedł na islam i związał się z ekstremistami Al-Kaidy, przygotował nie tylko eksplozję tzw. brudnej bomby, ale też ładunków klasycznych i gazu w dziewięciu apartamentowcach na Florydzie oraz atak chemiczny na centra handlowe. Dopiero podczas procesu karnego ujawniono, że służby, zatrzymując J. Padillę, nie dysponowały żadnymi dowodami świadczącymi o przygotowanych przez niego zamachach. Dla ich zdobycia zastosowały wobec oskarżonego tortury, w wyniku których ujawnił oczekiwane informacje. Informacje te posłużyły następnie do działań propagandowych. Ostatecznie J. Padillę oskarżono tylko o prawdopodobne naradzanie się z dwoma arabskimi wspólnikami w sprawie pozyskiwania pieniędzy dla grup muzułmańskich w Kosowie, Czeczenii, Libanie i Somalii oraz co do możliwości rekrutacji ludzi do walki w tych krajach z USA. Szerzej zob. M. Gadziński, *Już nie straszą Ameryki José Padillą*, „Gazeta Wyborcza" z dnia 17.05.2007 r. Zob. także N. Abrams, *Developments in US Anti-terrorism Law, Checks and Balances Undermined*, „Journal of International Criminal Justice" 2006, nr 4, s. 1117 i nast.

[7] Zakorzenione w kulturze islamskiej ataki samobójcze stosowali Sudańczycy z ruchu Mahdiego, walczący przeciw brytyjskim kolonistom w latach 80. XIX wieku. Bojownicy-samobójcy pojawili się również w latach 50. XX wieku w Malezji, stosując samobójcze zamachy przeciw Brytyjczykom. Młodzi żołnierze-samobójcy byli też wykorzystywani przez przywódców irańskich w wojnie z Irakiem w latach 80. ubiegłego wieku. Irańskim samobójcom walczącym na froncie z Irakiem autorytety religijne i polityczne tłumaczyły, że ich poświęcenie służy nie tyle zwycięstwu w wojnie z Irakiem, ile obronie Iranu przed USA i Zachodem, które skłoniły Bagdad do konfrontacji z Teheranem. W Czeczenii pierwsi kamikadze pojawili się zimą 1993/1994 wśród obrońców Groznego. Byli to młodzi ludzie, często dzieci, którzy z plecakami wypełnionymi materiałami wybuchowymi wysadzali się pod rosyjskimi czołgami.

[8] Nowym zjawiskiem jest samobójczy terroryzm morski. Zamachowcy-samobójcy, posługując się małymi jednostkami wyładowanymi silnymi materiałami wybuchowymi, mogą skutecznie atakować nawet duże obiekty pływające. Przykładem jest spektakularny atak na nowoczesny niszczyciel USS „Cole" w jemeńskim porcie Aden, przeprowadzony w październiku 2000 roku. Zob. W. Wosek, *Zagrożenia terroryzmem morskim z uwzględnieniem infrastruktury przemysłowej aglomeracji nadmorskiej* w: J. Szafrański, J. Kosiński (red.), *Współczesne zagrożenia terrorystyczne oraz metody ich zwalczania*, Wydaw. Wyższej Szkoły Policji, Szczytno 2007, s. 132 i nast.

[9] Bennazir Bhutto, która sama zginęła 27 grudnia 2007 r. prawdopodobnie w wyniku ataku samobójczego, będąc premierem Pakistanu napisała: *Islamski ekstremizm i terroryzm samobójczy zaczął się kształtować w konfrontacji muzułmanów z Izraelem i USA właśnie na Bliskim Wschodzie*. Zob. G. Złotow, *Rąbcie drzewa z korzeniami*, „Argumenty i Fakty" 2001, nr 41.

zginęło 141 osób. Rok później, 23 października 1983 r., w ataku na amerykańskie koszary w pobliżu Bejrutu, zginęło 241 żołnierzy USA[10]. Koszary kontyngentu francuskiego zostały zaatakowane 20 sekund później i 6 kilometrów dalej – zginęło 58 francuskich spadochroniarzy. Schemat tego ataku, z mniejszą liczbą ofiar, był powtórzony w Libanie w ciągu kolejnych trzech lat ponad trzydzieści razy[11]. Terroryzm samobójczy z Libanu przeniknął do Izraela, gdzie zaczęły go stosować ugrupowania palestyńskie[12]. Motywem wskazywanym do przeprowadzenia tego typu ataków był odwet na Izraelu za zamachy militarne na Palestyńczyków, izraelskie sankcje ekonomiczno-gospodarcze i poniżanie arabskich mieszkańców Palestyny[13]. Ostatnie zapowiedzi Hamasu dotyczące wznowienia zamachów samobójczych w Izraelu odnotowano w maju 2007 r., kiedy rzecznik tej organizacji oświadczył, że wskutek otwartej wojny wymierzonej w Palestyńczyków dopuszczalne są wszystkie opcje walki z Izraelem, w tym operacje męczeńskie[14].

Znamienne jest to, że po 1980 r. nastąpił lawinowy wzrost ilości samobójczych ataków terrorystycznych w regionach świata, gdzie trwają różnego rodzaju konflikty. W latach 1980 – 2000 na świecie dokonano ok. 270 takich ataków. Połowa z nich była wymierzona nie w cele wojskowe, a cywilne. Do końca 2000 r. odnotowano przeprowadzenie ataków samobójczych w 12 krajach, a o ich zorganizowanie oskarżono co najmniej 15 różnych ugrupowań. Już w roku 2000 ochotników do dokonania zamachów samobójczych przeciwko siłom indyjskim w Kaszmirze i obecności wojsk zachodnich w Pakistanie zaczęły przygotowywać pakistańskie organizacje terrorystyczne *Lashkar-e-Taiba* (Armia Czystych) oraz *Jaish-e-Muhammad* (Armia Mahometa)[15]. Rów-

---

[10] W październiku 1982 r. USA zadecydowały o wprowadzeniu do Bejrutu 1200 *marines*. Było to drugie wejście Amerykanów w tej wojnie, a trzecie w powojennej historii Libanu. W drugim desancie wraz z Amerykanami wylądowało 1560 francuskich spadochroniarzy i 1200 żołnierzy włoskich. Rząd USA zadeklarował całkowitą bezstronność w konflikcie, ale słowa nie dotrzymał. Specjalna komisja senatu USA badająca przyczyny ataku, kierowana przez generała Longa, wyjaśniła, że bezpośrednim powodem zamachu na koszary USA był ostrzał bojowych pozycji szyickich, druzyjskich i syryjskich przez działa okrętowe marynarki USA.

[11] Ostatnio schemat takiego ataku został zastosowany przez Al-Kaidę 8 września 2007 r. w portowym mieście Dellys w Algierii, gdzie dwóch terrorystów zdetonowało ładunki wybuchowe ukryte w samochodzie, wjeżdżając nim na teren bazy wojskowej. W ataku zginęło 28 algierskich żołnierzy, a ponad 60 zostało rannych. Zob. *Zamach samobójczy w Algierii*, informacja zamieszczona w portalu Onet.pl. w dniu 9.09.2007 r.

[12] W Izraelu apogeum terrorystycznych ataków samobójczych, dokonywanych przez ugrupowania palestyńskie – to rok 2003 r. Odnotowano wówczas 26 ataków samobójczych, w których zginęły 144 osoby. W 2004 r. liczba takich ataków spadła do 15; zginęło w nich 55 osób.

[13] W 2006 roku w wyniku działań armii izraelskiej w Strefie Gazy i na Zachodnim Brzegu Jordanu zginęło 660 Palestyńczyków, tj. trzykrotnie więcej niż rok wcześniej. Wśród 660 zabitych było 141 nieletnich (dane podała pozarządowa organizacja izraelska B'Tselem. Por. *Izraelska armia zabiła w tym roku 660 Palestyńczyków*, Onet.pl. z 29.12.2006 r. W maju 2007 r. Izrael dokonał spektakularnych uderzeń lotniczych na obiekty Hamasu w Strefie Gazy w celu wsparcia ugrupowań Fatah. Wg planów Izraela i USA, miały one po dozbrojeniu przejąć w sposób siłowy władzę od Hamasu w Strefie Gazy. Miesiące rywalizacji o władzę między Fatahem prezydenta Mahmuda Abbasa i Hamasem premiera Ismaila Haniji doprowadziły do faktycznej separacji między Zachodnim Brzegiem i Strefą. Obecnie podział na Gazę i Zachodni Brzeg zaczyna się coraz bardziej utrwalać w świadomości Palestyńczyków po obu stronach konfliktu.

[14] Informacje zostały podane w dniu 17.05.2007 r. przez znane agencje prasowe, w tym PAP.

[15] Pierwsza 6-osobowa grupa terrorystów-samobójców z *Lashkar-e-Taiba* próbowała przedostać się z ładunkami wybuchowymi do części wojskowej portu lotniczego w Srinagarze w 2000 r. Skutecznego zamachu na ochronę wojskową parlamentu krajowego w tym mieście dokonała w październiku 2000 r. inna 4-osobowa grupa terrorystów-samobójców.

nież w 2000 r. terroryzm samobójczy, skierowany początkowo przeciwko żołnierzom rosyjskim, pojawił się najpierw w Czeczenii, a potem w Rosji i republikach kaukaskich[16]. Ekstremiści islamscy uczynili z terrorystów-samobójców z Czeczenii i innych regionów świata narzędzia nie mające nic wspólnego z islamem, służące jedynie do osiągnięcia celów politycznych[17]. Czeczeńscy ekstremiści zaczęli stosować terroryzm samobójczy po to, aby skutecznie atakować cele silnie chronione (siedziby służb bezpieczeństwa, administracji) oraz potęgować strach w społeczeństwie Rosji poprzez atakowanie tzw. celów miękkich (metro, pociągi, zgromadzenia religijne, masowe imprezy kulturalne i w końcu samoloty pasażerskie). Do kategorii szczególnego, grupowego terroryzmu samobójczego należy zakwalifikować zajęcie teatru na Dubrowce w 2002 r. i wzięcie zakładników oraz atak na szkołę w Biesłanie w 2004 r. Wskazuje na to nie tylko wyposażenie terrorystów, którzy brali udział w obu atakach, w nasobne ładunki wybuchowe, ale też ich desperacja i gotowość do oddania życia.

Klasycznym przykładem żywiołowego rozwoju i ewolucji terroryzmu samobójczego jest Irak. Nikt nie przewidział, że fenomen terrorystycznych zamachów samobójczych pojawi się w tym kraju wraz z obecnością wojsk amerykańskich i osiągnie skalę niespotykaną wcześniej na żadnym innym obszarze świata. Terroryści-samobójcy ujawnili się w Iraku już na początku agresji amerykańskiej, atakując wszystkie cele uważane za sojusznicze z USA[18]. Od połowy 2005 r. zamachy samobójcze stały się jedną z ważniejszych metod walki ugrupowań ekstremistycznych[19]. W ciągu dwóch pierwszych lat okupacji amerykańskiej w tym kraju terroryzm samobójczy stał się tam zjawiskiem tak masowym i stałym elementem wojny, że niemożliwe stało się jego ujęcie w ramy statystyki i wiarygodnego opisu.

Znamienną ilustracją zjawiska terroryzmu samobójczego w Iraku był atak z 14 sierpnia 2007 r. na kompleks budynków w mieście Kathanija (120 km na zachód od Mosulu), zamieszkanych przez mniejszość wyznającą jazydyzm[20]. Był to największy atak samobójczy przeprowadzony nie tylko od początku wojny w Iraku, ale też jeden z największych na świecie, za wyjątkiem zamachów dokonanych w USA w 2001 r. Sprawcami zamachów było czterech samobójców, którzy jednocześnie zdetonowali ładunki w 4 samochodach-cysternach. W wyniku wybuchów zginęło ok. 400 osób; co najmniej 30 domów było zrównanych z ziemią. Do ataku nikt się nie przyznał[21]. Podobny zamach, z mniejszą liczbą ofiar, miał miejsce 25 października 2009 r., kiedy to zamachowcy-samobójcy zdetonowali w centrum Bagdadu dwa samochody-pułapki,

---

16) C. Reuter, *Zamachowcy - Samobójcy*, Świat Książki, Warszawa 2003, s. 289.

17) Do końca sierpnia 2004 roku czeczeńscy terroryści dokonali 25 samobójczych ataków terrorystycznych, z których 13 przeprowadziły kobiety. W danych, nie uwzględniania się tu terrorystek obecnych w teatrze na Dubrowce. W wyniku zamachów samobójczych zginęło w Rosji co najmniej 460 osób.

18) Wagę zagrożeń terroryzmem samobójczym wobec wojsk koalicji w Iraku unaocznił szczególnie zamach na żołnierzy włoskich w ich bazie w Nasirii, dokonany w listopadzie 2003 r. przez Algierczyka.

19) W 2005 r. w przybliżeniu oszacowano, że ok. 90 proc. wszystkich ataków samobójczych w Iraku dokonywanych było przez obywateli nie Iraku, ale Arabii Saudyjskiej, Jemenu, Kuwejtu, Zjednoczonych Emiratów Arabskich i Omanu. Wielu terrorystów-samobójców pochodziło z różnych państw Afryki Północnej.

20) Jazydzi to kurdyjscy i tureccy wyznawcy synkretycznej religii, łączącej elementy wierzeń indoirańskich, judaizmu, nestorianizmu i islamu. Pierwsza wspólnota jazydzka powstała w XII wieku. Wyznawcy jazydyzmu negują istnienie grzechu, diabła i piekła, oddają cześć aniołom, które, według nich, sprawują władzę nad światem w imieniu Boga.

21) Zob. *Irak: w zamachu zginęło co najmniej 200 osób*, wiadomość zamieszczona w portalu Onet.pl w dniu 15.08.2007 r.

powodując śmierć 155 osób i raniąc ponad 700. 8 grudnia 2009 r., również w Bagdadzie, w atakach (w tym w czterech samobójczych) zginęło co najmniej 127 osób, a 448 zostało rannych. Ataki te zostały przeprowadzone prawie równocześnie w różnych dzielnicach miasta, a celami były budynek Ministerstwa Sprawiedliwości, Ministerstwa Pracy i Spraw Wewnętrznych oraz targowisko[22].

Scenariusze kolejnych tego typu ataków są trudne do przewidzenia. Terroryzm samobójczy w Iraku stał się swoistym poligonem doświadczalnym dla islamskich ugrupowań terrorystycznych z Afganistanu, Pakistanu, Arabii Saudyjskiej, krajów Maghrebu, Somalii i innych regionów świata muzułmańskiego, a także dla obszaru kultury zachodniej. We wrześniu 2009 r. marokańskie służby bezpieczeństwa aresztowały 24 członków siatki terrorystycznej wyspecjalizowanej w werbowaniu ochotników do przeprowadzenia samobójczych zamachów w Iraku, Somalii i Afganistanie.

Szczególną uwagę należy zwrócić na terroryzm samobójczy w Afganistanie. Wraz ze zwiększaniem polskiej obecności militarnej w tym kraju zwiększa się również ryzyko samobójczych ataków terrorystycznych na nasze cele. Po ujawnieniu faktu zabicia afgańskich cywilów przez polskich żołnierzy w sierpniu 2007 r. dowódca talibów w prowincji Helmand oświadczył wysłannikowi Polskiego Radia, że jego ugrupowania bojowe będą atakować żołnierzy NATO bez względu na to, czy są Amerykanami, Brytyjczykami, czy Polakami. Według jego oświadczenia, rebelianci nie zgodzą się na jakiekolwiek negocjacje z afgańskim rządem, dopóki w Afganistanie stacjonują obce wojska, głównie Amerykanie. Dlatego będą atakowali żołnierzy bez względu na kraj ich pochodzenia, żeby zniszczyć plany NATO dotyczące Afganistanu[23].

Terroryzm samobójczy, wcześniej obcy tradycji afgańskiego ruchu oporu, przeniknął do Afganistanu z zewnątrz i przez ostatnich sześć lat był stosowany na skalę niemal masową[24]. Tę metodę walki zainicjował na tym terenie afgański mułła Dadullah[25] (zabity przez wojska amerykańskie 12 maja 2007 r. w prowincji Helmand). 2 stycznia 2007 r. oświadczył on w mediach zachodnich, że w 2007 r. talibowie nasilą samobójcze zamachy terrorystyczne na wojska międzynarodowe oraz zabiją każdego Afgańczyka, który będzie negocjował z proamerykańskim rządem w Kabulu[26]. Informował też, że wśród kilkunastu tysięcy partyzantów posiada kilkuset fedainów (zamachowców-samobójców), gotowych do zmasowanych ataków. Następca Dadullaha, jego brat Mansur Dadullah – rzekomo wcześniej zabity przez Amerykanów – 22 maja 2007 r. zapowiedział zwiększenie liczby samobójczych zamachów na obce wojska, których mieli dokonać ludzie powiązani z talibami. Poinformował również, że wszyscy talibowie są gotowi do przeprowadzenia takich ataków, a także do podkładania bomb i przygotowywania zasadzek na Amerykanów i przedstawicieli rządu[27].

---

22) *Seria krwawych zamachów w Bagdadzie*, PAP, AFP, Reuters z dnia 8.12.2009.

23) Zob. *Będziemy atakować Polaków*, informacja podana przez Polskie Radio oraz Onet.pl. w dniu 4.10.2007 r.

24) Zob. M. Gadziński, *Al Kaida bije rekord terroru*, „Gazeta Wyborcza" z dnia 2.05.2007 r.

25) Dadullah został pozyskany przez CIA w latach 80. do walk z ZSRR. Następnie dowodził mudżahedinami podczas walk bratobójczych w latach 90. Po zwycięstwie talibów został dowódcą ich wojsk. Był jednym z pierwszych byłych mudżahedinów, którzy po 2001 r. zorganizowali znaczący islamski ruch oporu przeciwko obecności USA w Afganistanie. Zabicie Dadullaha zostało uznane przez USA za wielki sukces militarny wojny w Afganistanie.

26) Informacja została podana przez agencję Reuters i Onet.pl w dniu 2.01.2007 r.

27) Zob. *Talibowie chcą pomścić mułłę Dadullaha*, wiadomość zamieszczona na portalu Onet.pl w dniu 23.05.2007 r.

Należy zaznaczyć, że pierwsze ataki samobójcze, których dokonano podczas wojny w Afganistanie odnotowano w marcu 2003 r.; w ciągu dwóch kolejnych lat przeprowadzono je dziewięciokrotnie. Wszystkie skierowane były przeciwko wojskom zachodnim i siłom afgańskim.

Gwałtowny wzrost liczby ataków samobójczych w Afganistanie odnotowano od marca 2005 r. Były one wymierzone również przeciwko celom cywilnym, nie biorącym udziału w walkach[28)]. Według różnych źródeł, ich sprawcy mogli należeć zarówno do grup powiązanych z Al-Kaidą, jak i do ugrupowań talibańskich. Od września 2005 do 15 stycznia 2006 r. w Afganistanie odnotowano 30 ataków przeprowadzonych przez zamachowców-samobójców. W tym okresie afgański ruch oporu tylko na terenie Kabulu próbował dokonać 25 ataków samobójczych skierowanych na obiekty ISAF (*International Security Assistance Force* – Międzynarodowe Siły Wspierające Bezpieczeństwo) i CF (*Canadian Forces* – Siły Zbrojne Kanady). Po serii trzech zamachów na wojska kanadyjskie w styczniu 2006 talibowie napisali w odezwie, że terroryzm samobójczy jest najskuteczniejszą metodą działania, a Kanadyjczycy stali się celami zamachów m.in. dlatego, że wsparli działania bojowe Amerykanów w Kandaharze[29)]. W marcu 2007 r. emir talibów, mułła Omar, zaapelował do afgańskich rebeliantów o stosowanie ataków samobójczych przeciwko zachodnim okupantom w północnych rejonach Afganistanu[30)]. Od stycznia do sierpnia 2007 r. w Afganistanie dokonano ich 70. W tym czasie zamachy samobójcze były dokonywane mniej więcej co 2 - 3 dni[31)]. Rok wcześniej, w 2006 r., odnotowano ich 47.

Inne dane zawarto w specjalnym raporcie ONZ, opublikowanym na początku września 2007 r.[32)]. Napisano tam, że od stycznia do końca sierpnia 2007 r. w Afganistanie dokonano 103 zamachów samobójczych i potwierdzono, że w 2006 r. odnotowano ich 47. W ciągu pierwszego półrocza 2007 r. w wyniku tego typu zamachów zginęły tam 193 osoby, z czego 121 to afgańscy cywile.

---

28) W marcu 2005 r. nieznani sprawcy zdetonowali ładunki wybuchowe przed budynkami rządowymi w Dżalalabadzie. 7 maja 2005 r. samobójca zdetonował ładunek wybuchowy w kawiarence internetowej w Kabulu. Atak był skierowany przeciwko cudzoziemcom. 1 czerwca 2005 r. zamachy samobójcze odnotowano pod meczetem w Kandaharze.

29) Trzy skuteczne ataki samobójcze na kolumny wojsk kanadyjskich w Kandaharze z wykorzystaniem pojazdów były przeprowadzone w pierwszych dwóch tygodniach stycznia 2006 r. W pierwszym ataku, z 2 stycznia 2006 r., terrorysta-samobójca zdetonował obok przejeżdżającej kolumny pojazdów wojsk kanadyjskich ładunek ukryty w samochodzie. W drugim, 15 stycznia, zdetonowano ładunek wybuchowy umieszczony w małym samochodzie osobowym w momencie omijania go przez transporter Mercedes G-Wagon. W zamachu zginął dyplomata z Kanady, Glyn Berry (dyrektor polityczny zespołu odbudowy Afganistanu), a rannych zostało czterech żołnierzy kanadyjskich. Dzień później terrorysta-samobójca zdetonował ładunek umieszczony w samochodzie, którym wjechał w konwój Kanadyjczyków zbliżający się do bazy wojskowej w Kandaharze.

30) Nie można wykluczyć, że w wyniku apelu ugrupowania z tego regionu Afganistanu dokonały samobójczego ataku na żołnierzy niemieckich na lokalnym targu w mieście Kunduz. Samobójca zabił trzech żołnierzy niemieckich i kilkunastu przypadkowych Afgańczyków. Drugiego w ciągu doby podobnego zamachu, skierowanego przeciwko żołnierzom amerykańskim, dokonano na targowisku w mieście Gardez. Terrorysta wmieszał się w tłum ludzi i zdetonował ładunek wybuchowy ukryty pod ubraniem. Zginęło ponad 10 osób, w tym amerykańscy żołnierze. W tym samym dniu polscy politycy poinformowali, że nasi żołnierze rozpoczęli czynności sprawdzające bezpieczeństwo na ulicach miasta, w którym afgański ruch oporu dokonał samobójczego ataku na żołnierzy amerykańskich (Gardez jest jednym z miejsc stacjonowania polskiego kontyngentu).

31) Zob. *Kolejny zamach samobójczy*, „Gazeta Wyborcza" z dnia 20.08.2007 r.

32) Zob. W. Jagielski, *Afgańscy zamachowcy to cudzoziemcy*, „Gazeta Wyborcza" z dnia 10.09.2007 r.

Raport ONZ z września 2007 r. należy ocenić w kategorii najbardziej wiarygodnych dokumentów obrazujących istotę terroryzmu samobójczego. Eksperci ONZ przypisali talibom dokonanie na terenie Afganistanu do końca sierpnia 2007 r. 123 ataków samobójczych[33]. Udowodnili też, że ich ilość gwałtownie rośnie i że mogą one zadecydować o losie wojny i powodzeniu misji NATO w tym kraju. Twierdzą również, że wzrost samobójczych ataków w Afganistanie jest pochodną zmiany taktyki walki talibów z zachodnią koalicją, ponieważ w jej założeniu taka metoda została uznana za jeden z najważniejszych sposobów walki. W ocenie rzecznika przedstawicielstwa ONZ w Kabulu, T. Koenigs'a, zamachy samobójcze skończą się dopiero wtedy, gdy talibowie wygrają wojnę z Zachodem. Raport sporządzony m.in. na podstawie rozmów z więzionymi w Kabulu niedoszłymi zamachowcami potwierdza, że Afgańczycy nie stanowią nawet połowy terrorystów-samobójców. Większość z nich to Pakistańczycy. Pozostali rekrutują się z krajów arabskich oraz muzułmańskich państw b. ZSRR (w Afganistanie i Pakistanie nazywani są Czeczenami). Kandydaci werbowani są głównie spośród przebywających w Pakistanie uchodźców afgańskich (ok. 2 mln), uczących się i wychowujących w medresach. Talibowie twierdzą, że z roku na rok do samobójczych misji zgłasza się też coraz więcej Afgańczyków[34].

Według raportu ONZ, 80 proc. zamachowców atakujących w Afganistanie odbyło przygotowanie w pakistańskim Waziristanie. W świetle raportów wywiadowczych, werbunek w Afganistanie i Pakistanie terrorystów do przeprowadzania ataków samobójczych jest coraz łatwiejszy, szczególnie wśród uczniów szkół koranicznych i w obozach uchodźców, gromadzących młodych Afgańczyków uciekających ze zbombardowanych przez Amerykanów wiosek. W werbowaniu główną rolę odgrywają mułłowie nauczający o powinności dżihadu oraz nienawiści wobec obcych i niewiernych. Kandydatom na samobójczą śmierć obiecuje się prawo do zemsty i zbawienie, a rodzinie – zapomogę finansową.

Terroryzm samobójczy w Afganistanie w najbliższym czasie może się nasilić wskutek nie tylko rozwiniętej bazy werbunkowej, większego motywowania kandydatów, ale też pozyskania przez talibów pokaźnych środków finansowych od rządu Korei Południowej. Podczas konferencji prasowej, zorganizowanej 29 sierpnia 2007 r. w Ghazni przez przedstawicieli Korei Południowej na żądanie talibów, jeden z członków Rady Islamskiego Talibanu oświadczył, że pieniądze otrzymane od rządu w Seulu w kwocie ponad 20 mln dolarów okupu za uwolnienie 19 koreańskich misjonarzy (zostali porwani 19 lipca 2007 r.[35]) będą wydane nie tylko na zakup broni i środków łączności, ale i pojazdów do przeprowadzania jeszcze większej liczby ataków[36].

Analizowany raport miał zdefiniować przyczyny zamachów samobójczych oraz określić możliwości ich ograniczenia. Wskazano w nim, że tego typu ataki są reakcją islamskiego ruchu oporu na obecność wojsk zachodnich w Afganistanie oraz aktem zemsty za zabijanie wyznawców islamu. Ta diagnoza zmusza do refleksji.

---

[33] W 2006 r. w Afganistanie dokonano pięciokrotnie więcej ataków samobójczych, niż w 2005 roku i dziesięciokrotnie więcej, niż w roku 2004.

[34] Student kabulskiego uniwersytetu zatrzymany podczas przygotowań do samobójczego ataku w Kabulu protestował przeciwko traktowaniu go jak pospolitego przestępcę i argumentował, że nie zrobił nic złego, ponieważ zgłosił się tylko na świętą wojnę przeciwko krzyżowcom.

[35] Dotąd nie ustalono, kto dokonał uprowadzenia 23 chrześcijańskich wolontariuszy z Korei Południowej. Mogli tego dokonać i talibowie, i powiązana z nimi grupa należąca do międzynarodowej przestępczości zorganizowanej. Porywacze uwolnili zakładników w trzech turach w sierpniu 2007 r.

[36] Informacje podała 1 sierpnia 2007 r. agencja Reutera. Szerzej zob. W. Jagielski, *Talibowie: Seul zapłacił 20 mln dol. okupu za zakładników*, „Gazeta Wyborcza" z dnia 3.09.2007 r.

Historia stosowania terroryzmu samobójczego dowodzi, że z czasem liderzy islamskiego ruchu oporu starają się przenieść przeprowadzanie ataków na terytorium przeciwnika, z którym walczą w rejonie konfliktu. Zabicie przez polskich żołnierzy siedmiu Afgańczyków w sierpniu 2007 r. oraz coraz bardziej znaczny nasz udział w wojnie afgańskiej pod, praktycznie, amerykańskim dowództwem, mogą być wystarczającymi motywami dla ekstremistów islamskich do przeprowadzania ataków samobójczych w naszym kraju. Latem 2006 r. Mohammed Jusuf Ahmadi, rzecznik talibów, przestrzegając Polaków przed wysyłaniem wojsk do Afganistanu, oświadczył: *Nie mamy śmigłowców ani bombowców, ale możemy sprawić Amerykanom i ich sojusznikom piekło, walcząc z nimi tak, jak nasi bracia z Iraku*. O. Roy, francuski ekspert i znawca Afganistanu oraz islamu, twierdzi, że o ile w 2001 r. afgańscy talibowie byli ruchem narodowym, a Al-Kaidzie udzielali jedynie schronienia, o tyle wojna z Amerykanami przemieniła ich z afgańskich wojowników plemiennych w dżihadystów, rycerzy świętej wojny[37)].

Pod koniec 2009 r., gdy problem Afganistanu zdominowała zmiana strategii wojny oraz zwiększenie obecności wojskowej do ok. 200 tys. żołnierzy, zagrożenia i skala terroryzmu samobójczego są umiejętnie pomijane w retoryce politycznej i relacjach medialnych. Uwagę należy zwrócić na powtarzające się zapowiedzi liderów afgańskiej rewolty, że na zwiększający się kontyngent wojsk zachodnich w Afganistanie bojownicy islamu odpowiedzą zmasowaną bronią w postaci terrorystów-samobójców.

Terroryzm samobójczy w Afganistanie od połowy lipca 2009 r. jest stosowany w ramach nowej taktyki. Taktyka ta polega na tym, że atak grupowy terrorystów-samobójców na obiekty silnie chronione, głównie militarne, wspomagany jest przez grupy klasycznej partyzantki, które ogniem broni strzeleckiej i moździerzy wspierają ataki samobójców. W lipcu 2009 r., kiedy wojska koalicji zachodniej poniosły największe straty od czasu inwazji w 2001 r., ośmiu talibów przebranych za kobiety zaatakowało cywilne urzędy administracji i bazę wojskową w Gardez i Dżalalabadzie. Wszyscy napastnicy zostali zastrzeleni, zanim udało im się przedrzeć do głównych bram. Kilku zdążyło jednak odpalić nasobne ładunki wybuchowe. W podobny sposób (przebrani za kobiety) terroryści-samobójcy zaatakowali wcześniej cywilne i wojskowe obiekty w Kabulu, Nuristanie, Paktice, Kandaharze i Choście. Podczas ataków wspierani byli ogniem przez zorganizowane grupy partyzanckie. W Choście wspomagani przez zamachowców partyzanci atakowali przez kilka godzin żołnierzy afgańskich i amerykańskich[38)].

Problem terroryzmu samobójczego w Afganistanie, tak jak przyszłość tego kraju i wyników prowadzonej tam wojny, musi być rozpatrywany w kontekście sytuacji militarno-politycznej w Pakistanie. Jeśli po 2001 r. nieliczne, samobójcze zamachy terrorystyczne były jeszcze ewidencjonowane i analizowane, to obecnie, gdy skala terroryzmu samobójczego osiągnęła w Pakistanie stan trudny do objęcia go statystykami spoza tego kraju, ewidencja nie jest już prowadzona w sposób dokładny. Do opinii publicznej trafiają tylko informacje o tych atakach, które w sposób istotny wpływają na przebieg konfliktu i ogólną sytuację w Afganistanie. Według danych opublikowanych w 2008 r., w wyniku ataków terrorystycznych w Pakistanie zginęło w latach 2003 – 2006 ponad 1600 cywilów. W samym tylko 2008 r. takich ofiar było 1800. Do października 2009 r. w licznych zamachach, w tym w 60 samobójczych, zginęło 2155 cywilów. Bilans ten nie

[37)] W. Jagielski, *Afgańscy talibowie stawiają na zamachy samobójcze*, „Gazeta Wyborcza" z dnia 22.10.2006 r.
[38)] W. Jagielski, *Zamachowcy przebrani za kobiety atakują w Afganistanie*, „Gazeta Wyborcza" z dnia 21.07.2009 r.

uwzględnia pakistańskich żołnierzy, policjantów i funkcjonariuszy służb specjalnych. Eksperci od terroryzmu w Pakistanie zgodnie twierdzą, że na froncie walki dominuje obecnie nowe pokolenie terrorystów, które coraz bardziej skłonne jest do podejmowania ataków samobójczych. Do ich przeprowadzania pakistańscy i afgańscy ekstremiści rekrutują coraz więcej ochotników, głównie młodsze dzieci[39].

Pakistan w dniu 18 października 2007 r. doświadczył największego w historii tego kraju samobójczego aktu terrorystycznego. W Karaczi, w dwóch eksplozjach w pobliżu konwoju wiozącego byłą pakistańską premier Benazir Bhutto, zginęło co najmniej 160 osób, a 450 odniosło obrażenia. Jako sprawców ataku pakistańska policja wskazała radykałów islamskich, przede wszystkim grupy protalibskie, którym przewodził Baitullah Mehsud[40]. W opinii wielu ekspertów, Pakistan pod względem intensywności działań bojowych wyprzedził obecnie sąsiedni Afganistan[41]. Terroryzm samobójczy nie tylko stał się w Afganistanie głównym narzędziem walki islamistów z siłami rządowymi, ale też pojawił się tam motyw sprzyjający kolejnym ochotnikom. W przeprowadzonej we wrześniu 2007 r. ankiecie sympatię dla Osamy bin Ladena zadeklarowało 46 proc. respondentów, zaś dla byłego prezydenta Musharrafa 38 proc.[42] Aktualny pakistański prezydent Asif Ali Zardari i jego rząd nie radzą sobie z rozwiązaniem konfliktu, który jest bardzo złożony, trudny i bez widoku na niezwłoczne unormowanie.

Po Iraku, Afganistanie i Pakistanie ofensywa islamskiego terroryzmu samobójczego rozpoczęła się na islamskich obszarach Afryki, szczególnie w Algierii i Maroku oraz w Somalii. Jeśli zjawisko to w Algierii i Maroku uległo pod koniec 2008 r. wyraźnemu osłabieniu, to bardzo się nasiliło w Somalii. Aktywność terrorystyczna w Algierii zaznaczyła się w styczniu 2007 r., a pierwsze i dobrze zorganizowane zamachy odnotowano 12 lutego 2007 r. W tym dniu terroryści, w tym samobójcy, dokonali równocześnie siedmiu ataków na komisariaty policji i budynek żandarmerii. Cztery eksplozje nastąpiły w pobliżu posterunków policji. Pięć z siedmiu bomb było ukrytych w samochodach-pułapkach. W atakach zginęło osiem osób.

Kolejnych dwóch ataków samobójczych dokonano 10 kwietnia. Eksplozja samochodu-pułapki, spowodowana przez samobójcę, nastąpiła przed siedzibą premiera Algierii Abdelaziza Belchadema i Ministerstwa Spraw Wewnętrznych. W zamachu zginęło ponad 30 osób, a sześciopiętrowy gmach został uszkodzony. Drugi ładunek samobójca zdetonował obok posterunku policji usytuowanego w pobliżu lotniska pod Algierem. W dniu następnym stołeczna policja otrzymała około 20 alarmów bombowych, których skutkiem były masowe ewakuacje ludzi z dworców autobusowych, marketów, uczelni, budynków administracji i użyteczności publicznej[43]. Samobójcze i zwykłe ataki terrorystyczne w Algierii były przeprowadzane po wejściu w życie przepisów o amnestii dla osób oskarżanych o terroryzm, które złożyły broń, wyraziły skruchę i zobowiązały się przestrzegać zakazu prowadzenia jakiejkolwiek działalności politycznej[44].

---

[39] J. Bajoria, *Pakistan's New Generation terrorystów*. Portal internetowy South Asia Terrorism (SATP) w dniu 26.10.2009 r.

[40] Zob. *Bhutto oskarża islamistów o atak w Karaczi*. Informacja umieszczona na portalu Onet.pl. w dniu 19.10.2007 r.

[41] W. Miasnikow, *Wojna domowa w cieniu głowic atomowych*, „Niezawisimaja Gazieta" z dnia 18.08.2007 r.

[42] E. Follath, H. Stark, *Niepewna przyszłość Pakistanu*, „Der Spiegel" z dnia 5.10.2007 r.

[43] Informacje podała witryna internetowa Arabia.pl – http://www.arabia.pl/content/view/288831/2/.

[44] Amnestia ta nosi oficjalnie nazwę „Karta Pokoju i Pojednania Narodowego" i została opracowana przez prezydenta Algierii Abdelaziza Bouteflikę. Jej postanowienia zostały skierowane głównie do liderów zdelegalizowanego Islamskiego Frontu Ocalenia. Na podstawie postanowień amnestii władze algierskie zwolniły z więzień 2000 osób. W początkowym okresie skorzystało z niej ok. 300 islamistów.

Dwa ataki samobójcze miały miejsce w odstępie dwóch dni na początku września 2007 r. W mieście Batina terrorysta-samobójca zdetonował ładunki przed wizytą algierskiego prezydenta, zabijając co najmniej 20 osób i raniąc 107. Drugiego ataku samobójczego dokonało dwóch terrorystów, wjeżdżając samochodem z ukrytymi ładunkami wybuchowymi na teren bazy wojskowej. Zginęło 37 osób. Do obu aktów przyznała się Al-Kaida w islamskim Maghrebie oświadczając, że były wymierzone w dwa symbole kraju walczącego z terroryzmem – prezydenta Abdelaziza Bouteflikę oraz armię[45)].

Obecność i aktywność terroryzmu samobójczego odnotowano w początkach 2007 r. również w Maroku. W marcu 2007 służby marokańskie ujawniły, że 12-osobowa samobójcza grupa terrorystyczna, działająca w Casablance, zaplanowała i przygotowała ataki samobójcze na zagraniczne statki zacumowane w porcie oraz na hotele „Marrakesz" i „Agadir". Pod koniec marca domniemany przywódca grupy, gdy usiłowano go aresztować, wysadził się w powietrze w kawiarence internetowej. Na początku kwietnia 2007 r. siły marokańskie podjęły próbę zatrzymania lub zlikwidowania członków tej grupy. W trakcie operacji trzech z nich poniosło śmierć, detonując nasobne ładunki wybuchowe w różnych miejscach miasta. Inni zbiegli.

Kolejne ataki samobójcze odnotowano w Casablance 15 kwietnia. Dokonali ich dwaj bracia (przy współudziale innych zamachowców): 31-letni Mohammed Maha i 22-letni Omar Maha. Starszy z braci, podchodząc do policjantów chroniących amerykańską szkołę i konsulat USA, zdetonował nasobne ładunki wybuchowe w celu odwrócenia uwagi od tych obiektów. W tym czasie przed wejściem do jednego z nich wysadził się w powietrze młodszy z braci. Trzeci członek grupy porzucił posiadany ładunek i próbował zbiec. Prawdopodobnie zamachowców było więcej.

Do zamachów samobójczych w Maroku i Algierii przyznała się (jak sami nazywają ją jej członkowie) Organizacja Al-Kaidy w Krajach Maghrebu. Organizacja ta rozpoczęła swój byt medialny 12 lutego 2007 r., kiedy to w rozmowie telefonicznej z kanałem telewizyjnym al Dżazira przyznała się do dokonania opisanych zamachów z 12 lutego 2007 r.[46)] Jej reprezentant poinformował, że organizacja przyjęła taką nazwę w styczniu 2007 r. na rozkaz Osamy bin Ladena[47)]. Wcześniej występowała pod nazwą Salaficka Grupa Modlitwy i Walki (GSPC)[48)]. W kolejnych komunikatach organizacja ta zapowiadała ataki na zachodnie biura, statki, samoloty i hotele dla cudzoziemców, niezależnie od miejsca ich położenia. Należy zaznaczyć, że samobójczy atak na siedzibę algierskiego premiera nastąpił na drugi dzień po zamachach na cele amerykańskie w Maroku, do których dokonania przyznała się właśnie Organizacja Al-Kaidy

---

45) *Zamach samobójczy w Algierii – 37 zabitych*. Wiadomość zamieszczona w portalu Onet.pl. w dniu 9.09.2007 r.

46) Według innych źródeł, organizacja Al-Kaida w Muzułmańskim Maghrebie używa tej nazwy od 28 stycznia 2007 r. Wcześniej faktycznie występowała pod nazwą Salafistyczna Grupa Modlitwy i Walki (GSPC). GSPC, obecna w Algierii, krajach Maghrebu i w Iraku, jest też od dwóch lat szczególnie aktywna w Hiszpanii, Francji, Niemczech i Włoszech.

47) Por. R. Katz, J. Devon, *Franchising Al Qaeda*, „Boston Globe" z dnia 22.06.2007 r. - http://www.boston.com/news/globe/editorial_opinion/oped/articles/2007/06/22/franchising_al_qaeda oraz *Franchising al-Qaeda, More Beheadings.* Informacja opublikowana na specjalistycznym blogu ThreatsWatch.org w dniu 21.04.2007 r.

48) *Al Kaida zabija w Algierii*. Informacja „AFP" z dnia 13.02.2007 r.

w Krajach Maghrebu. Według ekspertów, jest to nowa nazwa organizacji istniejącej już wcześniej, która obecnie jednak stała się groźna z racji doświadczeń jej członków w przeprowadzaniu ataków terrorystycznych oraz zasilania jej terrorystami-samobójcami. Organizacja ujawniła się tylko w Maroku, gdzie w atakach ginęli jej członkowie nie posiadający doświadczenia, ale głęboko umotywowani do samobójczych zamachów na zachodnie cele. W połowie 2007 r. znawcy problemu ostrzegli, że jeśli terroryści z Al-Kaidy w Maghrebie (GSPC) zostaną wyszkoleni i przygotowani do akcji, staną się groźni w krajach Europy[49].

Grupy terrorystyczne działające w Afryce w minionych latach dowiodły swojej żywotności, łatwości zawierania sojuszy i doskonalenia przepływu między sobą informacji, bojowników i funduszy. Liczba ataków w krajach Maghrebu, w Sudanie, Nigerii i Somalii wzrosła w 2006 r. o prawie 65 proc.[50] Nowe formy zagrożeń terrorystycznych w Afryce Północnej zaniepokoiły USA. Sekretarz obrony USA, Robert Gates, na początku lipca 2007 r. ostrzegł kraje europejskie przed możliwymi atakami terrorystycznymi ze strony tamtejszych komórek Al-Kaidy. W ocenie Amerykanów, komórki te coraz silniej zaznaczają swoją obecność w północnej Afryce, gdzie zwiększają siłę uderzeniową i zacieśniają współpracę z międzynarodową siecią terrorystyczną[51].

Ostrzeżenia i prognozy zagrożeń terrorystycznych dotyczących głównie terroryzmu samobójczego w Afryce Północnej potwierdziły się 11 grudnia 2007 r.[52] W tym dniu, w Algierze, dwaj terroryści-samobójcy dokonali dwóch ataków w odstępie 3 minut. Celem pierwszego była siedziba Sądu Najwyższego. Drugiego – siedziba przedstawicieli ONZ, w tym biuro Wysokiego Komisarza ds. Uchodźców ONZ (UNHCR), mieszczące się w sąsiedztwie algierskich ministerstw, Rady Konstytucyjnej, placówek dyplomatycznych, biur i firm zachodnich oraz domów zamieszkanych przez cudzoziemców. Oba zamachy przeprowadzono przy użyciu samochodów wyładowanych materiałami wybuchowymi. Pojazdy były kierowane przez zamachowców-samobójców. Według różnych danych zginęło ok. 70 osób, w tym pracownicy ONZ. Do zamachów przyznało się ugrupowanie przedstawiające się jako Al-Kaida w Afryce Północnej. Na swoich stronach internetowych ekstremiści ogłosili, że ataki przeprowadziło dwóch terrorystów-samobójców: Abdul-Rahman al-Aasmi i Ami Ibrahim Abou Othman. Opublikowali także ich zdjęcia[53]. Wybór celów oraz sposób dokonania tych zamachów dowiódł, że zapowiedzi ugrupowań terrorystycznych o atakowaniu obiektów należących

---

[49] Zob. D. Thomas, *Al-Kaida weźmie na cel Francję i Hiszpanię?*, „The Independent", „Gazeta Wyborcza" z dnia 16.04.2007 r.

[50] Niepokojące tendencje w tym rejonie odnotowano w pierwszych miesiącach 2007 r., kiedy gwałtownie zaczęła rosnąć liczba zorganizowanych grup terrorystycznych stosujących zamachy samobójcze i możliwość ich przeniesienia do Europy, głównie do Francji, Hiszpanii i Wielkiej Brytanii. Por. R. Gunaratna, *Al-Kaida w Afryce*, „Christian Science Monitor" z dnia 30.04.2007 r.

[51] *Al Kaida umacnia się w północnej Afryce*, Wiadomość zamieszczona na portalu Onet.pl. w dniu 14.07.2007 r.

[52] W połowie listopada 2007 r. algierskie służby bezpieczeństwa poinformowały o zatrzymaniu w Algierze jednego z głównych liderów Al-Kaidy, Fateha Buderbalę, alias Abdelfataha Abu Basira. Aresztowano go razem z dwoma pomocnikami. Ujawniono przy nich 800 kg materiałów wybuchowych, trzy przygotowane do użycia ładunki wybuchowe i 20 detonatorów. Aresztowanie Abu Basira uznano za sukces w eliminowaniu zagrożeń terrorystycznych w Algierii. Por. *Aresztowano szefa Al-Kaidy w Algierze*, Onet.pl w dniu 19.11.2007 r.

[53] Informacje o zamachu podały 11.12.2007 r. największe agencje informacyjne. Zob. *Al-Kaida przyznaje się do masakry w Algierze*. Informacja umieszczona na portalu TVN24.pl: http://www.tvn24.pl/0,1531830,wiadomosc.html.

do Zachodu przez terrorystów-samobójców są i – jak wskazuje retoryka ekstremistów islamskich – będą realizowane w zależności od rozwoju sytuacji politycznej w krajach Afryki Północnej.

W pierwszej połowie 2006 r. terroryzm samobójczy wraz z próbą militarnego uporządkowania sytuacji w tym kraju z głównym udziałem USA i Etiopii pojawił się w Somalii. We wrześniu 2006 r. islamistyczna partia Al Itihaad al Islamija – AIAI (Jedność Islamska), której bojownicy trzy miesiące wcześniej (tj. w czerwcu) zdobyli Mogadisz, poinformowała o otworzeniu obozów wojskowych dla bojowników oraz ochotników na terrorystów-samobójców. Jeden z przywódców bojowników islamskich, Fuad Mohammed Kalaf, zapowiedział, że nie ma nic złego w planach szkolenia młodych ludzi na wojnę z obcymi najeźdźcami, bo podobne rzeczy zdarzają się w wielu krajach świata. Kilka dni wcześniej nieudany atak samobójczy somalijska AIAI przeprowadziła na uznawanego przez wspólnotę międzynarodową somalijskiego prezydenta Abdullahiego Jusufa. Atak ten zmusił do ucieczki z Mogadiszu rząd somalijski, utworzony faktycznie przez USA i Etiopię. Zamach na Abdullahiego Jusufa był pierwszym w Somalii samobójczym zamachem bombowym[54]. W czerwcu 2007 r. terrorysta-samobójca zdetonował ładunek wybuchowy w samochodzie, usiłując zabić z kolei premiera Somalii. Kolejny, ale spektakularny, atak samobójczy miał miejsce 19 września 2009 r., a jego celem była baza sił pokojowych Unii Afrykańskiej (AMISOM) w Mogadiszu. Dwóch zamachowców-samobójców wjechało na teren bazy i zdetonowało ładunki wybuchowe ukryte w samochodach skradzionych ONZ. Samochody i sprawcy oznakowani byli symbolami ONZ. Atak na bazę sił Unii Afrykańskiej był odwetem bojówki miejscowych islamistów za wcześniejsze zabicie przez amerykańskie siły specjalne jednego z miejscowych bojowników islamskich, Saleha Alego Nabhana[55]. Przebieg konfliktu politycznego, religijnego i militarnego w Somalii wskazuje, że sytuacja stała się krytyczna dla przyszłości tego kraju i regionu. Wspólnota międzynarodowa zajęta wojną w Afganistanie nie jest w stanie obecnie podjąć jakichkolwiek kroków w tej sprawie.

W kontekście terroryzmu samobójczego na uwagę zasługuje również Iran. Pomimo retoryki propagandowej Zachodu, przedstawiającej ten kraj jako głównego „sponsora" najgroźniejszych szyickich, ale też sunnickich organizacji terrorystycznych, rolę Iranu powinno się rozpatrywać także w kontekście stosowania terroryzmu samobójczego[56]. Należy podkreślić, że państwo to posiada szczególnie bogate doświadczenia w organizowaniu i wykorzystywaniu terroryzmu samobójczego i nie zawaha się go zastosować w przypadku pojawienia się nowego konfliktu, w którym Teheran poczuje się zagrożony. Iran i jego islamscy przywódcy są prawdopodobnie w stanie uruchomić do walki z Zachodem terrorystów-samobójców na skalę trudną do wyobrażenia. W czasie kryzysu dyplomatycznego na linii Iran-Zachód, który rozpoczął się w marcu 2007 r. a wywołany był zatrzymaniem przez Irańczyków 15 brytyjskich marynarzy i żołnierzy w Zatoce Perskiej, 1 kwietnia 2007 r. podczas uroczystości upamiętniających rocznicę powstania republiki islamskiej, prezydent Iranu Ahmadineżad oświadczył: *Samobójstwo jest niezwyciężoną bronią, a Iran może – w razie potrzeby – wysyłać dziennie setki*

[54] W. Jagielski, *Somalijscy talibowie wyszkolą żołnierzy dżihadu*, „Gazeta Wyborcza" z dnia 20.09.2006.

[55] *Somalia: w ataku na bazę sił UA zginęło 16 ludzi*, http://www.euroislam.pl/index w dniu 20.09.2009.

[56] Senat USA w dniu 1 października 2007 r. zdecydowaną większością głosów uchwalił rezolucję o uznaniu irańskiej Gwardii Rewolucyjnej za organizację terrorystyczną. Zob. *Biały Dom przygotowuje atak na Iran*. Informacja umieszczona na portalu Onet.pl w dniu 1.10.2007 r.

samobójców uzbrojonych w bomby jak przed 20 laty podczas wojny z Irakiem Saddama Husajna. Wola popełnienia samobójstwa jest jedną z najlepszych dróg życia[57].

W Iranie kultywuje się bohaterstwo bojowników-samobójców, nazywanych męczennikami za wiarę, chociaż ginących najczęściej z motywów politycznych. Uważani są oni nie tylko za patriotów i bohaterów kraju, ale też za przedstawicieli religijnego męczeństwa, którzy w poczuciu islamskiej cnoty gotowi są do złożenia ofiary z siebie.

W marcu 2008 r. pojawiły się pierwsze informacje o zaistnieniu terroryzmu samobójczego w Tybetańskim Regionie Autonomicznym należącym do Chin. W wywiadzie dla włoskiej gazety „Corriere della Sera" przewodniczący młodzieżowego kongresu tybetańskiego Tsewang Rigzin oświadczył: *Pacyfizm, głoszony przez Dalajlamę XIV nie przynosi rezultatów i dlatego być może za kilka lat tybetański ruch oporu ucieknie się do samobójczych ataków terrorystycznych. Pacyfizm zaprowadził nas na ślepy tor. Mówi się o nas w sposób epizodyczny, ograniczony. Zostaliśmy zapomniani przez wspólnotę międzynarodową. Tyle pięknych słów, a potem nic. Widzimy natomiast, jak przypominają o sobie Palestyńczycy i aktywiści w Iraku dzięki samobójczym atakom. Uwaga światowych mediów skupiona jest wyłącznie na nich. Być może wkrótce nadejdzie pora zmiany strategii walki. W związku z tym – scenariusz samobójczych ataków, dokonywanych przez Tybetańczyków, walczących o niepodległość jest «bardziej niż możliwy»*. Biorąc pod uwagę historyczne doświadczenia konfliktów współczesnego świata nie można wykluczyć, że kolejnym obszarem, w którym rozwinie się terroryzm samobójczy, może być Tybet i Chiny[58].

W podsumowaniu tej części opracowania należy wskazać, że na całym arabskim Bliskim Wschodzie[59], w Afryce Północno-Wschodniej i Azji Środkowej oraz na Kaukazie Północnym terroryzm samobójczy może stosować około dwudziestu najbardziej zdeterminowanych, dużych islamskich organizacji terrorystycznych. Nie wiadomo, jak duży potencjał terroryzmu samobójczego tkwi również w rejonach Kaukazu Północnego, skąd ekstremiści przeniknęli do Afganistanu i Pakistanu[60]. W sumie, działające na interesujących nas obszarach świata organizacje mogły w ostatnim czasie wygenerować ok. 500 grup (komórek) terrorystycznych, dysponujących odpowiednimi zasobami finansowymi, doświadczeniem i zapleczem ludzkim i w związku z tym zdolnych do organizowania i dokonywania ataków samobójczych w każdym regionie świata.

---

[57] Zob. M. Zawadzki, *Brytyjczycy wciąż w niewoli w Iranie, ropa w górę*, „Gazeta Wyborcza" z dnia 2.04.2007 r.

[58] *Młodzi Tybetańczycy: możliwe samobójcze ataki*. Informacje internetowe, w tym Onet.pl, w dniu 25.03.2008.

[59] W 2007 r., po kilkuletniej przerwie ataki samobójcze ponownie zaczęto stosować w Turcji. Pod domem towarowym Anafartalar w Ankarze. 22 maja 2007 r. zamachu samobójczego dokonał 36-letni obywatel turecki pochodzenia kurdyjskiego. Celem ataku, w którym zginęło 6 przypadkowych osób, była przejeżdżająca kolumna pojazdów z Szefem Sztabu Generalnego, generałem Yasarem Buyukanitą. W tym samym dniu, po pościgu, policja turecka zatrzymała w Adanie kobietę, która zamierzała dokonać kolejnego ataku samobójczego. Przy niedoszłej szahidce ujawniono ponad 11 kilogramów materiałów wybuchowych i dwa inne ładunki. Zatrzymanej towarzyszył mężczyzna. Por. *Zamachu w Ankarze dokonał kurdyjski kamikadze*, „Hurriyet i Radikal" z dnia 23.05.2007 r.

[60] W sierpniu 2008 r. służby rosyjskie odnotowały wznowienie samobójczych ataków terrorystycznych w Czeczenii i sąsiadujących z nią republikach. W dniu 30 sierpnia 2008 r. samobójczego ataku dokonało dwóch sprawców, którzy wjechali samochodem z materiałami wybuchowymi na teren bazy wojskowej koło Groznego.

ABSTRACT

The paper focuses on one fighting method of contemporary terrorism – 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 always an activity done by a group of people rather than a single person.

The analysis consists of three parts. The first one presents the historical backgrounds of suicide terrorism, its origins and contemporary situation. The analysis presents many facts in order to support its theses. The second part encompasses criminological analysis of perpetrators' traits and their modus operandi. It describes such aspects as their main goals for employing suicide attacks, motivation of the suicide attackers and different types of group activities which are needed to conduct an attack. The third part presents legal aspects of suicide terrorism. It focuses on penal liability of those mainly, who assist and prepare an attack. In Authors' opinion, governmental agencies responsible for providing security should concentrate their endeavors on that exact group of people in order to effectively fight against this type of terrorism.

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

Przemysław Ligenza
Tomasz Nalepa
Cezary Sochala
Jan Szymanowski

Zapasy prekursorów bojowych środków trujących i niebezpiecznych substancji chemicznych a terroryzm

Cz. I – Wybrane zagadnienia teorii zapasów

Wstęp

Państwa reagują na dynamicznie zmieniające się zagrożenia, doskonaląc swe potencjały obronne. Istotny wpływ na współczesne poglądy w zakresie przygotowań gospodarczych państw w dziedzinie obronnej wywarły doświadczenia początku ubiegłego stulecia.

Pierwsza wojna światowa była konfliktem globalnym, podczas którego użyto nowej klasy uzbrojenia i środki bojowe, takie jak: karabiny maszynowe, czołgi, samoloty, amunicja o zwiększonej sile rażenia oraz broń chemiczna. Stosowane uzbrojenie i środki bojowe cechowała „materiałochłonność" niespotykana w przypadku wcześniej prowadzonych działań zbrojnych. Wojna pochłonęła zapasy wojenne walczących państw w ciągu zaledwie kilku miesięcy. Wydajność wytwarzania środków prowadzenia walki nie nadążała za potrzebami walczących armii; gospodarkom państw brakowało mocy wytwórczych oraz surowców. W celu zachowania priorytetu produkcji wojennej zastosowano interwencjonizm państwowy [1].

Rozwój technologiczny oraz potencjał ekonomiczny państw uznawano już w okresie międzywojennym za ważne elementy przygotowań wojennych. Planowanie wojenne najważniejszych państw świata realizowane było przy czynnym udziale resortów cywilnych [2]. Sposób prowadzenia działań wojennych przez siły zbrojne determinował poziom rozwoju technologicznego uzbrojenia, zaś o powodzeniu mobilizacji decydował potencjał ekonomiczny państwa.

W okresie „zimnej wojny", gdy do uzbrojenia wprowadzono broń jądrową, w ślad za gotowością bojową wojsk podążała gotowość obronna przemysłu. Zestawienie współzależnych elementów – struktury sił zbrojnych i zdolności do nieprzerwanej produkcji przemysłowej – postrzegano łącznie jako wpływające na osiągnięcie celów systemu obronnego. Z potrzebą zapewnienia nieprzerwanej produkcji obronnej wiązało się zapotrzebowanie na surowce i materiały niezbędne do zaspokojenia wzmożonych wymagań mobilizacji [3]**.**

Wraz z końcem zimnej wojny jednym z dominujących determinantów bezpieczeństwa państw stał się aspekt ekonomiczny [1].

Obecnie na bezpieczeństwo państw wpływ wywierają nowe rodzaje zagrożeń. Przeciwnikami, oprócz regularnych armii, do zwalczania których przystosowane są systemy obronne państw, stali się terroryści. [...] i*ch przywódcy oraz ich działania występują poza strukturami, w jakich są zorganizowane nasz świat i nasze społeczeństwo.* Terroryści, będąc zazwyczaj słabo wyposażeni, dla osiągnięcia swoich wojskowych ce-

lów adaptują zwykłe środki cywilne. Zagrożenia, które stwarzają [...] *dotyczą poczucia bezpieczeństwa naszych społeczności, społeczności innych krajów, naszych zdobyczy i sposobu życia, z zamiarem ich zmiany i w to miejsce narzucenia swoich* [4]. Jednocześnie nadal aktualne pozostają zagrożenia tradycyjne, wynikające z dążeń poszczególnych graczy państwowych. W sposób ewidentny dowodzą tego wydarzenia ostatnich miesięcy na Kaukazie.

Obecna wojna, jak wskazują doświadczenia XXI w., nie musi polegać na pokonaniu siły zbrojnej przeciwnika, natomiast może wykorzystywać: [...] *wszelkie możliwe powiązania – polityczne, ekonomiczne, społeczne i wojskowe – do przekonania politycznych decydentów przeciwnika, że ich cele strategiczne są nieosiągalne i zbyt kosztowne w stosunku do planowanych korzyści. Jej istota polega na ugruntowanym przeświadczeniu, że silniejsza wola polityczna odpowiednio użyta może pokonać znacznie mocniejszego ekonomicznie i militarnie przeciwnika* [5].

Państwa w ramach prowadzonych przygotowań obronnych podejmują określone działania mające na celu dostosowanie swych systemów obronnych do przeciwdziałania przewidywanym zagrożeniom. Określone funkcje w ramach tych przygotowań wypełniają potencjał przemysłowy państwa oraz jego rezerwy strategiczne. Te dwa istotne elementy przygotowań obronnych mogą stanowić źródło zagrożeń asymetrycznych. Realizowane przez nie zadania obronne wiążą się bowiem z gromadzeniem wielu asortymentów rezerw strategicznych, wśród których występują substancje i materiały potencjalnie przydatne terrorystom.

Jak podkreśla R. Kuźniar, [6] przewidywalne zagrożenia asymetryczne, pomimo że nie destabilizują całości systemu państwowego, mogą powodować skutki, które będą dotkliwe dla: obywateli, infrastruktury państwa czy dóbr materialnych. Mimo, iż stanowią zagrożenia z zewnątrz, omijają klasyczną obronę z centralnym elementem w postaci sił zbrojnych, materializując się od wewnątrz. Tak więc, akcent przygotowań w systemie bezpieczeństwa narodowego powinien zostać przesunięty z tradycyjnej obrony z użyciem klasycznych sił zbrojnych w stronę szerokiego spektrum instytucji i służb bezpieczeństwa wewnętrznego.

W artykule wskazano na wybrane przypadki aktów terroru, które potencjalnie mogłyby być zorganizowane i przeprowadzone w wyniku wykorzystania przez terrorystów zapasów prekursorów bojowych środków trujących (BST) oraz niebezpiecznych substancji chemicznych magazynowanych przez przedsiębiorców w Polsce. Wybrane aspekty przedmiotu rozważań cechują się wysokim poziomem szczegółowości, co podyktowane jest chęcią zapewnienia reprezentatywnych danych, możliwych do praktycznego wykorzystania przez instytucje i służby państwowe. Inne spośród nich zostały całkowicie pominięte. Mając na uwadze bezpieczeństwo państwa, autorzy nie wykazali innych potencjalnych możliwości wykorzystania przez terrorystów zapasów prekursorów BST oraz niebezpiecznych substancji chemicznych. Celem publikacji artykułu było wskazanie zakresu i skutków działań terrorystycznych, możliwych w przypadku wykorzystania podobnych środków chemicznych.

W opinii autorów, zawarte w artykule przykłady dowodzą potrzeby dalszych systemowych działań na rzecz optymalnego zabezpieczenia określonych asortymentów magazynowanych przez przedsiębiorców.

Zgodnie z klasyfikacją środków chemicznych, przyjętą przez NATO [7] oraz Konwencję o Zakazie Broni Chemicznej [8], wyróżnić można dwie grupy broni chemicznej: BST oraz środki chemiczne podwójnego przeznaczenia, stosowane w przemyśle.

Spośród 1100 środków chemicznych podwójnego zastosowania, około 100 może zostać wykorzystanych przez terrorystów. Niebezpieczeństwo działań terrorystycznych z ich użyciem jest tym większe, że materiały podwójnego zastosowania są łatwo dostępne na rynku komercyjnym. Na skalę zagrożenia takimi atakami wskazują skutki wypadków z tego typu substancjami. Przykładowo, wyciek około 30 t toksycznych substancji chemicznych, jaki miał miejsce w Indiach w grudniu 1984 r., spowodował śmierć 3 tys. osób, konieczność hospitalizacji 50 tys. osób i udzielenie pomocy lekarskiej około 100 tys. osób.

Nie można wykluczyć możliwości użycia przez terrorystów BST, czyli substancji zaliczanych do I grupy wyżej wspomianej klasyfikacji. Warto przypomnieć atak terrorystów z sekty Najwyższa Prawda dokonany w dniu 27 czerwca 1994 r. w Matsumoto. W wyniku uwolnienia około 30 kg sarinu zginęło wówczas 7 osób, a liczba hospitalizowanych wyniosła około 600. Terroryści tej samej sekty niecały rok po tym wydarzeniu, w dniu 20 marca 1995 r., zaatakowali sarinem metro w Tokio. Zginęło 12 osób, a 5,5 tys. zostało porażonych. Niewielka liczba ofiar śmiertelnych wynikała ze stosunkowo niskiej jakości użytego sarinu oraz nieprofesjonalnego sposobu rozprzestrzeniania tego środka.

Dynamiczny rozwój przemysłu chemicznego w XX w. stanowi potencjalną przesłankę powstania nowej kategorii zagrożeń dla człowieka i środowiska – skażenia toksycznymi środkami przemysłowymi (TSP). Stanowią one drugą grupę środków wymienianych w Konwencji. TSP mogą być produkowane, używane lub gromadzone w zakładach przemysłowych, w środkach transportowych, w medycynie, wojsku oraz innych obiektach gospodarki narodowej. Najczęściej do awarii chemicznej dochodzi wskutek wycieku TSP z instalacji przemysłowych, zbiorników czy cystern. Do tego typu zdarzeń dochodzi podczas kolizji transportowych, nieumyślnego działania pracowników lub powodowania zamierzonych zniszczeń powstałych w wyniku ataków terrorystycznych. Skalę problemu powiększa fakt, iż to nie tylko zakłady chemiczne stanowią potencjalne zagrożenie, lecz również zakłady sektora przemysłu przetwórczego, hurtownie, itp. Najważniejsze zakłady utrzymujące duże zapasy TSP skupione są w rejonach dwóch największych rzek Polski: Wisły i Odry. Lokalizacja zakładów przemysłu chemicznego usytuowana jest wzdłuż całego biegu Wisły (Kwidzyn, Bydgoszcz, Toruń, Włocławek, Płock, Puławy, Tarnobrzeg, Tarnów, Oświęcim, Czechowice-Dziedzice) oraz wzdłuż górnego biegu Odry (Police, Szczecin, Kostrzyń) oraz w rejonie Śląska (Brzeg Dolny, Kędzierzyn-Koźle, Racibórz, Gliwice, Chorzów, Jaworzno). Ponadto, duże zakłady chemiczne znajdują się w Gorzowie Wielkopolskim.

Do potencjalnych źródeł skażeń chemicznych zaliczyć należy również transport niebezpiecznych substancji (drogowy, kolejowy, lotniczy, morski i żeglugę śródlądową). Ze względu na skutki skażeń TSP do szczególnie zagrożonych rejonów, należą zurbanizowane obszary dużych aglomeracji miejskich, rzeki i jeziora (w tym ujęcia wody pitnej). W świetle dotychczasowych doświadczeń najbardziej prawdopodobnym wydaje się spowodowanie przez terrorystów katastrof kolejowych i drogowych, ze względu na olbrzymią ilość przewożonych pasażerów, wielkość i różnorodność niebezpiecznych ładunków (toksyczne, łatwopalne, wybuchowe i inne) zwiększających skalę i rozmiar zagrożeń, które w równej mierze dotyczą pasażerów i mieszkańców miejscowości leżących w pobliżu szlaków kolejowych i drogowych [9].

Uwzględniając fakt, że zapasy przedsiębiorstw mogą stanowić źródło ataków terrorystycznych, za celowe uznano prezentację wybranych zagadnień teorii ich dotyczących, której celem jest wyjaśnienie podstaw optymalizacji decyzji dotyczących zarządzania

zapasami. W dalszej części publikacji przedstawiono przykłady zapasów środków chemicznych, materiałów wybuchowych oraz ich prekursorów utrzymywanych przez przedsiębiorców w Polsce i możliwości ich wykorzystania przez terrorystów.

Teoria zapasów

Prowadzenie działalności gospodarczej wiąże się z koniecznością podejmowania określonych decyzji. Istotnym problemem dla przedsiębiorców prowadzących jakąkolwiek gospodarkę materiałową jest zarządzanie zapasami. Z tego problemu wynikają następujące problemy szczegółowe: wybór optymalnej wielkości zakupów, magazynowanie asortymentu, optymalizacja poziomu zapasów, minimalizacja kosztów zarządzania zapasami w różnych uwarunkowaniach rynkowych. Zagadnienie zarządzania zapasami uznaje się za na tyle istotne, że wypracowano naukową teorię zapasów. Teoria ta ściśle wiąże się z teorią decyzji i dotyczy optymalizacji rozwiązań w zakresie utrzymania ciągłości łańcucha dostaw i usług. W teorii zapasów rozpatruje się zazwyczaj podejmowane przez przedsiębiorcę decyzje dotyczące: wielkości utrzymywanego zapasu surowców oraz produktów i półproduktów. Decyzję o rodzajach oraz ilości rezerw strategicznych podejmują rządzący danym państwem, przy czym kompetencje w przedmiotowym zakresie zależą od przyjętych regulacji prawnych.

W procesie decyzyjnym, którego celem jest podjęcie decyzji, należy dokonać wyboru alternatywnego rozwiązania, które powinno zapewnić największe korzyści końcowe. Różnicę korzyści między rozpatrywanymi alternatywami określa się jako koszty utraconych korzyści [10]. Koszty utraconych korzyści stanowią specyficzne kryterium decyzyjne i mierzone są wielkością przyjętą za cel działań w okresie, do którego odnoszą się decyzje. W przypadku określenia celu działań jako maksymalizacji zysku, koszty utraconych możliwości stanowią niezrealizowany zysk lub marżę brutto. Zatem, koszty utraconych korzyści dotyczą marży brutto na jednostkę zasobu o ograniczonej dostępności oraz kosztów alternatywnych i optymalnych [10]. Specyficznym wyrazem zabezpieczania się przed kosztami utraconych możliwości jest optymalny zapas bezpieczeństwa. Zapas bezpieczeństwa stanowi zabezpieczenie przed trudnymi do przewidzenia sytuacjami. Ze względu na fakt, że utrzymywanie zapasów bezpieczeństwa stanowi dodatkowy koszt, ich istnienie uzasadnione jest jedynie wówczas, gdy korzyści przewyższają koszty [11]. Zapasy odnoszą się do przepływów w organizacji. Wyodrębniono różne metody sterowania tymi przepływami, jak również wypracowano różne systemy wspomagania zarządzania łańcuchem dostaw [12, 13]. Za najważniejsze problemy decyzyjne dotyczące zapasów uznaje się [14]:

- wybór towarów, których zapasy powinny być utrzymywane,
- określenie wielkości zamawianych partii towarów,
- określenie czasu składania zamówień,
- określenie systemu kontroli zapasów.

Zasadniczym celem utrzymywania zapasów w racjonalnych warunkach decyzyjnych jest zachowanie ciągłości łańcucha podaży w dynamicznym środowisku. Łańcuch podaży, dzięki lepszej organizacji i sprawniejszemu funkcjonowaniu, powinien w niektórych wypadkach zapewnić przewagę konkurencyjną. Zasadniczymi celami łańcucha podaży są [15]:

- obsługa klientów,
- niskie koszty operacyjne,
- minimalizacja aktywów.

Wyżej przedstawione cele wynikają z kształtujących strategię łańcucha podaży jego specyficznych cech [15]:
- nastawienia na optymalną obsługę klienta,
- działanie ponad organizacjami,
- skuteczności zależnej od czasu,
- nastawienia globalnego,
- złożonych powiązań systemowych,
- poziomych procesów zarządzania,
- indywidualnie postrzeganego zakresu działań.

Przyjmując wyżej określone cele, wynikające z charakterystyki łańcucha podaży, można wyróżnić cztery rodzaje strategii łańcucha podaży [15]:
- strategię funkcjonalną,
- strategię interakcji logistyki pomiędzy działaniami,
- strategię koordynacji poprzez informację,
- strategię jednolitego procesu zarządzania.

Skoro łańcuch podaży jest zarówno siecią, jak i systemem, jego model strategiczny powinien uwzględniać strukturę, proces i zależności. Konstrukcja struktury łańcucha podaży obejmuje [15]:
- określenie wymagań umożliwiających osiągnięcie celów,
- analizę struktury kosztów,
- określenie optymalnej konfiguracji reakcji na zmiany,
- określenie działalności podstawowej w kategoriach uzyskania przewagi konkurencyjnej,
- określenie organizacji,
- optymalizację kosztów – negocjacje,
- określenie wymagań organizacyjnych dotyczących koordynacji, pomiaru oraz kontroli,
- wyznaczenie form koordynacji organizacji uczestniczących w łańcuchu podaży oraz technik informacyjnych.

Model strategiczny łańcucha podaży (czyli określenie, w jaki sposób powinna dokonywać się podaż określonych rodzajów surowców i towarów na rynku lub rynkach międzynarodowych) wymaga dokonania wyboru strategicznego działania systemu i postawienia pytania: przewidywać popyt czy reagować na zmiany popytu? Kryterium wyboru strategii odnośnie procesu łańcucha podaży stanowią czas i koszty [15]. Czynnik czasu dotyczy obsługi w danym cyklu oraz zdolności reagowania na zmiany. Natomiast koszty obejmują zarówno utrzymywanie zapasów stanowiących skutek prognozowania, jak i koszty zysków utraconych, będące rezultatem kosztów utraconych przychodów.

Ze względu na fakt, że zarządzanie łańcuchem podaży (czyli dysponowanie zasobami określonych surowców i towarów na rynku lub rynkach międzynarodowych) nie oznacza jedynie reguł decyzyjnych i systemu informacji, ale charakteryzuje się również wzajemnym oddziaływaniem podmiotów procesów gospodarczych oraz ludzi, współpraca między organizacjami oraz ich wzajemna integracja stanowią podstawę tak struktury, jak i procesu łańcucha podaży [15]. Zarówno dla przedsiębiorstwa, jak i dla społeczeństwa i państwa, łańcuch podaży należy do elementów strategicznych. W przypadku państwa, niezależnie od jego strategii funkcjonowania, strategia łańcucha podaży, w szczególności w warunkach zagrożenia jego bezpieczeństwa, stanowi zasadniczy element wpływający na możliwość realizacji strategii funkcjonowania.

Oczywiście w przypadku państwa inna będzie struktura łańcucha podaży w warunkach jego względnie bezpiecznego funkcjonowania, inna zaś w warunkach zagrożenia jego bezpieczeństwa. Określenie warunków jako „względne bezpieczeństwo" odnosi się do możliwości zaistnienia lokalnych sytuacji wewnętrznych, które wpływają w pewien sposób na bezpieczeństwo, ale nie determinują działań w sposób globalny w odniesieniu do całego organizmu państwowego. W przypadku zagrożenia bezpieczeństwa państwa, wynikającego z wewnętrznych czy zewnętrznych uwarunkowań wpływających na całą kondycję państwa, łańcuch podaży będzie zawierał w sobie jedynie te elementy, które są niezbędne do utrzymania funkcjonowania tego państwa. Dotyczy to w szczególności różnych dziedzin życia ludności oraz utrzymania ciągłości produkcji na rzecz bezpieczeństwa i obronnności państwa.

Literatura

1. P. Górski, J. Płaczek, M. Skarżyński, M. Sułek, *Wojna a gospodarka. Problemy. Myśl. Proces przemian*, AON, Warszawa 2008.
2. L. Wyszczelski, *Prowadzenie wojny, kierowanie siłami zbrojnymi oraz planowanie wojenne w latach 1918-1939*, AON, Warszawa 1997.
3. M. Sułek, *Wykorzystanie syntetycznych miar potencjału gospodarczo-obronnego w polityce i strategii bezpieczeństwa*, AON, Warszawa 1994.
4. R. Smith: *The Utility of Force. The art of War in the Modern World. New York 2007*, w: M. K. Ojrzanowski, *Zdolności operacyjne warunkiem skutecznych sił zbrojnych*. http://www.dt.mon.gov.pl/plik/file/Ojrzanowski.pdf.
5. M. K. Ojrzanowski, *Zdolności operacyjne warunkiem skutecznych sił zbrojnych*. http://www.dt.mon.gov.pl/plik/file/Ojrzanowski.pdf.
6. R. Kuźniar, *Bezpieczeństwo – realizm oceny, dylematy polityki*, w: *Polska w Europie*, 2002, nr 3 (41).
7. Dokumenty: AAP-6, LG/7, AC/225, D/61 z dnia 18 lipca 1996 r..
8. *Konwencja o zakazie prowadzenia badań, produkcji, składowania i użycia broni chemicznej oraz zniszczeniu jej zapasów z 1993 r.*
9. T. Nalepa, C. Sochala, *Akty terroryzmu chemicznego i przeciwdziałanie im. Wybrane zagadnienia*, TWO, Zeszyt Problemowy, (w druku).
10. I. Sobańska, *Analiza relacji: koszty-rozmiary-wyniki. Ceny*, w: *Rachunek kosztów i rachunkowość zarządcza*, pod red. I. Sobańskej, C.H.Beck, Warszawa 2006.
11. T. Wnuk-Pel, *Zarządzanie zapasami*, w: *Rachunek kosztów i rachunkowość zarządcza*, pod red. I. Sobańskej, C.H.Beck, Warszawa 2006.
12. M. Ciesielski, *Instrumenty zarządzania logistycznego*, PWE, Warszawa 2006.
13. M. Fertsch, *Podstawy zarządzania przepływem materiałów w przykładach*, Biblioteka Logistyka, Poznań 2003..
14. F. J. Beier, K. Rutkowski, *Logistyka*, SGH, Warszawa 2006, s. 79.
15. P. B. Schary, T. Skjøtt-Larsen, *Zarządzanie globalnym łańcuchem podaży*, PWN, Warszawa 2002.

Cz. II. Środki toksyczne i materiały wybuchowe stosowane przez terrorystów

Zapasy środków chemicznych

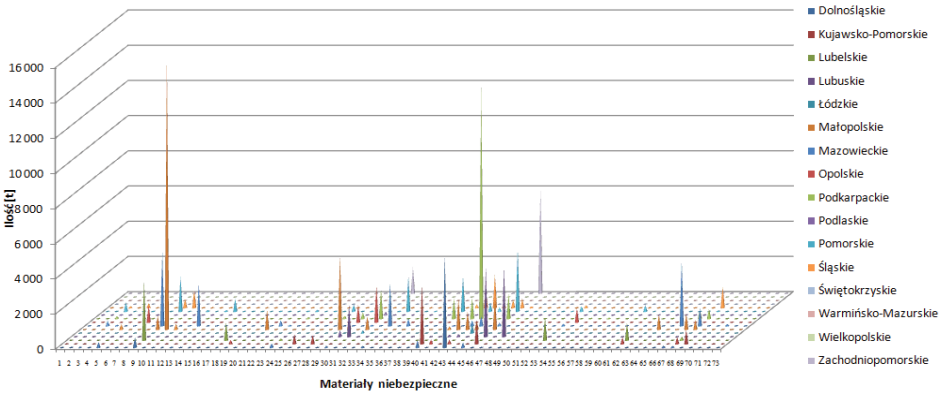
Postępowanie z zapasami prekursorów bojowych środków trujących (BST) oraz niebezpiecznych substancji chemicznych, stanowi skomplikowany problem decyzyjny. O ile teoria zapasów może w pewien sposób wspomagać zarządzanie takimi zapasami, o tyle utrzymywanie bojowych środków trujących ma podwójne zastosowanie i w niektórych przypadkach nie wiąże się bezpośrednio z uwarunkowaniami rynkowymi. Nieco inaczej rzecz się ma z niebezpiecznymi substancjami chemicznymi, takimi jak: aceton, benzen, cykloheksanon, formaldehyd, fenol, naftalen, octan etylu i toluen. Aceton, jako dobry rozpuszczalnik, znajduje szerokie zastosowanie w przemyśle chemicznym, gumowym i farmaceutycznym. Podobnie benzen, który jest stosowany jako rozpuszczalnik lub surowiec do dalszej syntezy. Cykloheksanon wykorzystywany jest głównie do produkcji nylonu, zaś formaldehyd stosowany jest jako środek dezynfekujący do produkcji barwników, żywic syntetycznych oraz do produkcji materiałów wybuchowych. Octan etylu wykorzystywany jest w przemyśle perfumeryjnym jako środek zapachowy oraz rozpuszczalnik, jak również jako dodatek aromatyzujący do żywności. Trietanoloamina (TEA) jest substancją powszechnie stosowaną w przemyśle kosmetycznym i budowlanym. Zapobiega rozwarstwianiu się składników kremów, żeli, emulsji, farb i pianek budowlanych. Wykorzystywana jest także do syntezy BST. Podobne zastosowanie do produkcji fosforoorganicznych BST znalazł trichlorek fosforu, który również wykorzystuje się w przemyśle chemicznym do syntezy barwników oraz jako dodatek do paliw. Obydwie substancje znajdują się na liście towarów objętych kontrolą obrotu [1] (TEA – 102-71-6; PCl_3 – 7719-12-2). Zatem utrzymywanie odpowiednich ilości zapasów niebezpiecznych substancji chemicznych znajdujących zastosowanie w przemyśle (możliwych do wykorzystania jako prekursory do syntezy bojowych środków trujących), stanowi z jednej strony podstawę utrzymania łańcucha produkcji i dostaw, z drugiej – problem z zakresu bezpieczeństwa.

BST to grupa toksycznych związków chemicznych, które w wyniku bezpośredniego działania na organizm ludzki lub przez skażenie środowiska mogą spowodować masowe porażenie ludzi, zwierząt i roślin. BST znajdują zastosowanie jako podstawowe składniki broni chemicznej. Występują najczęściej w stanie ciekłym lub stałym, rzadziej gazowym. W stanie bojowym występują w postaci par i aerozoli. Pary ciekłych BST są zazwyczaj cięższe od powietrza. Większość BST dobrze rozpuszcza się w tłuszczach (olejach, smarach) oraz w rozpuszczalnikach organicznych (alkoholach, dichloroetanie, benzenie). W wodzie rozpuszczają się tylko niektóre spośród BST (sarin, fluorometylofosfonian izopropylu $(CH_3)_2CHOPOFCH_3$, cyjanowodór, kwas fluorooctowy FCH_2COOH i jego sole). Ze względu na pożądane parametry fizyko-chemiczne (wysoka toksyczność, odporność na wpływ czynników atmosferycznych i odkażalników) nie wszystkie środki trujące zaliczane są do BST. Drogami przenikania trucizny do organizmu są: układ oddechowy, skóra, błony śluzowe, układ pokarmowy i otwarte rany [2, 3].

Natomiast TSP *(*ang. *TIM - toxic industrial materials)* to termin podstawowy określający toksyczne lub radioaktywne substancje w postaci stałej, ciekłej lub gazowej. Substancje te mogą być produkowane, używane lub gromadzone w zakładach przemysło-

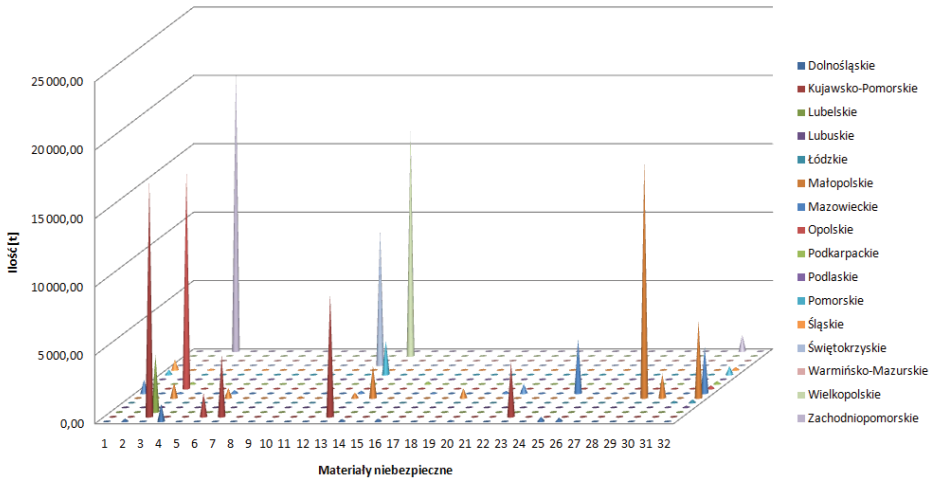
wych, środkach transportowych, medycynie, wojsku oraz w innych obiektach gospodarki narodowej. TSP mogą występować jako związki chemiczne, substancje biologiczne lub radioaktywne i mogą być opisywane jako: toksyczne środki chemiczne (TSC), toksyczne środki biologiczne (TSB), promieniotwórcze substancje przemysłowe (PSP) [4].

Ilości niebezpiecznych materiałów z podziałem na materiały wybuchowe i ich prekursory oraz toksyczne związki chemiczne, znajdujące się w zapasach zakładów, przedstawiono na rys. 1 i 2.



Rys. 1. Materiały wybuchowe i prekursory do ich syntezy znajdujące się w zapasach zakładów produkcyjnych:

1 – 2,4,6-trinitrotoluen $CH_3C_6H_2(NO_2)_3$; 2 – 2-pentanon $CH_3CH_2CH_2COCH_3$; 3 – aceton CH_3COCH_3; 4 – anilina $C_6H_5NH_2$; 5 – azotan amonu (saletra amonowa) NH_4NO_3; 6 – azotan potasu KNO_3; 7 – azotan sodu $NaNO_3$; 8 – azotyn sodu $NaNO_2$; 9 – benzen C_6H_6; 10 – benzol (benzen, toluen, ksylen); 11 – bezwodnik kwasu chromowego CrO_3; 12 – bezwodnik kwasu octowego $(CH_3CO)_2O$; 13 – butyloglikol $C_4H_8(OH)_2$; 14 – chloran potasu $KClO_3$; 15 – chloran sodu $NaClO_3$; 16 – chlorobenzen C_6H_5Cl; 17 – chromian potasu K_2CrO_4; 18 – cykloheksan C_6H_{12}; 19 – dibenzylotoluen $C_6H_5CH_2CH_2C_6H_4CH_3$; 20 – dichromian potasu $K_2Cr_2O_7$; 21 – dichromian sodu Na_2Cr2O_7; 22 – dietyloamina $NH(CH_2CH_3)_2$; 23 – difenyloamina $NH(C_6H_5)_2$; 24 – diizocyjanian toluenu $CH_3C_6H_3(CNO)_2$; 25 – dimetyloanilina $C_6H_5N(CH_3)_2$; 26 – dinitrotoluen $CH_3C_6H_3(NO_2)_2$; 27 – dynamit (nitrogliceryna, ziemia okrzemkowa); 28 – epichlorochydryna C_3H_5ClO; 29 – etylobenzen $C_6H_5C_2H_5$; 30 – fenol C_6H_5OH; 31 – formaldehyd HCHO; 32 – formalina (wodny roztwór aldehydu mrówkowego); 33 – fosfor czerwony; 34 – glikol etylenowy $C_2H_4(OH)_2$; 35 – heksogen $(CH_2NNO_2)_3$; 36 – hydrazyna N_2H_4; 37 – hydroksyloamina NH_2OH; 38 – izopropyloamina $CH_3CH(NH_2)CH_3$; 39 – krezole $HOC_6H_4CH_3$; 40 – ksylen (dimetylobenzen) $CH_3C_6H_4CH_3$; 41 – kwas azotowy HNO_3; 42 – kwas octowy CH_3COOH; 43 – kwas siarkowy H_2SO_4; 44 – kwas solny HCl; 45 – materiały wybuchowe (niezdefiniowane związki chemiczne); 46 – metanol CH_3OH; 47 – metyloetyloketon $CH_3COC_2H_5$; 48 – mocznik $CO(NH_2)_2$; 49 – nadchloran amonu NH_4ClO_4; 50 – nadmanganian potasu $KMnO_4$; 51 – nadtlenek benzoilu $C_6H_5COOOCOC_6H_5$; 52 – nadtlenek dodekanolu; 53 – nadtlenek wodoru H_2O_2; 54 – naftalen $C_{10}H_8$; 55 – nitroceluloza $[C_6H_7O_2(OH)_{3-x}(ONO_2)_x]_n$; 56 – nitrogliceryna $C_3H_5(ONO_2)_3$; 57 – o-chloronitrobenzen $ClC_6H_4NO_2$; 58 – o-nitrotoluen $CH_3C_6H_4NO_2$; 59 – o-toluidyna $CH_3C_6H_4NH_2$; 60 – pentryt $C(CH_2ONO_2)_4$; 61 – pirydyna C_6H_5N; 62 – propylen $CH_3CH=CH_2$; 63 – pyrolidon C_4H_7NO; 64 – rtęć Hg; 65 – siarczan dihydrazyny $N_2H_4*1/2H_2SO_4$; 66 – siarka; 67 – styren $C_6H_5CH=CH_2$; 68 – toluen $C_6H_5CH_3$; 69 – toluenodiizocyjanian (TDI) $CH_3C_6H_3(NCO)_2$; 70 – trietanoloamina $N(CH_2CH_2OH)_3$; 71 – trietyloamina (TEA) $N(CH_2CH_3)_3$; 72 – urotropina (HMTA) $C_6H_{12}N_4$; 73 – wodzian hydrazyny $N_2H_4*H_2O$.



Rys. 2. Związki toksyczne będące w zapasach zakładów produkcyjnych:
1 – 2-furylometanol (furfurol) $C_4H_3OCH_2OH$; 2 – akrylan butylu $CH_2=CHCO_2(CH_2)_3CH_3$; 3 – amoniak NH_3; 4 – arsen As; 5 – arsenowodór AsH_3; 6 – chlor Cl_2; 7 – chlorek winylu $CH_2=CHCl$; 8 – cyjanamid NH_2CN; 9 – cyjanowodór HCN; 10 – ditlenek siarki SO_2; 11 – ditlenek węgla CO_2; 12 – disiarczek węgla CS_2; 13 – etanol C_2H_5OH; 14 – fosfor P; 15 – fosgen $COCl_2$; 16 – kwas chlorooctowy $ClCH_2COOH$; 17 – kwas fluorowodorowy HF; 18 – kwas ortofosforowy H_3PO_4; 19 – octan etylu $CH_3COOC_2H_5$; 20 – octan winylu $CH_3COOCH=CH_2$; 21 – pestycydy (nie zdefiniowane związki chemiczne); 22 – siarkowodór H_2S; 23 – tetrachloroetylen C_2Cl_4; 24 – tlenki azotu; 25 –tlenek etylenu (oksiran) C_2H_4O; 26 – tlenek propylenu C_3H_6O; 27 – tlenochlorek fosforu $POCl_3$; 28 – trichlorek fosforu PCl_3; 29 – tritlenek arsenu (arszenik) As_2O_3; 30 – tritlenek siarki SO_3; 31 – woda amoniakalna NH_3 aq; 32 – wodorotlenek sodowy NaOH.

Część spośród tych związków chemicznych znajduje zastosowanie zarówno w syntezie materiałów wybuchowych jak i w produkcji BST. Z tego powodu zaproponowany podział uwzględnia możliwość przemysłu w wytwarzaniu niebezpiecznych materiałów (rys. 2 nie uwzględnia związków chemicznych ujętych w rys. 1). Rysunki obrazują skalę realnego zagrożenia w przypadku awarii chemicznej i ataku terrorystycznego. Do TSP stwarzających statystycznie potencjalne zagrożenie ze względu na ilość zgromadzonych zapasów zaliczyć należy: amoniak, chlor, disiarczek węgla, tetrachloroetylen, tlenek etylenu oraz tritlenek arsenu (rys. 2). Województwa szczególnie zagrożone skażeniami to: kujawsko – pomorskie, opolskie, małopolskie, śląskie, wielkopolskie i zachodniopomorskie.

Prekursory BST oraz niebezpieczne środki chemiczne a terroryzm

Najstarszą formą terroryzmu było zatruwanie żywności. Obecnie nawet fakt stosowania zaawansowanych procedur kontroli jakości nie eliminuje negatywnego oddziaływania psychologicznego, jakie może wywołać informacja o zatruciu pewnej ilości środków żywnościowych produktu globalnej marki. Mimo, że taki atak może uśmiercić niewielką liczbę ludności, to strach powoduje ogromne straty gospodarcze

i psychozę. Osoby pozostające w konflikcie z ekologistami (farmerzy, urzędnicy) niejednokrotnie otrzymywały anonimowe pogróżki. Nic więc dziwnego, że groźby Animal Right Militia (ARM) o spowodowaniu zatrucia słodyczy Mars Bars (Wielka Brytania, 1984) i Cold Buster (Kanada, 1992), czy indyczego mięsa w sklepach Safeway i Save-On-Foods (Vancouver, 1994) zostały potraktowane bardzo poważnie [5]. Potwierdza to akcja ARM, przeprowadzona w dniu 3 stycznia 1994 r. w Kanadzie. Dokonano zatrucia batonów Cold Buster, sprzedawanych w Edmonton i Calgary, umieszczając w nich środek do czyszczenia piekarników. Cała akcja była zorganizowana jako protest przeciwko finansowaniu badań na zwierzętach przez producenta wspomnianych batonów. Przeprowadzono również akcję propagandową poprzez dostarczenie dwóch skażonych batonów do mediów. W rezultacie, z ponad 250 kanadyjskich sklepów wycofano dziesiątki tysięcy batonów, a badania potwierdziły zanieczyszczenie chemiczne tylko 85 batonów. Ponadto okazało się, że nawet spożycie zanieczyszczonych batonów nie zagroziłoby życiu ani zdrowiu konsumentów [6]. Mimo, że od 30 lat rośnie zainteresowanie terrorystów wykorzystaniem środków chemicznych, skuteczność akcji jest ograniczana koniecznością wykorzystania precyzyjnej technologii. Możliwość ewentualnego wykorzystania zapasów środków chemicznych przez terrorystów, wymusza konieczność ich odpowiedniego zabezpieczania, w tym podejmowania stosownych interwencji o charakterze prewencyjnym.

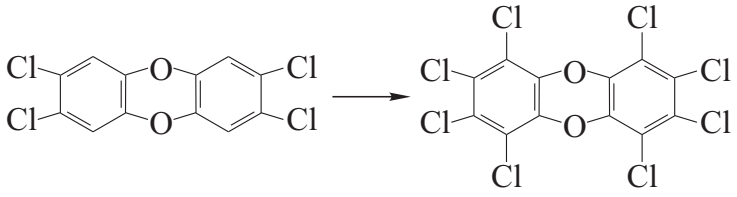
W dniu 3 grudnia 1984 r. w zakładach chemicznych należących do Union Carbide w Bhopalu w Indiach miała miejsce katastrofa przemysłowa. Przyczyną skażenia terenu i śmierci ludzi, była reakcja izocyjanku metylu (nitrylu metylu–MIC) z wodą (reakcja hydrolizy) oraz reakcja polimeryzacji. Obydwie reakcje są egzotermiczne. Izocyjanek metylu jest silnie trującą cieczą, która wrze w temp. 27^0C. Skutki niekontrolowanej reakcji hydrolizy lub polimeryzacji MIC są nieprzewidywalne. Reakcja hydrolizy MIC zachodzi wg równania:

$$CH_3NC + 2H_2O \xrightarrow{H^+} CH_3NH_2 + HCOHC + \text{energia}$$

Jak wynika z powyższego równania, wzrost energii spowodował przejście MIC z cieczy w parę (stan gazowy). W wyniku wzrostu temperatury doszło do powstania pęknięć w betonowej przykrywie zbiornika, w którym zgromadzono MIC. W ciągu 60 minut poprzez powstałe szczeliny do atmosfery wydostało się około 30 ton trującego gazu, co było przyczyną masowych zatruć [7].

10 lipca 1976 r. w Seveso we Włoszech, gdzie produkowano 2,3,5-trichlorofenol (TCP) z glikolu etylenowego, ksylenu, tetrachlorobenzenu i sody kaustycznej (wodorotlenek sodowy), doszło do niekontrolowanej reakcji w wyłączonym reaktorze. W wyniku otwarcia się zaworu bezpieczeństwa do atmosfery wydostało się, między innymi, 2 kg 2,3,7,8-tetrachlorodibenzoparadioksyny (TCDD), silnej trucizny, która wchłania się do organizmu poprzez układ pokarmowy, oddechowy lub skórę (środek kontaktowy). Stwierdzono około 700 przypadków zatruć wśród okolicznej ludności i liczne padnięcia zwierząt. Duże obszary upraw rolnych zostały wyłączone z produkcji na 10 lat. Dioksyny są szczególnie niebezpiecznymi substancjami chemicznymi ze względu na to, że powodują uszkodzenia narządów wewnętrznych (nerek, płuc, wątroby, rdzenia kręgowego). Są one produktami ubocznymi w syntezie pestycydów, mają właściwości

rakotwórcze. TCDD w glebie ulega powolnym przemianom do octachlorodibenzoparadioksyny (OCDD), który jest tysiąckrotnie słabszą trucizną [8].



TCDD OCDD

Innym znanym przypadkiem masowego zatrucia dioksynami było zatrucie olejem ryżowym w 1968 r. w Japonii 1800 osób (Yusho – choroba ryżowa). Podobne zdarzenie miało miejsce na Tajwanie w 1978 r. oraz w Belgii w 1999 r. (tzw. afera kurczakowa) [9].

E. Croddy [10] opisuje działanie dywersyjne, polegające na zamiarze podłożenia bomby pod zbiornikami stacji paliw z mieszaniną propanu i butanu, co w wyniku wybuchu miało doprowadzić do uszkodzenia zbiorników pobliskiego zakładu przemysłowego wypełnionych siarkowodorem (H_2S). Przypadek ten mógł spowodować poważne zagrożenie zdrowia i życia ludzi przebywających w pobliżu miejsca awarii.

Zapasy materiałów wybuchowych

Kolejną z wymienionych grup materiałów niebezpiecznych stanowią materiały wybuchowe (MW). Zgodnie z obowiązującymi w Polsce przepisami prawnymi [11], materiałami wybuchowymi są substancje (indywidua) chemiczne stałe lub ciekłe, albo mieszaniny substancji, zdolne do reakcji chemicznej z wytwarzaniem gazu o takiej temperaturze i ciśnieniu i z taką szybkością, że mogą powodować zniszczenia w otaczającym środowisku, a także wyroby wypełnione materiałem wybuchowym. MW w myśl wspomnianych przepisów są również materiały pirotechniczne zdefiniowane jako materiały lub mieszaniny materiałów przewidzianych do wytwarzania efektów cieplnych, świetlnych, dźwiękowych, gazu, dymu lub kombinacji tych efektów, w wyniku bezdetonacyjnej, samopodtrzymującej się reakcji chemicznej, a także wyroby wypełnione materiałem pirotechnicznym. Ich ilości w zestawieniu z miejscem przechowywania (podział administracyjny) przedstawia rys. 1. Do prekursorów materiałów wybuchowych stwarzających statystycznie potencjalne zagrożenie ze względu na ilość zgromadzonych zapasów zaliczyć należy m.in.: benzen, benzol, cykloheksan, etanol, formalinę, glikol etylenowy, ksyleny, kwas octowy, metanol, mocznik, toluen. Województwa szczególnie zagrożone to: kujawsko – pomorskie, lubuskie, małopolskie, mazowieckie, opolskie, podkarpackie, pomorskie, śląskie.

Od 1989 r. dynamicznie rozwija się import do Polski wyrobów pirotechnicznych widowiskowych (WPW), znanych również jako sztuczne ognie bądź fajerwerki. Na terenie kraju działa kilkanaście dużych hurtowni, w których składowane są znaczne ilości WPW.

Liczbę największych hurtowni WPW przedstawiono w tabeli 1.

Lp.	Województwo	Liczba hurtowni składujących WPW
1	Dolnośląskie	3
2	Kujawsko-Pomorskie	2
3	Lubelskie	3
4	Lubuskie	2
5	Łódzkie	2
6	Małopolskie	3
7	Mazowieckie	4
8	Opolskie	3
9	Podkarpackie	1
10	Podlaskie	1
11	Pomorskie	3
12	Śląskie	4
13	Świętokrzyskie	2
14	Warmińsko-Mazurskie	1
15	Wielkopolskie	3
16	Zachodniopomorskie	2
	Polska - razem	39

Tab. 1. Szacunkowa liczba największych hurtowni WPW

Ze względu na ilość hurtowni oraz zgromadzony w nich tonaż WPW najbardziej zagrożonymi województwami są: dolnośląskie, lubelskie, małopolskie, mazowieckie, opolskie, pomorskie, śląskie i wielkopolskie.

Prekursory materiałów wybuchowych i materiały wybuchowe a terroryzm

Wykorzystanie na szeroką skalę ładunków wybuchowych do celów terrorystycznych nastąpiło w drugiej połowie XIX wieku. Było to spowodowane postępem nauk chemicznych, zwłaszcza w dziedzinie syntezy związków chemicznych służących do wytworzenia materiałów wybuchowych (MW). Również Polacy mają swój udział w rozwoju terroryzmu zwanego obecnie bombowym. W wyniku wybuchu bomby podłożonej przez Polaka Ignacego Hryniewieckiego zginął w dniu 13 marca 1881 r. rosyjski car Aleksander II. W 1906 r. na terenie Królestwa Polskiego przeprowadzono ponad 600 zamachów z użyciem ładunków wybuchowych, w których zginęło około 300 osób.

W czasach współczesnych zamachy bombowe są jedną z najbardziej popularnych form terroryzmu. Wiąże się to ze stosunkowo łatwą dostępnością – pomimo rygorystycznych form ochrony – do gotowych MW. Osobny problem stanowią prekursory MW, które – poza nielicznymi wyjątkami – są ogólnie dostępne. Za prekursory MW uważa się pierwiastki lub związki chemiczne, z których po odpowiedniej obróbce chemicznej lub fizycznej (np. zmieszaniu) otrzymuje się MW.

Jako przykład zastosowania prekursora MW mogą posłużyć zamachy przeprowadzone w Madrycie w dniu 11 marca 2004 r., gdzie w wyniku wybuchu 11 bomb zginęło 191 osób, a 1900 zostało rannych. Wśród zabitych i rannych znajdowali się również Polacy. Do wytworzenia użytych we wspomnianym zamachu ładunków wybuchowych użyto saletry amonowej, stosowanej powszechnie jako nawóz sztuczny. W wyniku zmieszania saletry amonowej o wysokiej zawartości azotu, zawierającej powyżej 70% azotanu amonu (NH_4NO_3) z substancjami palnymi (np. olejem napędowym) powstaje MW. W Unii Europejskiej prowadzone są prace nad odpowiednimi przepisami [12],

określającymi pewną liczbę związków chemicznych (prekursorów), które mogą być wykorzystane do wytworzenia MW „sposobem domowym". Wejście w życie wyżej wymienionych przepisów spowoduje, iż saletra amonowa będzie dostępna jedynie dla upoważnionych użytkowników prowadzących działalność rolniczą, naukową, produkcyjną itp.

Azotan amonowy stanowi obecnie podstawowy surowiec do produkcji wszystkich nowoczesnych MW, przeznaczonych do użytku cywilnego. Azotan amonu jest utleniaczem, w związku z czym wspomaga palenie substancji. Ulega on rozkładowi w temperaturze 169°C z wydzieleniem tlenków azotu (NO_x) i amoniaku (NH_3). Powyżej temperatury 260°C możliwy jest rozkład wybuchowy. Stanowi to szczególne zagrożenie podczas pożarów magazynów, w których jest przechowywany.

W dniu 2 października 2003 roku w miejscowości Saint – Romain-en-Jarez (Francja), w pomieszczeniu gospodarczym na farmie zapaliło się siano. W pomieszczeniu tym przechowywanych było również 3000 - 5000 pustych plastikowych skrzynek do owoców i wykonanych z polietylenu oraz 3 - 4 t saletry amonowej. Straż pożarna rozpoczęła gaszenie pożaru po ok. 30 minutach, a eksplozja nastąpiła po ok. 1 godz. od momentu zauważenia ognia. Rannych zostało 26 osób. Prawdopodobną przyczyną wybuchu było wymieszanie stopionego polietylenu z saletrą amonową, w efekcie czego powstał MW, który zdetonował na skutek działania wysokiej temperatury.

W dniu 21 września 2001 w miejscowości Toulouse we Francji doszło do eksplozji w magazynie saletry amonowej, gdzie magazynie tym przechowywano 300 - 400 t tego związku, z czego 30 - 40 t zdetonowało. W skutek wybuchu zginęło 30 osób, ponad 2500 zostało poszkodowanych. Podkreślenia wymaga fakt, iż nie zauważono ani ognia, ani dymu w czasie poprzedzającym wybuch.

W 1954 roku, podczas transportu saletry amonowej przez Morze Czerwone, wybuchł pożar w części ładunkowej przewożącego statku. Powstała mieszanina o składzie saletra amonowa/papier opakunkowy/substancja organiczna/miedź. W wyniku eksplozji spowodowanej przez pożar statek zatonął w krótkim czasie. Szybka ewakuacja ludzi zapobiegła ofiarom.

9 marca 2004 r. w Hiszpanii samochód przewożący saletrę amonową uległ kolizji z innym samochodem. Nastąpiło wymieszanie saletry z paliwem z rozbitych samochodów w skótek czego powstał MW. W wyniku pożaru nastąpił wybuch. Zginęły 2 osoby, a 5 zostało rannych.

Właściwa kontrola dystrybucji saletry amonowej na każdym etapie eksploatacji producent – dystrybutor – użytkownik (w sposób określony jak dla MW) powinna zapewnić zmniejszenie prawdopodobieństwa jej przejęcia przez osoby nieuprawnione. Przede wszystkim, powinna zostać zapewniona dokładna kontrola zużywanej ilości tej substancji. Do czynników zwiększających zagrożenie niebezpieczeństwem wybuchu podczas przechowywania oraz przewozu saletry amonowej należy zaliczyć:

- nieodpowiednie warunki składowania – np. przechowywanie w budynkach wykonanych z materiałów palnych wspólnie z innymi materiałami palnymi, ekspozycja słońca itp.;
- nieodpowiedni sposób przewozu – bez zachowania warunków określonych w europejskiej umowie ADR;
- brak wiedzy na temat bezpieczeństwa stosowania tego związku.

Innym ogólnie dostępnym prekursorem MW jest aceton. W czterech zamachach bombowych przeprowadzonych w Londynie w dniu 7 lipca 2005 r., w których zginęły 52 osoby, wykorzystano MW otrzymany z acetonu. Był to nadtlenek acetonu. Należy

zauważyć, iż zgodnie z przepisami UE [13] sprzedaż acetonu jako prekursora stosowanego do wytwarzania narkotyków również w Polsce podlega rejestracji, co jednak nie wpływa na znaczące ograniczenie dostępu do tej substancji.

Niewłaściwe warunki przechowywania WPW oraz nieprzestrzeganie warunków bezpieczeństwa podczas wykonywania operacji z ich wykorzystaniem może doprowadzić do niekontrolowanego zadziałania tych wyrobów. Taki wypadek wydarzył się 13 maja 2000 r. w Holandii, w Enschede. Zginęło wówczas 20 osób, a około 1000 doznało obrażeń [8]. Przyczyną wypadku było nieostrożne obchodzenie się z WPW, prawdopodobnie w trakcie załadunku. Wysoka liczba ofiar wynikała z lokalizacji magazynów – kontenerów WPW, które znajdowały się w centrum miasta. Innym powodem było zainteresowanie zaistniałą sytuacją osób postronnych, które przebywały w miejscu wypadku. Trzeba podkreślić, iż w początkowej fazie opanowano powstały pożar, jednak dalej sytuacja całkowicie wymknęła się spod kontroli: zginęły również osoby zainteresowane pożarem, który to przekształcił się w masowy wybuch.

W pewnej z hurtowni znajdującej się na terenie naszego kraju kilka lat temu wydarzył się podobny wypadek. Powodem były, prawdopodobnie, błędy popełnione przez personel przygotowujący WPW do wykonania pokazu widowiskowego. Zginęły wówczas dwie osoby, biorące bezpośredni udział w pracach przygotowawczych do pokazu. Z uwagi na położenie budynków hurtowni, z zachowaniem odpowiednich stref bezpieczeństwa, więcej ofiar ani też strat materialnych nie było.

Składowanie WPW – oprócz zagrożeń związanych z niewłaściwą ich eksploatacją – może powodować niebezpieczeństwa wynikające z właściwości chemicznych mieszanin pirotechnicznych. Szczególnym zagrożeniem jest wysoka wilgotność otoczenia. Mieszaniny pirotechniczne wykazują na ogół właściwości higroskopijne. Zatem, niewłaściwie zaprojektowane czy też wadliwie wykonane wyroby pirotechniczne zawierające MP mogą chłonąć wodę, co może skutkować różnego rodzaju reakcjami chemicznymi. I tak, np. w mieszaninie, w skład której wchodzi między innymi azotan sodu oraz aluminium, mogą zachodzić następujące reakcje:

$$Al + 3H_2O \rightarrow Al(OH)_3 + 1{,}5H_2$$
$$3NaNO_3 + 8Al + 18H_2O \rightarrow 7Al(OH)_3 + 3NH3 + Na_3[Al.(OH)_6]$$

Zarówno wodór jak i amoniak mogące powstać w wyżej wymienonych reakcjach tworzą z powietrzem mieszaniny palne i wybuchowe. Istnieje duże prawdopodobieństwo, iż zapalenie się tych gazów spowoduje niekontrolowane zadziałanie składowanych WPW.

Wszystkie poddane analizie przypadki wskazują, iż każde zdarzenie z użyciem środków chemicznych i materiałów wybuchowych może spowodować straty osobowe oraz materialne, a także nieodwracalne straty w środowisku naturalnym. Działania prewencyjne powinny być realizowane dwutorowo, obejmując z jednej strony permanentną analizę zagrożeń, w tym rozpoznanie grup terrorystycznych, z drugiej zaś – realizację przedsięwzięć w zakresie efektywnego przeciwdziałania skutkom skażenia chemicznego. Istotną rolę w tym zakresie powinien odgrywać rozwinięty (zintegrowany) system informatyczny instytucji i służb państwowych kompetentnych do przeciwdziałania aktom terroru.

Osobnym zagadnieniem jest zagrożenie produktami przeróbki ropy naftowej, w tym benzynami, olejem napędowym i olejem opałowym. Ze względu na zasięg ogólnokrajowy, autorzy wyłączyli tę grupę materiałów niebezpiecznych z dalszych rozważań.

Literatura

1. Rozporządzenie Rady (WE) nr 1183/2007 z dnia 18 września zmieniające i aktualizujące rozporządzenie (WE) nr 1334/2000 ustanawiające wspólnotowy system kontroli eksportu produktów i technologii podwójnego zastosowania. Załącznik I, *Wykaz towarów i technologii podwójnego zastosowania, Kategoria 1 Materiały, substancje chemiczne, mikroorganizmy i toksyny* (Dz.U UE 2007 r. L 278),.2. Praca zbiorowa, *1000 słów o chemii i broni chemicznej*, Wydawnictwo MON, Warszawa 1987.
3. J. Grochowski, S. Głozak, *Chemia środków trujących*, WAT, Warszawa 1973.
4. Praca zbiorowa, *Zasady postępowania ratowniczego - poradnik dot. materiałów niebezpiecznych,* „Firex" Zakład Wydawnictw i Szkolenia Fundacji Rozwoju Ochrony Przeciwpożarowej, Warszawa 2004.
5. J. Tomasiewicz, *Terroryzm na tle przemocy politycznej*. http://www.terroryzm.com/article/267/Przemoc-w-ruchu-ekologicznym.html.
6. J. Adamski, *Ewolucja form działalności terrorystycznej na tle postępu technologicznego*, AON, Warszawa 2004.
7. http://wiadomosci.polska.pl/kalendarz/kalendarium/article.htm?id=87905.
8. http://www.tworzywa.com.pl/zagadnienia/zagadnienia.asp?ID=1161.
9. E. Kołodziejak-Nieckuła, T. Pająk, *Czy bać się dioksyn*, Wiedza i Zycie, Warszawa 1999. http://archiwum.wiz.pl/1999/99102900.asp.
10. E. Croddy, C. Perez-Armendariz, J. Hartem, *Broń chemiczna i biologiczna. Raport dla obywatela*, WNT, Warszawa 2005.
11. Ustawa z dnia 21 czerwca 2002 r. o materiałach wybuchowych przeznaczonych do użytku cywilnego (Dz. U. Nr 117, poz. 1007, z późn. zm.).
12. Komunikat Komisji *w sprawie poprawy warunków bezpieczeństwa materiałów wybuchowych* COM (2007) 651.
13. Rozporządzenia (WE) Nr 273/2004 Parlamentu Europejskiego i Rady z dnia 11 lutego 2004 r. w sprawie prekursorów narkotykowych, Załącznik nr 1 (Dz. UE L. 04.47.1).

ABSTRACT

The following article presents potential possibilities of terrorists using precursor supplies of toxic fighting products, dangerous chemicals and explosives, including their precursors obtained by entrepreneurs in Poland. The aim of this article is to indicate the scope and effects of terrorist activities strengthened by the use of the mentioned chemicals, including – first and foremost – the need for the best possible protection of such supplies.

Piotr Mickiewicz

Terroryzm morski i piractwo. Analiza zjawiska i formy przeciwdziałania na wybranym przykładzie

Wprowadzenie

Intensyfikacja działań przestępczych na akwenach morskich jest konsekwencją globalnych przeobrażeń w sferze politycznej, ekonomicznej i społecznej. Restytucja piractwa w Zatoce Adeńskiej oraz występujące akty terroru na akwenach morskich stanowią obecnie jedno z najpoważniejszych zagrożeń bezpieczeństwa, a skuteczne przeciwdziałanie im wymaga podjęcia działań ochronnych, zbrojnych oraz społeczno-ekonomicznych[1)]. Skala i charakter tego zjawiska powoduje, że niezbędne jest stworzenie skutecznego mechanizmu ograniczającego ryzyko wystąpienia bezprawnych aktów przemocy. Zasadne jest także ponowne zdefiniowanie pojęć *piractwo morskie* i *terroryzm na morzu*. Zbieżność form działań przestępczych powoduje, że trudno jest rozgraniczyć ich zakres. Za uzasadnione uznać należy również pogląd, że należy wprowadzić wspólną definicję prawną uznającą związek między piractwem i terroryzmem, czy wręcz zastąpienie w prawie międzynarodowym terminu *piractwo* przez pojęcie *terroryzm morski*[2)]. Politykę taką od ponad dekady prowadzi Federacja Rosyjska. Oceniając wdrażane przez to państwo rozwiązania należy stwierdzić, że ich naczelną zasadą jest skuteczne ograniczanie możliwości przeprowadzenia aktu piractwa lub terroru na morzu. Kierując się tą zasadą, ustawodawstwo rosyjskie skoncentrowało się na maksymalnym uszczegółowieniu i - w pewnym sensie - rozszerzeniu zakresu definicyjnego przestępczości na morzu. Przyjęte uregulowania różnią się znacznie od sposobów działania w tym zakresie np. Unii Europejskiej. Jednak sprawdziły się one doskonale na akwenach Zatoki Adeńskiej. Podejmowane przez rosyjskie okręty działania w postaci użycia uzbrojenia czy poddania piratów sankcjom w oparciu o ustawodawstwo wewnętrzne doprowadziło do przewartościowania układu sił zaangażowanych w zwalczanie tego procederu na tych akwenach.

[1)] Słusznie wskazuje na to szef sektora prawa karnego rosyjskiego Instytutu Państwa i Prawa Siergiej Maksymow, odnosząc się do problemu przeciwdziałania piractwu w Zatoce Adeńskiej. Stwierdził on, że [...]*same środki militarne do likwidacji piractwa są niewystarczające* [...] *Równocześnie jest sprawą jak najbardziej oczywistą, że na terytorium państwa, gdzie rząd nie daje sobie rady z zapewnieniem porządku prawnego i prześladowaniem przestępców, trzeba rozpatrywać kwestię ewentualnego wprowadzenia sankcji międzynarodowych. Oczywiście, nie chodzi o sankcje natury gospodarczej, lecz o wykonanie specjalnych akcji policyjnych.*Cytat za *RUVR. The Voice of Russia*, http://ruvr.ru/index.php?lng=pol.

[2)] Taka sugestia pojawiła się miedzy innymi w „New York Times" (wydanie z 15.12.2008). Jest ona również zbieżna z przedłożoną 15.07.2009 r. propozycją prezydenta Rosji, D. Miedwiediewa. Zakłada ona, między innymi, powołanie międzynarodowego trybunału zajmującego się karaniem sprawców aktów piractwa i wdrażaniem przez ONZ jednoznacznych rozwiązań zezwalających na skuteczne zwalczanie piractwa nie tylko na akwenach morskich, ale i na lądzie.

1. Przeciwdziałanie aktom piractwa i terroryzmu na morzu w rozwiązaniach międzynarodowych

Prawo do tworzenia międzynarodowych regulacji prawnych dotyczących żeglugi ma Międzynarodowa Organizacja Morska[3]. Opracowane pod jej auspicjami *Prawo Morza*[4] w sposób bardzo szeroki definiuje pojęcia p*iractwo* i *akt terroru*. Zgodnie z jej zapisami, aktem terroru na morzu jest podjęcie działań zmierzających do zajęcia statku lub przejęcie nad nim kontroli przy użyciu siły, fakt nakłaniania lub zmuszania do podjęcia takich działań lub prowadzenie innych działań zagrażających bezpieczeństwu żeglugi, w tym:

- dokonanie aktu przemocy przeciwko osobie znajdującej się na statku,
- uszkodzenie lub niszczenie statku lub ładunku,
- uszkodzenie urządzeń nawigacyjnych oraz przekazywanie fałszywych informacji[5].

Za piractwo *Konwencja Narodów Zjednoczonych o prawie morskim* uznaje natomiast:

- każdy bezprawny akt gwałtu, zatrzymania bądź grabieży statku lub mienia skierowany na morzu otwartym przeciwko innemu statkowi morskiemu lub powietrznemu, przeciwko osobom lub mieniu znajdującemu się na pokładzie takiego statku morskiego lub powietrznego,
- akt dobrowolnego uczestnictwa w działaniu statku morskiego lub powietrznego z wiedzą o faktach, które nadają mu charakter pirackiego statku morskiego lub powietrznego,
- podżeganie lub umyślne ułatwianie powyższych czynów[6].

---

[3] Posiada ona status Organizacji Wyspecjalizowanej systemu ONZ, a zakres jej działalności dotyczy problematyki bezpieczeństwa na morzu oraz zapobiegania zanieczyszczeniu środowiska morskiego. Status członków tej organizacji posiadają 162 państwa (w tym trzy są członkami stowarzyszonymi), a 36 organizacji międzyrządowych posiada umowy o współpracy z IMO. Dorobek prawny tej organizacji to kilka konwencji oraz szereg rezolucji i okólników regulujących zasady wykorzystania morza. Zob. *Leksykon Bezpieczeństwa Morskiego*, Gdynia 2009 i D. R. Bugajski, *Międzynarodowe organizacje morskie*, Gdynia 2009.

[4] Prawo Morza stanowi system rozwiązań międzynarodowych, opartych na usankcjonowanym zwyczaju oraz umowach ponadnarodowych. W praktyce określa ono sytuację prawną obszarów morskich i statków, reguluje zasady wykorzystania akwenów morza pełnego, znajdujących się poza zasięgiem zwierzchnictwa terytorialnego państw nadbrzeżnych oraz unifikuje przepisy wewnętrzne dotyczące obrotu morskiego. Najważniejszym dokumentem, regulującym te kwestie jest *Konwencja Narodów Zjednoczonych o prawie morza* z 10 grudnia 1982 (*Konwencja Jmajska)*. Pełny tekst konwencji zob. m.in. *www.lex.com.pl/serwis/du/2002/0544.htm.*

[5] Społeczność międzynarodowa nie wypracowała jednej, powszechnie akceptowanej definicji terroryzmu morskiego. Najczęściej cytowaną jest definicja zaakceptowana przez Radę ds. Bezpieczeństwa i Współpracy w Regionie Azji i Pacyfiku (*Council for Security and Cooperation in the Asia-Pacific – CSCAP*). Według niej, terroryzm morski to *działalność prowadzona w środowisku morskim, skierowana przeciwko statkom, stałym platformom na morzu lub w porcie oraz ich pasażerom albo pracownikom, a także przeciwko infastrukturze nadbrzeżnej, włączając w to obiekty turystyczne, obszar portu oraz miasta portowe.* Zob. G. Ong, *Ships can be dangerous too – coupling piracy and maritime terrorism in Southeast Asia`s maritime security framework*, Singapur 2004, s. 17; Michael D. Greenberg, Peter Chalk, Henry H. Willis, Ivan Khilko, David S. Ortiz, *Maritime terrorism: risk and liability.*, RAND Centre for Terrorism Risk Management Policy 2006, s. 9.

[6] Możliwe formy ataku terrorystycznego oraz aktu piractwa i ich następstwa szeroko omówione zostały w: K. Kubiak, A. Makowski, P. Mickiewicz, *Polska wobec zagrożenia terroryzmem morskim*, Warszawa 2005, s. 73-140 oraz M. Ilnicki, K. Kubiak, P. Mickiewicz, *Morski transport ropy i gazu w warunkach zagrożenia aktami przemocy*, Wrocław 2006, s 67-97.

Rozwiązania te tylko pozornie stwarzają możliwości skutecznego zwalczania powyższych zjawisk. Zakres możliwych form przeciwdziałania ogranicza obowiązek stosowania zapisów *Prawa Morza*. Jego podstawę – w odniesieniu do morza otwartego[7] – stanowią trzy zasady, określane jako: wolność mórz, swoboda (wolność) żeglugi, oraz prymat uprawnień państwa bandery. Rozgraniczają one jednoznacznie zakres uprawnień państw na akwenach morskich, dzieląc je na:

- prawa wynikające z jurysdykcji terytorialnej na akwenach wód wewnętrznych i terytorialnych;
- uprawnienia o charakterze jurysdykcji funkcjonalnej, w postaci szczegółowego określenia praw państwa na poszczególnych akwenach.

Stosowane przez IMO definicje pozwalają na uznanie za proceder piractwa czy terroru praktycznie większość aktów przemocy na morzu. Ale jednocześnie obowiązek stosowania przedstawionych powyżej zasad swobody żeglugi i uprawnień państwa bandery w praktyce uniemożliwia podjęcie skutecznych form przeciwdziałania, zwłaszcza o charakterze prewencyjnym. Zgodnie z zapisami *Konwencji Prawo Morza, zajęcie pirackiego statku morskiego jest możliwe przez jednostkę pozostającą w służbie państwowej, a o wymiarze kary czy też dalszym postępowaniu z takim obiektem decydują sądy państwa, którego jednostki zajęły statek*[8]. Ponadto, jeżeli statek został zajęty bez dostatecznych podstaw, państwo, które dokonało takiego czynu, ponosi odpowiedzialność za szkody związane z działalnością wobec państwa przynależności państwowej statku (morskiego lub powietrznego). Przedstawione zapisy powodują, że za podstawowe formy podejmowanych działań uznaje tzw. prawo wizyty oraz prawo pościgu[9]. Pierwsze z nich (prawo wizyty) sprowadza się do przeprowadzenia kontroli statków na morzu pełnym przez jednostki pozostające w służbie państwowej. Kontrola ta może jednak mieć miejsce tylko w przypadku zaistnienia podejrzenia, iż kontrolowany statek:

- zajmuje się procederem piractwa lub handlem narkotykami,
- nadaje nielegalne audycje radiowe,
- nie posiada przynależności państwowej i jest w sytuacji, w której statek podnosi tę samą banderę, co jednostka pozostająca w służbie państwowej, lecz odmawia ujawnienia tego faktu[10].

Natomiast do prawa pościgu na morzu pełnym upoważnione są jednostki w służbie państwowej (w tym także samoloty i statki powietrzne), które rozpoczęły go w momencie, gdy jednostka innej bandery naruszyła przepisy prawne obowiązujące na wodach wewnętrznych lub morzu terytorialnym państwa ścigającego. Prawo wykony-

---

[7] Na akwenach morza otwartego (morze pełne) jurysdykcji nie może sprawować żadne państwo. Obowiązują na nim natomiast prawa gwarantujące: prawo swobodnej żeglugi, rybołówstwa, układania kabli podmorskich i rurociągów, prowadzenia badań naukowych oraz budowy instalacji i sztucznych wysp. Tamże.

[8] Artykuł 105 *Konwencji Narodów Zjednoczonych o prawie morza*. Natomiast zgodnie z artykułem 106, jeżeli statek został zajęty bez dostatecznych podstaw, państwo, które dokonało takiego czynu, ponosi odpowiedzialność za szkody związane z działalnością wobec państwa przynależności państwowej statku (morskiego lub powietrznego).

[9] Zakres podejmowanych przedsięwzięć określony został w artykułach 110 i 111 *Konwencji Narodów Zjednoczonych o prawie morza*.

[10] Szerzej zob. D.R. Bugajski, *Prawa żeglugowe okrętu w świetle prawa międzynarodowego*, Warszawa 2009.

wania pościgu nie ma zastosowania, gdy ścigana jednostka wpływa na wody terytorialne państwa trzeciego lub własnego kraju[11].

2. *Międzynarodowe rozwiązania prawne a praktyka przeciwdziałania piractwu i terroryzmowi w rozwiązaniach Unii Europejskiej*

Nałożone przez prawo międzynarodowe ograniczenia spowodowały, że większość państw, określanych jako mocarstwa morskie[12], zdecydowała się na rozszerzenie rozwiązań zalecanych przez Międzynarodową Organizację Morską, przy zachowaniu pełnej aprobaty dla regulacji zawartych w *Konwencji Prawo Morza* i uszczegółowionych w sferze przeciwdziałania czynom przestępczym na morzu w przyjętej w 1988 roku *Konwencji Rzymskiej*[13]. Na akwenach europejskich obowiązują dwie formuły przeciwdziałania aktom piractwa i terroryzmu na morzu. Pierwsza z nich, wdrożona przez Unię Europejską, jest realizowana przez państwa członkowskie oraz współpracujące[14]. Zmierza ona do poprawy poziomu bezpieczeństwa żeglugi, w oparciu o system monitoringu żeglugi, zezwalającego na:

- stworzenie systemu nadzoru i monitorowania ruchu statków na akwenach Unii Europejskiej[15],
- wdrażanie adekwatnego do bieżącego stanu zagrożenia poziomu bezpieczeństwa konkretnego statku i obiektu portowego.

Zadaniem systemu nadzoru jest kontrola ruchu i identyfikacja jednostki znajdującej się na monitorowanym akwenie, dokonywana dzięki tzw. *Vessel Traffic Management Information System* (VTMIS)[16]. Natomiast rozwiązania wdrażane w ramach podnoszenia poziomu bezpieczeństwa statków i obiektów portowych są *de facto* rozszerzeniem zapisów wprowadzanych na mocy, opracowanego przez IMO *Międzynarodowego Kodeksu Ochrony Statku i Obiektu Portowego* (ISPS). Komisja Europejska zdecydowała się na wprowadzenie rozwiązań nie tylko obowiązujących w *Kodeksie*, ale również mających status zaleceń. Istotą funkcjonowania systemu monitoringu jest odbiór przez stację brzegową sygnału automatycznie nadawanego przez statek. Pozwala on na identyfikację i kontrolę trasy rejsu jednostek[17]. Natomiast podstawą ochrony

---

[11] K. Kubiak, A. Makowski, P. Mickiewicz, *Polska wobec zagrożenia terroryzmem morskim*, Warszawa 2005, s. 163-160.

[12] Jest to państwo, które posiada możliwości lub wolę polityczną do utrzymywania sił morskich, przeznaczonych do działań na dużych akwenach i potencjał pozwalający na kontrolowanie mórz poza własnymi akwenami.

[13] *Konwencja w sprawie przeciwdziałania bezprawnym czynom przeciwko bezpieczeństwu żeglugi morskiej* z dnia 10.03.1988 r. - Dz. U. z 1994 nr 129, poz. 635 (weszła w życie dnia 01.03.1992 r.).

[14] Szerzej zob. P, Mickiewicz, T. Szubrycht, K. Kubiak, *Akweny morskie w systemie reagowania kryzysowego,* w: J. Gryz (red.), *System reagowania kryzysowego UE. Struktura - charakter - obszary*, Wrocław 2009, s. 262-315.

[15] System ten tworzony jest w oparciu o *Dyrektywę nr* 2002/59/EC *Komisji Europejskiej* z 27 czerwca 2002 roku.

[16] Zasadniczymi elementami składowymi systemu VTMIS są: systemy nadzoru ruchu statków (VTS), systemy automatycznej identyfikacji statków (AIS), systemy meldunkowe okrętów (SRS), krajowy komputerowy system wymiany informacji – krajowy system SafeSeaNet.

[17] Zalicza się do nich: jednostki rybackie, statki handlowe o długości 65 stóp, jednostki pasażerskie uprawnione do przewożenia 150 pasażerów lub o wyporności powyżej 150 ton, statki holownicze o długości 26 stóp i więcej oraz mocy większej, niż 600 koni mechanicznych. Zob. http://www.navcen.uscg.gov/enav/ais/default.htm.

statku jest indywidualnie przygotowywany, tzw. *Plan ochrony statku (Ship Security Plan-SSP*)**,** polegający w praktyce na wprowadzeniu szczegółowych rozwiązań chroniących statek[18]. Podobne rozwiązania obowiązują w portach państw członkowskich, a ich podstawą jest opracowany w oparciu o wspomnianą Konwencję ISPS indywidualny *Plan Ochrony Obiektu Portowego (Port Facility Security Plan - PFSP*)[19]. W obydwu rozwiązaniach państwa europejskie, wdrażając zalecenia Komisji Europejskiej, rozszerzyły zakres stosowanych rozwiązań. Jako obligatoryjne na statkach i w portach państw UE uznano zapisy *ISPS*, posiadające status zaleceń. Ponadto, za obszary objęte postanowieniami *Kodeksu ISPS* uznano pozostałe obiekty okołoportowe, w tym stocznie. Natomiast podstawowymi środkami zapobiegawczymi są działania zmierzające do ograniczenia dostępu do obiektu portowego oraz szczegółowe procedury reagowania na zagrożenia w postaci naruszenia systemu ochrony.

Unijna koncepcja zwalczania piractwa i terroryzmu na morzu zakłada, że odpowiedni poziom bezpieczeństwa ma zapewnić system monitoringu akwenów. Operacja antypiracka (antyterrorystyczna) jest rozwiązaniem ostatecznym, co powoduje, iż większość działań podejmowanych na akwenach morskich sprowadza się do selekcji jednostek uznawanych za podejrzane, monitorowaniu ich ruchu oraz ewentualnym przeprowadzeniu kontroli poprzez zastosowanie tzw. prawa wizyty. Kontrola odbywa się po wcześniejszym uprzedzeniu kapitana kontrolowanej jednostki i zobowiązaniu go do przygotowania załogi do kontroli (kapitan jest zobowiązany do udostępnienia wszystkich pomieszczeń oraz zebrania załogi w wyznaczonym miejscu). Ze względu na ograniczony czas kontroli, jej zakres sprowadza się do równoległego sprawdzenia dokumentacji oraz przeszukania części pomieszczeń i ładunku. Jedynie w przypadku stwierdzenia niezgodności lub uchybień, jednostka poddawana jest szczegółowej kontroli lub kierowana do wyznaczanego portu[20].

Przeprowadzenie klasycznej operacji opanowania jednostki, w przypadku działań podejmowanych przez państwa UE, może nastąpić w sytuacji skrajnej, za którą uznaje się porwanie zakładników lub narażenie życia. Standardowo celem grup antyterrorystycznych państw unijnych jest przeprowadzenie akcji abordażowej. Zadaniem

---

[18] Plan ochrony statku zawiera ocenę stanu zagrożeń i prawdopodobieństwo ich zaistnienia, wskazówki, dotyczące niezbędnych środków ochrony, słabe punkty w infrastrukturze jednostki oraz sfery wymagające ochrony. Uwzględnia się w nim także wymagania dotyczące poziomu wyszkolenie załogi, formy niezbędnych treningów, sposoby rejestrowania symptomów wskazujących na zaistnienie zagrożenia aktem terroru. Za jego realizację odpowiada Oficer Ochrony Statku (*Ship Security Officer*), do którego obowiązków należy zapewnienie poprawnego wdrażania planu ochrony statku, wyszkolenie załogi w tym zakresie oraz utrzymywanie statku w tak zwanej „świadomości związanej z ochroną". Zob. M. Ilnicki, K. Kubiak, P. Mickiewicz, *Morski transport ropy i gazu w warunkach zagrożenia aktami przemocy*, Wrocław 2006, s 116-124.

[19] *Port Facility Security Plan* zawiera między innymi: wykaz środków ograniczających dostęp osób nieupoważnionych do obiektu portowego, statków w nim zacumowanych oraz do obszarów o ograniczonym dostępie i zapobiegających możliwości wniesienia na teren obiektu portowego lub na statek broni, niebezpiecznych substancji oraz przedmiotów umożliwiających ich wykorzystanie przeciwko osobom, statkom lub obiektowi portowemu; procedury reagowania na zagrożenia lub naruszenia ochrony, szczególnie w przypadku wprowadzenia najwyższego poziomu zagrożenia, aktywacji systemu alertu o zagrożeniu ochrony statku na statku przebywającym w porcie; procedury ewakuacyjne w przypadku zagrożenia bezpieczeństwa, umożliwiające zejście załogi statku na ląd lub wymianę załogi i powiadamiania o zdarzeniach naruszających bezpieczeństwo; zadania personelu obiektu portowego i środki zapewniające skuteczną ochronę ładunku oraz sprzętu przeładunkowego w porcie. Tamże.

[20] Zob. K. Kubiak, P. Mickiewicz, M Rosiak, A. Szulczewski, *Koncepcja działania grupy kontrolno-inspekcyjnej w warunkach MW RP*, „Przegląd Morski", 2002, nr 4.

sił wspierających jest próba rozproszenia uwagi piratów (terrorystów), a nie ostrzał lub prowadzenie innych działań o charakterze zbrojnym[21]. Celem działań abordażowych jest zajęcie statku i obezwładnienie znajdujących się na nim osób. Zasadą jest, że komandosi dopiero po obezwładnieniu osób dokonują filtracji (działania ukierunkowane na ograniczenie możliwości wmieszania się terrorystów w grupy uwolnionych zakładników), selekcji zatrzymanych, udzielają pomocy medycznej i przeprowadzają sukcesywną ewakuację z zajętego statku.

3. Przeciwdziałanie piractwu i terroryzmowi w rozwiązaniach Federacji Rosyjskiej

Przeciwdziałanie aktom piractwa i terroryzmu na morzu w polityce rosyjskiej stanowi element przedsięwzięć ukierunkowanych na zwalczanie przestępczości zorganizowanej na akwenach morskich. Z tego względu system monitoringu żeglugi i akwenów morskich nie jest uznawany za zasadniczy instrument umożliwiający skuteczne ograniczanie tego rodzaju przestępczości[22]. Decydując się na jego wdrożenie, zrealizowano wymóg IMO, ale jednocześnie uznano, iż będzie on wykorzystywany głównie jako zautomatyzowana i scentralizowana baza danych o pasażerach przewożonych przez przewoźników rosyjskich i zagranicznych[23]. W odmienny sposób potraktowano natomiast rozwiązania *Kodeksu ISPS*. Uznając, że pozwala on na przygotowanie załóg i portów do przeciwdziałania aktom piractwa i terroru, Rosjanie zdecydowali się na wprowadzenie standardowych rozwiązań, znacznie rozszerzając definicję obiektów objętych jego zakresem. Został on dosyć ściśle określony w ustawie *O bezpieczeństwie transportu*[24], która, między innymi, definiuje pojecie czynu przestępczego podejmowanego wobec tzw. obiektu infrastruktury transportowej. Zgodnie z przyjętymi rozwiązaniami, za morski obiekt infrastruktury transportowej uznaje się dworce i porty morskie (handlowe, rybackie, specjalistyczne) oraz rzeczne, obiekty portowe wraz z urządzeniami, budowle hydrotechniczne, obiekty zarządzania ruchem i transportem morskim oraz inne budynki zabezpieczające prawidłowe funkcjonowanie morskiego kompleksu transportowego. Ustawa zalicza do tych obiektów również całość infrastruktury dojaz-

[21] Zadaniem jednostek nawodnych i statków powietrznych (śmigłowców) jest prowadzenie manewrów mających na celu rozproszenie piratów (terrorystów) i umożliwienie podjęcia próby abordażu na pokład uprowadzonej jednostki. Akcję taką przeprowadza kilka sekcji abordażowych, wyposażonych z reguły w liny, bosaki i drabinki oraz broń osobistą. Zasadą jest przeprowadzenie abordażu z morza (w zależności od wielkości jednostki dokonują tego dwie – trzy sekcje). W uzasadnionych przypadkach stosuje się także, przeprowadzany równolegle lub z opóźnieniem, abordaż z powietrza.

[22] Jego walory w większym stopniu stwarzają możliwość uzyskania informacji o ruchu jednostek przewożących ładunki niebezpieczne, czy podejrzanych o możliwość popełnienia przestępstwa na morzu. Postawa ta wynika z przekonania o niskiej skuteczności wprowadzonych rozwiązań w sferze zwalczania przestępczości na morzu. Ale równie ważnym powodem jest możliwość wykorzystania systemu monitoringu do kontroli ruchu jednostek przewożących ładunki niebezpieczne i stwarzających zagrożenie katastrofy ekologicznej na akwenach morskich. W sytuacji radykalnego wzrostu dostaw ropy naftowej i jej przetworów drogą morską wdrożenie tego rozwiązania stanowić może poważne ograniczenie planów zdominowania dostaw surowców energetycznych na obszar Europy.

[23] Baza taka zawiera najistotniejsze dane osobowe pasażera, w tym: nazwisko, imię, imię ojca; datę i miejsce urodzenia; numer dokumentu potwierdzającego personalia osoby posiadającej bilet; dane przebiegu podróży, z zaznaczeniem jej trasy oraz czasu trwania. Zob. *Fiedieral'nyj zakon Rossijskoj Fiedieracyjii ot 9 fiewralja 2007 g. N 16-F3 O transportnoj biezopasnosti, s. 5.*

[24] *Fiedieral'nyj zakon Rossijskoj Fiedieracyji ot 9 fiewralja 2007 g. N 16-F3 O transportnoj biezopasnosti,* Ustawa obowiązuje od 14 sierpnia 2007 roku.

dowej do portów morskich i rzecznych[25]. System ochrony tych obiektów w praktyce jest oparty na rozwiązaniach przyjętych przez *Kodeks ISPS*.

Przedstawione podejście do implementacji rozwiązań międzynarodowych pozwala, z jednej strony, na pełną akceptację międzynarodowych rozwiązań dotyczących swobody żeglugi i prawnej jurysdykcji państwa bandery. Równocześnie jednak umożliwia skuteczne przeciwdziałanie aktom przestępczym, w tym piractwu i terroryzmowi na morzu. W cytowanej ustawie, oprócz implementacji rozwiązań międzynarodowych, dokonano także stosownego rozszerzenia niektórych jego zapisów. Wprowadzono w niej pojęcie tzw. aktu bezprawnej ingerencji, który określa się jako *działanie niezgodne z prawem z włączeniem w to aktów terrorystycznych, a także gróźb wobec kompleksów transportowych, które mogą pociągnąć za sobą spowodowanie uszczerbku zdrowia lub życia ludzi*"[26]. Pojęcie to rozszerza powszechnie stosowane w *Konwencji Prawo Morza* definicje piractwa i terroryzmu na morzu. Ponadto, w oparciu o tę definicję określono także zadania państwa rosyjskiego w zakresie zapewnienia bezpieczeństwa transportu. Za takowe uznano wszelkie *„czynności prawne, ekonomiczne i organizacyjne wykonywane przez państwo, a mające na celu zabezpieczenie kompleksu transportowego przed aktami bezprawnej ingerencji*.

4. *Sankcje karne wobec sprawców aktów piractwa i terroru na morzu w rozwiązaniach prawnych Federacji Rosyjskiej*

Zasadą sukcesywnie wdrażanych od 1996 roku rozwiązań legislacyjnych dotyczących zwalczania zorganizowanej przestępczości na akwenach morskich jest pełne podporządkowanie się wymogom międzynarodowego prawa morza przy jednoczesnym znacznym rozszerzeniu zakresu sankcji karnych. W obowiązującym kodeksie karnym definicja aktu piractwa jest w pełni zbieżna z zapisami *Konwencji Prawo Morza*. Za akt piractwa uznaje się w nim *napad na statek morski lub rzeczny, dokonany z użyciem siły lub z zagrożeniem jej zastosowania oraz pozostałe czynności mające na celu przygotowanie napadu*[27]. Również rosyjska wykładnia pojęcia „piractwo" nie odbiega od definicji prawa międzynarodowego. Za akt piractwa uznaje się w nim wszelkie działania, skierowane na osiągnięcie rezultatu przestępczego na drodze stosowania siły wobec poszkodowanych, bądź stworzenia (fakt przygotowania) realnego zagrożenia niezwłocznego jej użycia**.** Tym samym stwierdzić należy, że „piractwo" w myśl rosyjskiego systemu karnego, to działania skierowane przeciwko członkom załogi oraz pasażerom, które są ukierunkowane na:

- zawładnięcie statkiem lub ładunkiem czy wyposażeniem znajdującym się na jego pokładzie,
- wyrządzenie krzywdy fizycznej załodze i pasażerom porwanej jednostki,
- porwanie z użyciem siły i zatrzymanie statku,
- porwanie w celu uzyskania okupu[28].

---

[25] Są to kompleksy obsługujące żeglugę śródlądową, linie kolejowe, tramwajowe i autobusowe, a także tunele, estakady, mosty oraz dworce. Tamże

[26] Artykuł 1 ustawy *Fiedieralnyj zakon Rossijskoj Fiedieracyji ot 9 fiewralja 2007 g. N 16-F3 O transportnoj biezopasnosti*.

[27] Artykuł 30 *Kodeksu Karnego Federacji Rosyjskiej*.

[28] Postanowienie Sądu Najwyższego Federacji Rosyjskiej *O praktyce zastosowania ustawodawstwa o odpowiedzialności za bandytyzm przez statki* z dnia 17 stycznia 1997 roku.

Równocześnie jednak do rosyjskiego systemu legislacyjnego wprowadzono szereg rozszerzeń zaczerpniętych z rozwiązań międzynarodowych. Między innymi, dokonano kategoryzacji aktów piractwa, dzieląc je na trzy kategorie, które tworzą tzw. piractwo: proste, wykwalifikowane i szczególnie wykwalifikowane. Podstawowym ryterium definicyjnym jest niejednokrotność dokonania aktu piractwa, rozumiana jako dokonanie dwóch lub więcej przestępstw przewidzianych jednym artykułem lub częścią artykułu kodeksu karnego[29], fakt posiadania broni i jej wykorzystania. Wprowadzono także szczegółowe zapisy dotyczące odpowiedzialności prawnej sprawców aktu piractwa oraz zakresu jurysdykcji prawa rosyjskiego wobec sprawców przestępstw na morzu. Zgodnie z rozwiązaniami rosyjskimi, odpowiedzialność prawną za akt piractwa ponosi osoba poczytalna, która osiągnęła wiek 16 lat. Zaś rosyjską jurysdykcją prawną objęci zostali także:

- obcokrajowcy przebywający na terenie Rosji i jej akwenach morskich,
- osoby pracujące na statkach, które pływają pod banderą Federacji Rosyjskiej,
- załogi jednostek pod banderą obcą, ale znajdujących się w granicach wewnętrznych wód oraz morza terytorialnego Federacji Rosyjskiej, jak również poza granicami kraju w przypadkach przewidzianych międzynarodowymi umowami, które podpisała Federacja Rosyjska.

Podobną zasadę do swoich rozwiązań prawnych Rosja wprowadziła w sferze zwalczania terroryzmu na morzu. Akceptując w pełni międzynarodowe rozwiązania dotyczące definicji aktów terroru na morzu i zakresu działań antyterrorystycznych, jednoznacznie określono cel tych operacji[30]. Zgodnie z zapisami ustawy *O walce z terroryzmem*[31] obiektem działań antyterrorystycznych mogą być:

- statki pływające pod państwową banderą Federacji Rosyjskiej w wodach wewnętrznych na morzu terytorialnym Federacji Rosyjskiej oraz na pełnym morzu,
- statki pływające na akwenach morskich Federacji Rosyjskiej będące pod banderą państwa zagranicznego,
- statki pływające pod banderą Federacji Rosyjskiej na obszarach morskich innego państwa,

---

[29] Termin „niejednorodność" precyzuje artykuł 16 kodeksu karnego. Autorzy kodeksu wyszli z założenia, że akty piractwa najczęściej dokonywane są przez zorganizowane grupy przestępcze. Zaś definicję grupy przestępczej zawiera artykuł 35 kodeksu karnego. Za taką grupę uznaje się „*stałą grupę osób połączonych w celu dokonania jednego lub kilku przestępstw*". Grupa ta charakteryzuje się stałą więzią między współuczestnikami, a także strukturą organizacyjną. Może ona być utworzona w celu dokonania jednego lub większej ilości przestępstw. W wyniku działań pirackich może dojść do spowodowania śmierci członków załogi będącej rezultatem napadu. W omawianym kodeksie istnieje zapis o spowodowaniu śmierci przez nieostrożność. Mówi o tym artykuł 24. Zaznaczyć trzeba, iż w przypadku piractwa można się spotkać z umyślnym spowodowaniem śmierci jednej bądź kilku osób. W takim przypadku wymagana jest dodatkowa kwalifikacja, zgodna z artykułem 105.

[30] Zgodnie z międzynarodowymi rozwiązaniami, w przypadku zaistnienia aktu terroru na akwenach morskich celem działań jest:

- uwolnienie pasażerów i załogi porwanego statku,
- unieszkodliwienie napastników, którzy zdobyli lub próbują zdobyć statek,
- zapewnienie bezpieczeństwa innym statkom, ich pasażerom i załodze,
- zapewnienie bezpieczeństwa pracownikom organizacji morskich oraz obiektów portowych w przypadku dokonania bezprawnych aktów w porcie morskim.

[31] *Zarządzenie Rządu Federacji Rosyjskiej z dnia 30 lipca 2004 roku numer 398 O federalnej służbie nadzoru w dziedzinie transportu odpowiada Służba Morskiego Bezpieczeństwa. Położenije o fiedieral'noj sistiemie zaszczity morskowo sudochodstwa ot niezakonnych aktow, naprawliennych protiw biezapasnosti miepławanija,* zatwierdz. przez zarządzenie Rządu FR z 11 kwietnia 2000 r., nr 324, s. 4.

- statki pływające pod banderą zagraniczną, ale z obywatelami Federacji Rosyjskiej na pokładzie.
- obiekty zarządzania ruchem morskim, nawigacji morskiej, infrastruktury portowej oraz ich personel, znajdujący się na terytorium Federacji Rosyjskiej[32].

Ustawa ta tworzy także prawne podstawy umożliwiające podjęcie działań nie tylko na rosyjskich wodach wewnętrznych, ale także na morzu otwartym[33]. Samo przeprowadzenie działań prewencyjnych uwarunkowane jest wyłącznie posiadaniem sił i środków złożonych z federalnych organów władzy wykonawczej. Zaś wymogiem o charakterze ponadnarodowym jest obowiązek informowania o zaistniałym działaniu bezprawnego aktu przeciwko żegludze danego państwa lub grupy państw w przypadku, gdy na statku, na którym miało miejsce przedsięwzięcie na obszarach morskich Federacji Rosyjskiej znajdują się obcokrajowcy. Informacje o zaistniałym zdarzeniu przesyła się kanałami dyplomatycznymi do przedstawicielstw tych krajów znajdujących się na terytorium Federacji Rosyjskiej. Przewidywane przez rosyjskie rozwiązania sposoby prowadzenia operacji antyterrorystycznych i antypirackich to:
- ostrzał jednostki podejrzanej o akt piractwa,
- odbijanie porwanych jednostek,
- zabezpieczanie jednostek poprzez system monitoringu i reakcji na wezwanie.

Podsumowanie

Dokonując oceny rozwiązań wdrażanych przez Federację Rosyjską należy stwierdzić, że wynikają one z przekonania o ograniczeniach, jakie nakłada Międzynarodowe Prawo Morza. W rosyjskiej polityce zwalczania przestępczości na morzu naczelną zasadą jest skuteczne ograniczanie skali tego zjawiska. Jej prymat powoduje, że ustawodawstwo rosyjskie skoncentrowało się na maksymalnym uszczegółowieniu i – w pewnym sensie – rozszerzeniu zakresu definicyjnego przestępczości na morzu (w tym piractwa i terroryzmu). Gros podejmowanych przedsięwzięć zmierza do opracowania zbieżnych z generalnymi zasadami Prawa Morza sankcji karnych dla przestępców oraz rozszerzenia zakresu jurysdykcji państwa poddanego aktowi przestępstwa w stosunku do państwa bandery. Natomiast marginalnie traktowana jest działalność związana z monitoringiem ruchu jednostek. Polityka ta wynika z negatywnych konsekwencji, jakie niesie za sobą system nadzoru żeglugi. Jego immanentną częścią jest kontrola zanieczyszczeń akwenów morskich i przeciwdziałanie zagrożeniu wystąpienia katastrofy na morzu. Jednym z podstawowych rosyjskich towarów eksportowych transportowanych, drogą morską jest ropa naftowa i jej przetwory. Równie istotnym czynnikiem jest stan techniczny rosyjskich (i czarterowanych przez rosyjskich armatorów) jednostek, które nie zawsze spełniają unijne normy techniczne. Obecnie jedyną konsekwencją dla takich jednostek jest zakaz wstępu do unijnych portów, co nie uniemożliwia przebywania na wokółeuropejskich akwenach. Natomiast wdrożenie systemu monitoringu wymagałoby konsekwentnej i szybkiej przebudowy rosyjskiej floty transportowej.

[32] Tamże, s. 5.

[33] Przewiduje on ewentualne podjęcie działań na wodach państwa trzeciego za jego zgodą lub na wniosek.

Porównując rosyjską koncepcję zwalczania zagrożenia przestępczością na morzu z rozwiązaniami unijnymi[34] należy stwierdzić, iż obejmuje ona szerszy zakres działań oraz jest bardziej restrykcyjna. Pomimo ograniczeń co do zakresu form podejmowanych działań antypirackich i antyterrorystycznych, unijny system przeciwdziałania należy uznać za bardziej efektywny w wymiarze regionalnym. Zapewnia on stały monitoring sytuacji i stwarza szansę na podjęcie skutecznych działań o charakterze prewencyjnym. Natomiast słabością tego rozwiązania, co ukazuje casus Zatoki Adeńskiej[35], jest ograniczenie jurysdykcji prawnej wobec osób podejrzanych o prowadzenie piractwa lub terroryzmu na akwenach morskich. Ścisłe stosowanie się do zapisów Prawa Morza dotyczących statusu państwa bandery uniemożliwia zastosowanie sankcji prawnych wobec takich osób, gdy nie nastąpi akt przestępczy. Przedstawione uwarunkowania znacznie ograniczają zakres możliwej współpracy Unii Europejskiej i Federacji Rosyjskiej w sferze ochrony bezpieczeństwa na morzu, w tym zwalczania przestępczości na akwenach morskich. Zwalczanie piractwa i przeciwdziałanie aktom terroru na morzu pozostanie w gestii poszczególnych państw. Możliwym rozwiązaniem jest korelacja podejmowanych działań, a zwłaszcza informacja o skali zagrożenia. Natomiast nie jest możliwa wzajemna, nawet częściowa, implementacja wzajemnych rozwiązań w sferze zwalczania piractwa i aktów terroru na morzu.

ABSTRACT

Scale and nature of crime at sea results in necessity of creating the effective counteract mechanism. For a decade ‚such policy has been pursued by the Russian Federation. Assessing its implementation, it should be stated that the first priority for the Russian Federation is the effective decrease of the possibility of conducting the acts of piracy or terror at sea. Having this principle in mind, the Russian legislation concentrated on maximum rigorousness and-in a way-broadening the meaning of crime at sea definition. The adapted methods differ, to great extent, from the ways accepted for instance by the European Union. However, they proved perfect within the waters of Aden Bay.

[34] Dla Komisji Europejskiej podstawowym założeniem jest literalne przestrzeganie zasad wolności mórz i jurysdykcji państwa bandery. Polityka taka jest konsekwencją zarówno uznania konieczności stosowania rozwiązań międzynarodowych, jak i prowadzonej zgodnie z wymogami stawianymi mocarstwu morskiemu polityki obecności na akwenach morskich. Utrzymanie liberalnego charakteru żeglugi, a zwłaszcza swobody żeglugi oraz ograniczonych praw państwa kontrolującego akwen, jest jednym z najważniejszych założeń budowy europejskiego systemu strumieni transportowych w wymiarze globalnym i regionalnym. Stworzenie prawnych możliwości kontroli jednostki przez państwo kontrolujące akwen, możliwość tworzenia morskich stref kontrolnych poprzez np. ogłaszanie akwenów pod nadzorem i swobodne wykorzystywanie prawa wizyty może negatywnie oddziaływać na morski system przewozów, stanowiący jeden z zasadniczych środków wymiany towarowej państw europejskich.

[35] Przykładem jest fakt zwolnienia załóg jednostek podejrzanych o piractwo przez okręt duński i niemiecki po wcześniejszym zatopieniu znalezionej na pokładach tych jednostek broni.

Tomasz Szewczyk
Maciej Pyznar

Ochrona infrastruktury krytycznej a zagrożenia asymetryczne

Termin zagrożenia asymetryczne już od dłuższego czasu funkcjonuje zarówno w teorii stosunków międzynarodowych, jak i w nauce o bezpieczeństwie. Należy podkreślić, że istnieje wiele koncepcji związanych z definiowaniem powyższego terminu oraz jego klasyfikacji. Dla potrzeb tego artykułu zagrożenie asymetryczne zdefiniowane zostanie jako działanie podmiotu, przede wszystkim pozapaństwowego, który wykorzystuje niekonwencjonalne z punktu widzenia swego przeciwnika środki i techniki. Jako zagrożenia asymetryczne wyróżnić możemy m.in.: terroryzm międzynarodowy, użycie przez podmioty pozapaństwowe broni masowego rażenia oraz wrogie zastosowanie technologii informatycznych (cyberterroryzm)[1].

Ochrona infrastruktury krytycznej

W wyniku zdarzeń spowodowanych przez siły natury lub będących konsekwencją działań człowieka infrastruktura krytyczna może ulec zniszczeniu, uszkodzeniu, a jej działanie zakłóceniu, w związku z czym zagrożone może być życie i mienie. Równocześnie tego typu wydarzenia negatywnie wpływają na rozwój gospodarczy państw.

Infrastruktura krytyczna pełni kluczową rolę w funkcjonowaniu państwa i życiu jego obywateli, a jej ochrona jest jednym z priorytetów stojących przed państwem polskim. Istota zadań związanych z infrastrukturą krytyczną sprowadza się nie tylko do zapewnienia jej ochrony, ale również do tego, aby ewentualne uszkodzenia i zakłócenia w jej funkcjonowaniu były możliwie krótkotrwałe, łatwe do usunięcia i nie wywoływały dodatkowych strat dla obywateli i gospodarki.

Infrastruktura krytyczna oraz jej ochrona to pojęcia stosunkowo nowe. Po raz pierwszy pojawiły się w oficjalnych dokumentach państwowych w USA wraz z dyrektywą prezydenta Billa Clintona z 22 maja 1998 r. w sprawie ochrony infrastruktury krytycznej. Dyrektywa ta wskazywała na konieczność wzrostu wrażliwości Stanów Zjednoczonych na ewentualne ataki terrorystyczne, ze zwróceniem szczególnej uwagi na bezpieczeństwo infrastruktury krytycznej. Tego typu infrastrukturę zdefiniowano jako rzeczywiste i cybernetyczne systemy niezbędne do funkcjonowania gospodarki i państwa w minimalnym zakresie. Wśród tych systemów wymieniono m.in.: system telekomunikacyjny, energetyczny, transportowy, bankowy i finansowy. Co znamienne, podkreślono, iż w celu efektywnej ochrony infrastruktury krytycznej zachodzi konieczność ścisłej współpracy z sektorem prywatnym (wg danych Departamentu Bezpieczeństwa Narodowego USA, operatorami lub właścicielami około 85% infrastruktury krytycznej są podmioty prywatne) w ramach partnerstwa publiczno-prywatnego. Od tego czasu zagadnienia ochrony infrastruktury krytycznej były systematycznie rozwijane, a Amerykanie stali się światowymi liderami w tej dziedzinie.

---

[1] Definicja została zaczerpnięta z książki M. Madeja – *Zagrożenia asymetryczne bezpieczeństwa państwa obszaru transatlantyckiego,* PISM, Warszawa 2007, która w sposób kompleksowy opisuje zagadnienie, przedstawiając jego wieloaspektowość.

W polskim prawodawstwie pojęcie infrastruktury krytycznej nie było obecne. Brakowało definicji w dokumencie rangi ustawy lub rozporządzenia. Jednakże brak jednoznacznych przepisów definiujących tego typu infrastrukturę i jej ochronę nie oznaczał, że w ogóle jej nie było, lub że nie była ona chroniona.

W Polsce dostrzegano konieczność ochrony niektórych składników infrastruktury państwa. Już w 1997 r. przyjęto ustawę o ochronie osób i mienia, w której wskazano obszary, obiekty, urządzenia i środki transportu, mające znaczenie dla obronności, gospodarki, bezpieczeństwa publicznego i innych ważnych interesów państwa, które miały być obowiązkowo chronione przez specjalne, uzbrojone formacje lub odpowiednie zabezpieczenie techniczne.

W ramach ochrony obowiązkowej, kierownik jednostki, który bezpośrednio zarządza obszarami, obiektami i urządzeniami umieszczonymi w ewidencji albo upoważniona przez niego osoba, zobowiązany zostaje do opracowania oraz uzgodnienia z właściwym terytorialnie komendantem wojewódzkim policji planu ochrony tych obszarów, obiektów i urządzeń. Dodatkowo, w 2003 roku, przyjęto rozporządzenie Rady Ministrów w sprawie obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa oraz ich szczególnej ochrony, które regulowało sprawę ochrony tych obiektów w warunkach pozapokojowych. Natomiast podstawy do zdefiniowania i zapewnienia odpowiedniej ochrony krytycznej infrastruktury teleinformatycznej zawarto w ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych. Należy podkreślić, że polska administracja miała styczność z pojęciem infrastruktury krytycznej podczas uczestnictwa w pracach toczących się zarówno na forum Paktu Północnoatlantyckiego, jak i Unii Europejskiej[2)].

Można zatem wnioskować, iż dotychczasowy stan prawny zawierał przepisy dotyczące ochrony tego typu infrastruktury. Dążąc do pełniejszego jej zabezpieczenia, w ślad za innymi krajami oraz instytucjami UE, w administracji polskiej rozpoczęto prace nad stworzeniem programu, w który, poza administracją, zaangażowani byliby właściciele oraz posiadacze obiektów, instalacji lub urządzeń infrastruktury krytycznej. Konieczność stworzenia systemu ochrony tej infrastruktury wynika z dwóch powodów. Po pierwsze, rozproszone działania podejmowane przez administrację publiczną, mające na celu ochronę infrastruktury krytycznej muszą zostać poddane procesowi koordynacji. Po drugie, w działania z zakresu ochrony tej infrastruktury należy zaangażować podmioty, które nią zarządzają, poprzez intensyfikację współpracy sektora prywatnego i publicznego w tym zakresie. Ochrona infrastruktury krytycznej leży bowiem w interesie zarówno podmiotów prywatnych, jak i odpowiedzialnej za funkcjonowanie państwa administracji państwowej. Aktywny, oparty na warunkach partnerskich, udział prywatnych i państwowych właścicieli oraz posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej w tworzonym systemie pozwoli na stabilne jej funkcjonowanie.

Omawiany typ infrastruktury jest szczególnie podatny na zagrożenia. W przeszłości elementy tworzące obecną infrastrukturę krytyczną funkcjonowały jako niezależne lub jedynie w niewielkim stopniu zależne systemy. Obecnie, w dobie postępującej globalizacji i rozwoju technologicznego, poszczególne obiekty są coraz bardziej współ-

[2)] Obecnie trwa proces nowelizacji *Ustawy o zarządzaniu kryzysowym* pod kątem dostosowania polskich przepisów do *Dyrektywy z dnia 8 grudnia 2008 r. w sprawie rozpoznawania i wyznaczania europejskiej infrastruktury krytycznej oraz oceny potrzeb w zakresie poprawy jej ochrony (2008/114/WE).*

zależne nie tylko w wymiarze jednego państwa, ale i w skali regionalnej, europejskiej, a nawet światowej. Postęp, poza oczywistymi korzyściami, spowodował równoczesne zwiększenie podatności tego rodzaju obiektów na potencjalne zagrożenia. Pojawiły się nowe rodzaje niebezpieczeństw, wcześniej nie znane. W efekcie, istniejąca sieć powiązań powoduje, że uszkodzenie lub utrata części infrastruktury krytycznej w jednym systemie spowoduje straty i uszkodzenia w innych. Zależność sprawnego funkcjonowania państwa i bezpieczeństwa obywateli od kluczowych systemów i usług, a tym samym konieczność ochrony infrastruktury, wchodzącej w skład tych systemów, jest zagadnieniem szerszym i nie może opierać się wyłącznie na ochronie fizycznej obiektu. Dlatego właśnie ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[3)] wprowadziła do polskiego prawodawstwa pojęcie infrastruktury krytycznej. Zgodnie z definicją zaproponowaną w tej ustawie, za infrastrukturę krytyczną uważa się systemy oraz wchodzące w ich skład powiązane ze sobą funkcjonalnie obiekty, w tym obiekty budowlane, urządzenia, instalacje i usługi, kluczowe dla bezpieczeństwa państwa i jego obywateli oraz służące zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców. Infrastruktura krytyczna obejmuje takie systemy, jak:

a) zaopatrzenia w energię i paliwa,
b) łączności i sieci teleinformatycznych,
c) finansowe,
d) zaopatrzenia w żywność i wodę,
e) ochrony zdrowia,
f) transportowe i komunikacyjne,
g) ratownicze,
h) zapewniające ciągłość działania administracji publicznej,
i) produkcji, składowania, przechowywania i stosowania substancji chemicznych i promieniotwórczych, w tym rurociągi substancji niebezpiecznych.

Ochrona infrastruktury krytycznej (OIK) to zespół przedsięwzięć organizacyjnych realizowanych w celu zapewnienia funkcjonowania lub szybkiego odtworzenia infrastruktury krytycznej w przypadku zagrożeń, w tym awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie. W wyniku zeszłorocznej nowelizacji ustawy o zarządzaniu kryzysowym (art. 3 ust. 3 ustawy) definicja OIK otrzymała następujące brzmienie: [...] *wszelkie działania zmierzające do zapewnienia funkcjonalności, ciągłości działania i integralności infrastruktury krytycznej w celu zapobiegania zagrożeniom, ryzykom lub słabym punktom oraz ograniczenia i neutralizacji ich skutków oraz szybkiego odtworzenia tej infrastruktury na wypadek awarii, ataków oraz innych zdarzeń zakłócających jej prawidłowe funkcjonowanie*. Zmiana definicji miała na celu dostosowanie polskiego stanu prawnego do przepisów unijnych.

W poszczególnych systemach, o których mówi ustawa, infrastruktura krytyczna zostanie wyłoniona na podstawie określonych kryteriów. Kryteria[4)] te podzielone są na dwie grupy:

1) kryteria sektorowe (systemowe), charakteryzujące ilościowo lub podmiotowo parametry (funkcje) obiektu, urządzenia, instalacji lub usługi, których spełnienie może

[3)] Dz. U. z 2007 r., nr 89, poz. 590 z późn. zm.

[4)] Kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej, spełniające przedstawione powyżej założenia, zostały w dniu 18 grudnia 2009 r. zatwierdzone przez Dyrektora RCB. Ich wykaz został opatrzony klauzulą „zastrzeżone".

spowodować zaliczenie do elementów infrastruktury krytycznej. Kryteria te przedstawione są dla każdego z systemów IK;
2) kryteria przekrojowe, opisujące parametry odnoszące się do skutków zniszczenia lub zaprzestania funkcjonowania obiektu, urządzenia, instalacji lub usługi.

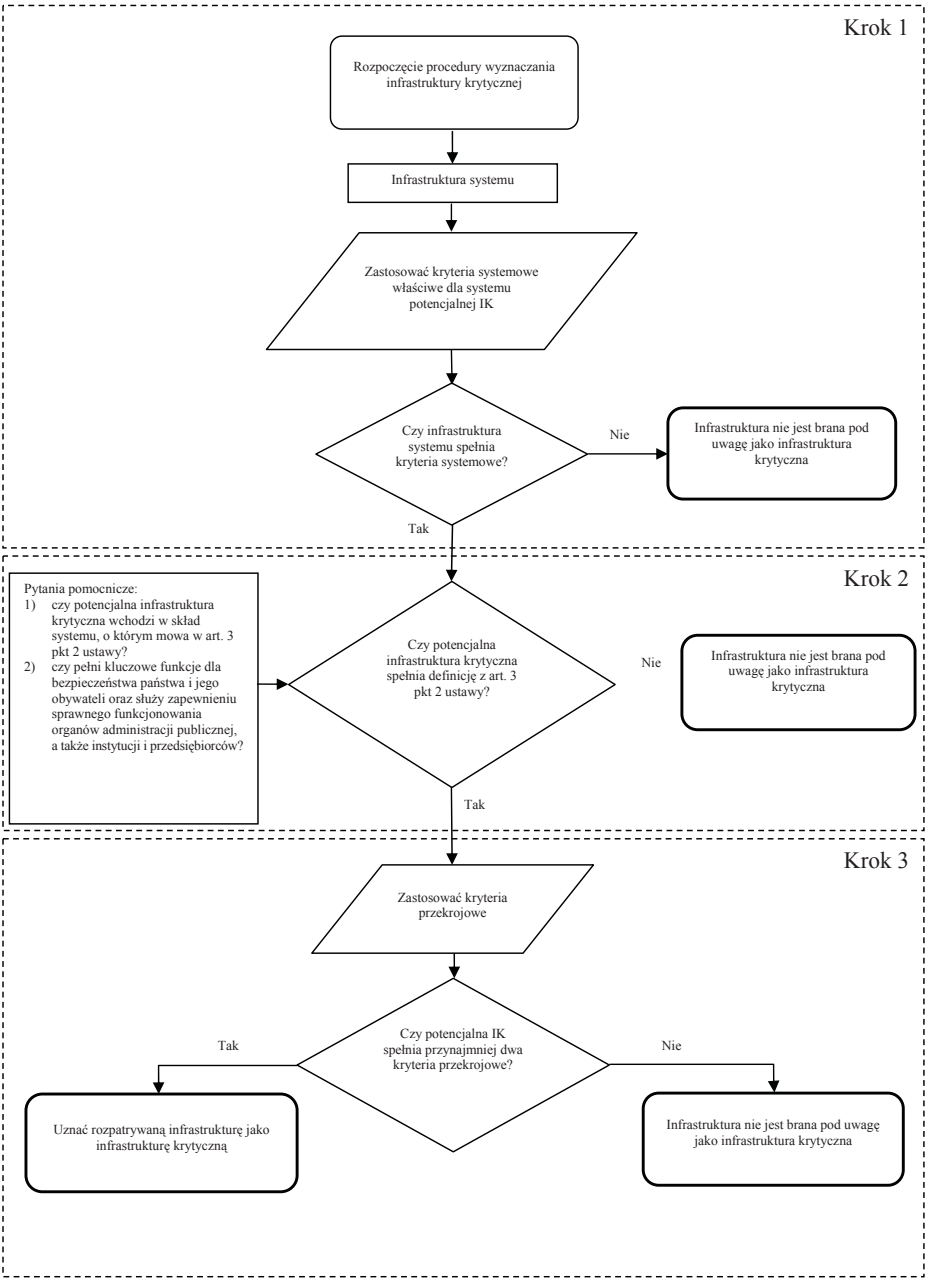
Aby obiekt, urządzenie, instalacja lub usługa mogły być zakwalifikowane jako IK, zgodnie z przyjętą metodyką muszą być zrealizowane wszystkie trzy niżej przedstawione kroki:
1) w kroku pierwszym – w celu dokonania pierwszej selekcji obiektów, instalacji, urządzeń lub usług, które potencjalnie mogłyby zostać uznane za IK w danym systemie, do infrastruktury systemu należy zastosować kryteria sektorowe (systemowe), właściwe dla danego systemu IK;
2) w kroku drugim – w celu sprawdzenia, czy obiekt, urządzenie, instalacja lub usługa pełni kluczową rolę dla bezpieczeństwa państwa i jego obywateli oraz czy służy zapewnieniu sprawnego funkcjonowania organów administracji publicznej, a także instytucji i przedsiębiorców, do infrastruktury wyłonionej w drodze spełnienia pierwszego kroku należy zastosować definicję zawartą w art. 3 pkt. 2 ustawy;
3) w kroku trzecim – w celu wskazania, jakie będą skutki zniszczenia lub zaprzestania funkcjonowania potencjalnej IK, do infrastruktury wyłonionej w drodze spełnienia kroku pierwszego i drugiego należy zastosować kryteria przekrojowe (należy wybrać kryteria najlepiej odzwierciedlające charakterystykę systemu), przy czym aby wypełnić krok trzeci, potencjalna IK musi spełnić przynajmniej dwa kryteria przekrojowe.

Proces postępowania podczas wyznaczania infrastruktury krytycznej przedstawia algorytm na rysunku 1.

Jak przedstawiono powyżej, decydujące znaczenie dla wskazania obiektów, instalacji, urządzeń lub usług IK ma spełnienie kryteriów przekrojowych. Położenie akcentu na skutki zniszczenia lub zaprzestania funkcjonowania IK, mające bezpośredni związek z powiązaniem z sytuacją kryzysową, ma głębokie uzasadnienie w rozumieniu jej jako pełniącej kluczową funkcję dla państwa jako całości i jego obywateli.

Kryteria, o których była mowa wyżej, będą stanowić element Narodowego Programu Ochrony Infrastruktury Krytycznej[5)] i podobnie jak on będą podlegały systematycznej aktualizacji. Można będzie zatem wykorzystać mechanizm do „regulacji" kryteriów w taki sposób, aby objęły one większą lub mniejszą liczbę elementów IK. Założeniem jest, by w przyszłości, po opracowaniu narzędzi, które w miarodajny sposób pozwalałyby na ocenę skutków zniszczenia lub zaprzestania funkcjonowania IK (Rządowe Centrum Bezpieczeństwa pracuje nad ich przygotowaniem) w ogóle zrezygnować z kryteriów sektorowych (systemowych). W efekcie, kryteria przekrojowe stosowane byłyby do dowolnie wybranej infrastruktury systemu lub do jakiejkolwiek krajowej infrastruktury.

[5)] Zgodnie z art. 5 b ustawy o zarządzaniu kryzysowym na program składają się następujące elementy:
1. Narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury.
2. Wykaz ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy, o których mowa w ustawie o zarządzaniu kryzysowym.
3. Szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej.



Rys. 1 – Proces postępowania podczas wyznaczania infrastruktury krytycznej.

Jedną z kluczowych zmian wprowadzonych do ustawy o zarządzaniu kryzysowym nowelizacją z 2009 r. jest podkreślenie roli Szefa Agencji Bezpieczeństwa Wewnętrznego w zakresie przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym, również w odniesieniu do infrastruktury krytycznej. Ograny administracji publicznej oraz posiadacze takiej infrastruktury zobowiązani zostali do przekazywania Szefowi ABW będących w ich posiadaniu informacji na temat zagrożeń terrorystycznych w stosunku do niej. Jednocześnie Szef ABW może udzielać zaleceń zagrożonym podmiotom, pomocnych w przeciwdziałaniu zagrożeniom.

Zgodnie z przyjętą przez Rządowe Centrum Bezpieczeństwa filozofią, ochronę infrastruktury krytycznej należy rozumieć jako sumę:

1) ochrony fizycznej,
2) ochrony technicznej,
3) ochrony osobowej,
4) ochrony teleinformatycznej,
5) ochrony prawnej,
6) planów odtwarzania.

W przedstawionym powyżej podziale ochrona fizyczna jest najbardziej znanym i rozpowszechnionym elementem OIK. Dotyczy jej nawet konkretna ustawa o ochronie osób i mienia. Na ochronę fizyczną składają się: ochrona osób, rozumiana jako działania mające na celu zapewnienie bezpieczeństwa życia, zdrowia i nietykalności osobistej oraz ochrona mienia, czyli działania zapobiegające przestępstwom i wykroczeniom przeciwko mieniu, a także przeciwdziałające powstawaniu szkody wynikającej z tych zdarzeń oraz niedopuszczające do wstępu osób nieuprawnionych na teren chroniony. Ochrona fizyczna realizowana jest przez pracowników ochrony, którzy „fizycznie" bronią dostępu do obiektów, urządzeń, instalacji lub usług infrastruktury krytycznej (IK). Pozostałe elementy ochrony IK nie są już tak rozpowszechnione i wymagają krótkiego wyjaśnienia.

Ochrona techniczna to zespół przedsięwzięć związanych z budową i eksploatacją obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, w tym również techniczne środki ochrony, mające na celu minimalizację ryzyka zakłócenia w funkcjonowaniu IK. Oznacza to, że techniczna ochrona infrastruktury krytycznej dotyczy nadzoru nad zgodnością konstrukcji budynków, urządzeń, instalacji i usług z obowiązującymi normami (np. budowlanymi) oraz innymi przepisami (np. przeciwpożarowymi), co ma zagwarantować bezpieczne użytkowanie IK. Jest to również wymienione w ustawie o ochronie osób i mienia zabezpieczenie techniczne obiektu, czyli wykorzystanie do ochrony obiektów płotów, barier, systemów telewizji przemysłowej, systemów dostępowych i tym podobnych środków.

Przez ochronę osobową należy rozumieć zespół przedsięwzięć i procedur mających na celu minimalizację ryzyka będącego ewentualnym skutkiem działań pracowników oraz usługodawców, którzy poprzez autoryzowany dostęp do obiektów, urządzeń, instalacji i usług infrastruktury krytycznej, mogą spowodować zakłócenia w jej funkcjonowaniu. Oznacza to, iż właściciele oraz posiadacze samoistni i zależni obiektów, instalacji lub urządzeń infrastruktury krytycznej chronią ją, zarówno poddając weryfikacji kwalifikacje pracowników, jak i dokonując sprawdzenia, czy dana osoba gwarantuje świadczenie pracy na wymaganym poziomie (także uczciwości) Tego typu weryfikacja to najczęściej kontakt z byłym pracodawcą lub wysłanie zapytania do rejestru skazanych. Następnie proces weryfikacji i obserwacji pracownika jest kontynuowany. Podobne sprawdzenie powinno dotyczyć również pracowników firm świadczących usługi na rzecz operatora IK.

Zależność infrastruktury krytycznej od informatycznych narzędzi zarządzania i kierowania nie ulega wątpliwości. Dlatego istotnym elementem jej ochrony jest ochrona teleinformatyczna. Przez ochronę teleinformatyczną należy rozumieć zespół przedsięwzięć i ich procedur mających na celu minimalizację zakłóceń w funkcjonowaniu IK związanych z wykorzystaniem do użytkowania tego typu infrastruktury systemów i sieci teleinformatycznych. Oznacza to ochronę przed atakami hakerskimi i cyberterroryzmem oraz skuteczne przeciwdziałanie tego typu incydentom[6)].

Ochrona prawna jest pojęciem nowym, związanym z kształtem współczesnej gospodarki rynkowej, w której pojawiają się zagrożenia ze strony innych podmiotów gospodarczych państwowych lub prywatnych, których działania mogą prowadzić do zakłócenia funkcjonowania IK. Stąd też przez ochronę prawną infrastruktury krytycznej należy rozumieć zespół przedsięwzięć, mających na celu minimalizację ryzyka związanego z działalnością innych podmiotów gospodarczych, państwowych lub prywatnych, których działania mogą prowadzić do zakłócenia w funkcjonowaniu obiektów, urządzeń, instalacji i usług IK. Mamy tu na myśli zastosowanie narzędzi prawnych (ustaw) niedopuszczających, poprzez możliwość kontroli i ewentualnego blokowania lub ograniczania decyzji zarządów, do np. wrogiego przejęcia, fuzji czy też sprzedaży niektórych elementów infrastruktury, której efektem mogą być zakłócenia jej w funkcjonowaniu.

Podsumowanie

Jak widać, powyższa koncepcja ochrony zaproponowana przez RCB jest kompleksowa i ukierunkowana na przeciwdziałanie wszelkim rodzajom zagrożeń, w tym zagrożeniom asymetrycznym. W tym obszarze, oprócz ochrony fizycznej, szczególnie istotne znaczenie ma ochrona osobowa i teleinformatyczna.

ABSTRACT

The aim of the article is to describe undertaken by the polish administration in the sphere of critical infrastructure protection, which are targeted At creating a comprehensive critical infrastructure protection system of the most important elements of the national infrastructure. The above mentioned actions ensure proper functioning of the state and enterprises in case of asymmetric threats. They require a coordinated interaction between the central and local governments, but also with the private sector.

[6)] Należy podkreślić, iż obecnie trwają prace nad przygotowaniem Rządowego Programu Ochrony Cyberprzetrzeni, który przedstawi kompleksowe działania polskiego rządu w tym obszarze.

Andrzej Krzak

Terrorystyczna i wywrotowa działalność organizacji komunistycznych w Polsce w latach 1921-1939

Wstęp

Rzeczpospolita w 1918 r. stanęła przed trudnym wyborem budowy podstaw państwa i niepodległego bytu. Sytuację tę dodatkowo komplikowało bardzo trudne położenie międzynarodowe Polski. Trwająca do połowy 1921 r. walka o granice uniemożliwiała podjęcie efektywnych prac nad utworzeniem sprawnie funkcjonującego systemu zewnętrznego i wewnętrznego bezpieczeństwa państwa. Powstające wraz z odradzającym się krajem służby bezpieczeństwa starały się nie tylko chronić państwo przed działalnością wywiadowczą ze strony obcych służb specjalnych, lecz także zwalczały wszelkie przejawy terrorystycznej (destrukcyjnej) działalności zmierzającej do naruszenia podstaw konstytucyjnych państwa. Przeciwko państwu polskiemu wraz z organizacjami nacjonalistycznymi związanymi z mniejszościami narodowymi aktywnie występowali również i komuniści. Walka z terroryzmem ukraińskich organizacji nacjonalistycznych oraz polskich, białoruskich i ukraińskich komunistów spowodowały, że kontrwywiad wojskowy i policja polityczna (Defensywa Polityczna) znaczną część swoich sił ukierunkowywały na rozpoznanie i likwidację wciąż odradzających się struktur organizacji wywrotowych. Walka z ruchem komunistycznym była niewątpliwie jednym z priorytetowych zadań polityki wewnętrznej II Rzeczypospolitej prowadzonej przez ówczesną policję polityczną, komórki bezpieczeństwa administracji państwowej i samorządowej oraz kontrwywiad wojskowy.

Działania polskich organizacji komunistycznych w dwudziestoleciu międzywojennym miały charakter wielopłaszczyznowy. Polegały jednak na dążeniu do osiągnięcia jednego konkretnego celu, jakim było dokonanie przewrotu i obalenie porządku konstytucyjnego, aby przejąć pełnię władzy. Metody i formy działań, jakie stosowali komuniści odbiegały od obowiązujących norm prawnych. Nie należy oczywiście zapominać, że partia komunistyczna prowadziła legalną działalność polityczną, miała swoich posłów i próbowała odgrywać istotną rolę na politycznej scenie II Rzeczypospolitej. Jednocześnie uznała, że zmiana systemu władzy w Polsce może nastąpić jedynie w wyniku rewolucji. Dlatego też obok oficjalnej działalności politycznej polskie organizacje komunistyczne na masową skalę prowadziły aktywną działalność o charakterze destrukcyjnym wobec państwa polskiego. W dokumentach archiwalnych oraz literaturze przedmiotu stosunkowo rzadko spotykamy się z użyciem pojęcia „terroryzm" w odniesieniu do działalności bojówek komunistycznych. Najczęściej funkcjonariusze policji czy oficerowie kontrwywiadu stosowali określenie „działalność wywrotowa" lub „dywersyjna". Opisując struktury organizacyjne zakonspirowanych komórek komunistycznych, spotykamy się również z określeniem „działalności („roboty") dywersyjnej" i „wywrotowej". Jeśli używa się określenia „aktu terrorystycznego", to ma to miejsce w odniesieniu do zorganizowanych na dużą skalę, spektakularnych zamachów na obiekty i ludzi współpracujących z organami bezpieczeństwa Rzeczypospolitej. Nie znaczy to, że pojęcie „terroryzm" było wówczas nieznane. Jeśli porównamy którąś ze współczesnych definicji terroryzmu z pojęcia-

mi dywersji i działalności wywrotowej, okaże się, że oba te pojęcia, choć niejednoznaczne, będą się zawierać we współczesnym rozumieniu terroryzmu jako zjawiska mającego wywołać chaos, niepewność i doprowadzić do osiągnięcia zamierzonych wcześniej celów, czyli np. destabilizacji sytuacji wewnętrznej i przejęcia władzy w państwie. Ponadto należy pamiętać, że działania bojowe grup komunistycznych miały wywołać chaos, który wzorem rosyjskim doprowadziłby do masowych wystąpień społecznych i zainicjował proces rewolucji. Zatem działania terrorystyczne, dywersyjne (ataki na ośrodki administracyjne, zamachy i niszczenie infrastruktury) miały być tylko preludium dla rewolucji. Trzeba pamiętać również o tym, iż komuniści nie byli wyrazicielami wolnej woli polskich robotników i chłopów, lecz jednymi z wykonawców polityki komunistycznej Rosji i będąc członkiem Kominternu – Międzynarodówki Komunistycznej[1)], realizowali jej wytyczne. Komintern jako agenda rządu radzieckiego, wykorzystywany był przede wszystkim do działalności destrukcyjnej i szpiegowskiej na całym świecie. Oczywiście, nie wszyscy działacze komunistyczni (zwłaszcza szeregowi członkowie) zdawali sobie sprawę z tego, że byli manipulowani i wykorzystywani przez swoich przywódców do prowadzenia aktywnej działalności terrorystycznej przeciwko własnej ojczyźnie.

Dotychczasowy stan badań nad problematyką działalności terrorystycznej, dywersyjnej i wywiadowczej, będącej udziałem skrajnej lewicy w latach 1918-1939, należy określić jako skromny. Do tej pory nie powstało bowiem całościowe opracowanie na temat roli, jaką polscy komuniści odgrywali w destrukcyjnej działalności przeciwko II Rzeczypospolitej oraz tego, w jakim stopniu byli inspirowani przez ośrodki zewnętrzne, przede wszystkim przez Komintern (a tym samym przez radzieckie władze i służby specjalne).

W latach 1945 - 1989 powstało co najmniej kilkaset opracowań (jeśli nie więcej), związanych z tzw. dziejami ruchu robotniczego oraz setki, jeśli nie tysiące artykułów, lecz są to w przeważającej ilości źródła zupełnie nieprzydatne ze względu na treść propagandową (ideologiczną). Tylko niektóre z nich mogą służyć pośrednio jako materiał pomocniczy podczas krytyki źródeł. Nie mogą natomiast stanowić podstawy naszej wiedzy źródłowej do dziejów organizacji wywrotowych i ich wpływu na system bezpieczeństwa państwa polskiego. Z kolei, rzadko pojawiające się po 1989 r. artykuły opisujące ruch komunistyczny w Polsce z reguły odnoszą się do dziejów po 1945 r., czasami tylko nawiązując do jego korzeni. Są one jednak nacechowane sporą dawką emocji nie popartych rzetelną analizą problemu i wiedzą historyczną. Dlatego też wydaje się konieczne, aby naukowcy zajęli się tym obszarem naszych dziejów, ponieważ miał on znaczny wpływ na kształtowanie się polskiej polityki wewnętrznej w dwudziestoleciu międzywojennym. Więcej uwagi należałoby poświęcić pracy I. Pawłowskiego – *Poli-*

[1)] Komintern – inaczej Międzynarodówka Komunistyczna. Organizacja o charakterze międzynarodowym, skupiająca w swym składzie partie komunistyczne. Powstała w dniach 2-6 marca 1919 r.; założona przez 19 partii komunistycznych na I Kongresie w Moskwie. Organem kierującym był wybieralny Komitet Wykonawczy. Organizację tworzyły sekcje, czyli poszczególne partie członkowskie, przedstawicielstwa organizacji partyjnych oraz oddziały propagandy, agitacji, szkolenia, kadr i łączności międzynarodowej (OMS). Ten ostatni zajmował się działalnością poza granicami ZSRR i regulował kontakty ze strukturami partii komunistycznych, a faktycznie był rozległą rezydenturą OGPU i Razwiedupru, czyli radzieckich służb specjalnych. Komintern stał się jednym z narzędzi polityki zagranicznej ZSRR, a ponadto stanowił bazę do prowadzenia na skalę globalną działalności o charakterze szpiegowskim i dywersyjnym.

tyka i działalność wojskowa KPP 1918-1928[2)], która prezentuje fragment działalności wojskowej polskich komunistów, i choć nasycona jest sloganami politycznymi, to jednak opierając się na dokumentach kominternowskich, odsłania kulisy współpracy KPP ze służbami specjalnymi ZSRR oraz destrukcyjną i terrorystyczną działalność tej organizacji wobec państwa polskiego. Oczywiście, nie może ona służyć jako zasadnicze źródło wiedzy historycznej o omawianym problemie, tylko jako materiał uzupełniający i często potwierdzający np. dane zachowane w dokumentach źródłowych policji politycznej i kontrwywiadu wojskowego.

Do najciekawszych artykułów dotyczących przedmiotowego tematu, opublikowanych przed 1989 r., zaliczamy: cykl artykułów pod redakcją prof. Andrzeja Pepłońskiego i Henryka Kopczyka, opisujących metody i formy zwalczania przez policję organizacji komunistycznych w dwudziestoleciu międzywojennym pod tytułem *Udział organów bezpieczeństwa II RP w inwigilacji ruchu komunistycznego w latach 1918--1926*, *Oddział II oraz formacje ochrony granic wobec ruchu komunistycznego w Polsce (1918-1926)*, *Geneza Policji Państwowej w II RP*, *Współpraca wojskowych i policyjnych służb informacyjnych w zwalczaniu ruchu komunistycznego w Polsce 1918-1926* i *Zwalczanie ruchu komunistycznego przez policję polityczną II RP (1918-1926)*. Ponadto, do problematyki zwalczania ruchu komunistycznego nawiązują w swoich pracach prof. Andrzej Misiuk i dr A. Krzak[3)].

Inną grupą opracowań traktujących o działalności komunistów i ich powiązań z radzieckimi służbami specjalnymi są prace autorów rosyjskich i anglosaskich. Należy jednak pamiętać, iż problematyka udziału polskich komunistów w tej działalności jest fragmentaryczna. Większość z nich prezentuje natomiast sam schemat organizacyjny i metodologiczny funkcjonowania komórek komunistycznych w ramach Kominternu oraz rolę, jaką w tej działalności odgrywały władze ZSRR. Do najciekawszych prac z tej grupy niewątpliwe zaliczymy: J. Lindera i S. Czurkina – *Krasnaja Pautina. Tajny razwiedki Kominterna 1919–1943*, N. W. Pietrowa i A. I. Kukerina – *Łubianka. WCZK--GPU-OGPU-NKWD-MGB-MWD-KGB 1917–1960* oraz *Pamiętniki dyplomaty sowieckiego* Z. G. Biesiedowskiego i *Wspomnienia niewygodnego świadka* P. Sudopłatowa.

Ponadto, aby zaprezentować ogólne tło historyczne i działalność KPP oraz jej sojuszników wykorzystano przede wszystkim opracowania: W. T. Kowalskiego i A. Skrzypka, *Stosunki polsko-radzieckie 1917–1945* oraz H. Cimka – *Komuniści, Polska, Stalin 1918–1939.*

Działalność wywrotowa i terrorystyczna KPRP do 1925 r.

Organizacje komunistyczne w Polsce nie powstały wraz z odzyskaniem niepodległości. Korzeni ich należy szukać w ruchach socjalistycznych, które zrodziły się w drugiej połowie XIX w., jednak, podobnie jak i w innych krajach Europy, powstające

---

[2)] I. Pawłowski, *Polityka i działalność wojskowa KPP 1918-1928,* Warszawa 1964.

[3)] Są to jednak opracowania, które problematykę zwalczania terrorystycznej, dywersyjnej i wywrotowej działalności komunistów ujmują jako jeden z elementów funkcjonowania systemu bezpieczeństwa II Rzeczypospolitej w latach 1918-1939. Do najciekawszych prac wymienionych autorów należą: A. Pepłoński – *Wywiad polski na ZSRR 1921-1939*, *Kontrwywiad II Rzeczypospolitej*, *Wywiad a dyplomacja II Rzeczypospolitej*; A. Misiuk – *Od MSW do Posterunku PP. Dzieje ustroju organów policyjnych i administracyjnych w II RP w latach 1919-1926*, *Służby specjalne II Rzeczypospolitej*; A. Krzak – *Kontrwywiad wojskowy II Rzeczpospolitej przeciwko radzieckim służbom specjalnym 1921-1939.*

partie socjalistyczne ewoluowały i radykalizowały swoją działalność, dając początek powstaniu szeregu skrajnych odłamów. Konsolidacja polskich skrajnie lewicowych organizacji nastąpiła w grudniu 1918 r. po połączeniu SDKPiL oraz PPS–Lewicy, dzięki czemu powstała Komunistyczna Partia Robotnicza Polski (KPRP)[4]. Lansowane przez jej działaczy leninowskie koncepcje państwa oraz zmian rewolucyjnych nie spotkały się jednak z poparciem w II Rzeczypospolitej. Komuniści polscy, wzorując się na działalności swoich towarzyszy ze wschodu, postawili sobie za cel utworzenie Polskiej Republiki Rad[5]. Przyszłe państwo polskie miało być ściśle związane z Rosją Radziecką, dlatego też odrodzona II Rzeczypospolita była przez nich postrzegana jako jeszcze jeden twór traktatu wersalskiego i tzw. zmowy państw imperialistycznych, który musi zostać unicestwiony w wyniku ogólnoświatowego procesu rewolucyjnego. KPRP, podobnie jak jej rosyjska „siostra", uważała, że odrodzone państwo polskie jest „bękartem" i sztucznym tworem paryskiej konferencji pokojowej, który musi zostać unicestwiony, tak jak cały europejski porządek powersalski.

Wzorując się na bolszewikach, polscy komuniści już na przełomie 1918 i 1919 r. rozpoczęli tworzenie struktur Rad Delegatów. Na obszarze Zagłębia Dąbrowskiego utworzono jednostki Rad Delegatów Robotniczych i Czerwonej Gwardii, liczące ok. 700 osób, a w Warszawie ponad 1 000. Wzrastająca aktywność tych organizacji spowodowała natychmiastowe przeciwdziałanie defensywy policyjnej, której udało się stosunkowo szybko rozbić komunistyczne struktury[6]. Aby je odbudować, z Rosji Radzieckiej skierowano do Polski Stefana Żbikowskiego – komunistę i wyższego dowódcę Armii Czerwonej. Otrzymał on zadanie stworzenia wojskowych struktur kompartii, w tym również bojówek dywersyjno-terrorystycznych. Kolejna kontrakcja służb bezpieczeństwa nie pozwoliła jednak zrealizować zamiaru komunistów[7].

Aktywność komunistów uległa nasileniu wraz z wybuchem wojny polsko-bolszewickiej. Przede wszystkim podjęli oni zakrojone na szeroką skalę działania z zakresu dywersji politycznej. Krytykowali ponadto władze polskie za wszczęcie działań wojennych oraz przeszli do aktywnej działalności, która polegała na organizacji strajków oraz aktów terrorystycznych i dywersyjnych na zapleczu frontu. Część z nich organizowała i prowadziła działania o charakterze wywiadowczym. We wrześniu 1920 r. komunista Henryk Stein vel Rosemal vel Kamiński został aresztowany przez organy defensywy. Znaleziono przy nim paszport wystawiony przez Dyrekcję Prezydium Policji w Gdańsku. W toku prowadzonych przesłuchań uzyskano informacje o pomocy udzielonej przez władze niemieckie rosyjskim komunistom, zajmującym się przerzucaniem działaczy komunistycznych i agentów do Polski przez Gdańsk. Uzyskano informacje, z których wynikało, że w Gdańsku znajdowała się rezydentura wywiadu Rosji Radzieckiej, której kierownikiem miał być były oficer carski, por. Aleksander Popow[8].

---

[4] W skład KPRP weszły również: Żydowski Komunistyczny Związek Robotniczy w Polsce (Kombund), Żydowska Socjalno-Demokratyczna Partia Robotnicza – Robotnicy Syjonu (Poale Syjon), Żydowska Socjalistyczna Partia Robotnicza – Zjednoczeni (Frajnigte) oraz pojedynczy działacze z Polskiej Partii Socjalistycznej i Komunistycznej Partii Górnego Śląska. H. Cimek, *Komuniści, Polska, Stalin 1918-1939*, Białystok 1990, s. 14.

[5] Tamże, s. 9.

[6] I. Pawłowski, *Polityka i działalność wojskowa KPP 1918-1928*, Warszawa 1964, s. 27.

[7] Tamże s. 69. S. Żbikowski został aresztowany 14 marca 1919 r., a następnie w ramach wymiany więźniów politycznych przekazany Rosji Radzieckiej.

[8] Komunikat nr 6 (Pismo nr 16975/20Def/) z 20.12.1920 r., CAW, Oddz. II SG, sygn. 1917/03/31. Komunikat Defensywy nr 3 z 20.09.1920 r., nr pisma L. 14816/20/Def., CAW, Oddz. II SG, sygn. 1917/03/31.

Przykładem przygotowywanych wystąpień zbrojnych kierowanych przez komunistów była afera[9] Mariana Buczka i towarzyszy z lipca 1921 r. Wydział II DOK Lublin rozpracował organizację dywersyjną KPRP, podejrzewaną o działalność terrorystyczną i powstańczą w województwie lubelskim. Dokonano wielu aresztowań, m. in. członków Centralnego Wydziału Bojowego – Stefana Pakulskiego i Kucharuka oraz pracownika Rosyjskiej Misji Repatriacyjnej – Antoniego Krzyżanowskiego. Kierownictwo organizacji planowało rozpoczęcie akcji powstańczej, która rzekomo miała zostać wsparta przez oddziały wojskowe Rosji Radzieckiej, które zamierzały przekroczyć granicę i zainicjować powstanie niezależnego państwa komunistycznego[10].

Po zakończeniu wojny polsko-rosyjskiej KPRP z jednej strony podjęła aktywną, legalną działalność polityczną, biorąc udział w wyborach parlamentarnych i zasiadając w Sejmie, a z drugiej nadal rozbudowywała nielegalne konspiracyjne struktury (w tym wojskowe), nie rezygnując z głównego celu, jakim było dążenie do obalenia konstytucyjnego porządku w Polsce i stworzenie (wzorowanej na Rosji Radzieckiej) Republiki Rad.

Tajna instrukcja bolszewicka z 1919 r., przejęta przez funkcjonariuszy defensywy policyjnej, zalecała organizować działalność propagandową, która powodowałaby wzrost nienawiści i waśni o charakterze narodowościowym. W tym celu agitatorzy komunistyczni mieli organizować zamachy na cudzoziemców i przedstawicieli mniejszości narodowych, aby z jednej strony doprowadzić do chaosu wewnętrznego, a z drugiej do konfliktów w stosunkach międzynarodowych. Ponadto, mieli uczestniczyć w organizacji i podtrzymywaniu strajków i buntów przeciwko władzom administracyjnym i wojskowym[11].

Wiosną 1921 r. formowane przez rosyjskie służby specjalne (Razwiedupr) oddziały terrorystyczne były przerzucane na terytorium wschodniej Polski. Głównym ich zadaniem było sianie terroru i doprowadzenie do wybuchu powstania, które umożliwiłoby przyłączenie Zachodniej Ukrainy i Białorusi do Rosji Radzieckiej. Działania te były koordynowane zarówno przez dowództwo Armii Czerwonej, Razwiedupr, WCzeka, jak również przez kierownictwo polskiej kompartii i Kominternu. Grupy terrorystyczne składały się w większości z uciekinierów oraz działaczy komunistycznych z Polski, Białorusi i Ukrainy. Wśród członków grup byli też pospolici przestępcy, na czele zaś stali doświadczeni i zaufani działacze polskiej partii komunistycznej[12]. Obok działań wywiadowczych, mieli oni również organizować akcje dywersyjno-terrorystyczne, eliminujące żołnierzy i ludność wrogiego państwa, paraliżujące komunikację, demoralizujące wojsko i dowództwa sił zbrojnych. Latem 1921 r. działania terrorystyczne prowadzone przez komunistów objęły swoim zasięgiem powiaty: sarneński, kowelski, dubnowski, równieński i włodzimiersko-wołyński. 8 sierpnia 1921 r. służby specjalne Rosji Radzieckiej podpisały z Kominternem porozumienie regulujące współpracę w zakresie działalności agencyjnej i dywersyjno-sabotażowej (de facto terrorystycznej), w którym zaznaczono, iż całość działalności wywiadowczej i terrorystycznej będzie koordynowana przez Komintern i służby specjalne Rosji Radzieckiej[13]. Członko-

[9] Afera szpiegowska, czyli rozpracowanie operacyjne prowadzone przez kontrwywiad.
[10] *Raport kontrwywiadowczy za okres od 06.11 do 16.11.1921 r.*, CAW, Oddz. II SG, sygn. I.303.4.6884.
[11] *Tajna Instrukcja Bolszewicka z 22 lutego 1919 r.*, CAW, Oddz. II SG, sygn. 1917/03/592.
[12] J. Linder, S. Czurkin, *Krasnaja Pautina. Tajny razwiedki Kominterna 1919-1943*, Moskwa 2005, s. 89.
[13] Tamże, s. 92.

wie partii komunistycznych należących do Międzynarodówki mieli udzielać pomocy Razwieduprowi i WCzeka, choć w jednym z punktów zaznaczono, że pomoc ta mogła być udzielana tylko wtedy, gdy władze Kominternu wydadzą na nią zgodę[14]. Według wiadomości uzyskanych od agentów Oddziału II, w 1923 r. z Rosji wysłano do Polski grupę 30-tu komunistów – „techników" do portów morskich i śródlądowych, których zadaniem było prowadzenie dywersji[15].

Porażki, jakich doznali komuniści w latach 1922-1923 r. doprowadziły do częściowej zmiany taktyki ich działania: zaktywizowali swoją działalność w parlamencie oraz zaczęli prowadzić aktywną agitację wśród chłopów i robotników[16]. Skomplikowana sytuacja wewnętrzna Rzeczypospolitej, brak pracy, kolejne kryzysy rządowe, pogłębiający się kryzys ekonomiczny i społeczny spowodowały, że hasła działaczy komunistycznych trafiały na podatny grunt. Dzięki intensywnej działalności z zakresu dywersji ideologicznej i politycznej działacze ci starali się stworzyć podwaliny pod masowy ruch społeczny, który miał zapoczątkować zmiany ustrojowe. Ruch ten byłby wsparty szeroką akcją dywersyjno-terrorystyczną prowadzoną początkowo na Kresach Wschodnich (obszar zachodniej Białorusi i Ukrainy), aby następnie rozprzestrzenić się na całe terytorium Rzeczypospolitej.

Na przełomie 1923 i 1924 r. oddziały dywersyjne (zwane przez komunistów partyzanckimi)[17] zaktywizowały swoją działalność głównie na obszarze zachodniej Białorusi. Zgrupowanie Muchy-Michałowskiego (wł. K. Orłowskiego) dokonało kilku uderzeń na posterunki policji, tartaki i dwory. 18 lipca 1924 r. oddział Stanisława Waupszasowa rozbił patrol policyjny koło wsi Wiśniewo. W tym samym czasie grupa F. Jabłonowskiego zmusiła do odwrotu interweniujący oddział policji w przysiółku Żodiszki. W obu przypadkach, po zwycięskiej walce, komuniści zorganizowali wiec, w czasie którego agitowali za kontynuowaniem walki rewolucyjnej przeciwko „burżuazyjnej Polsce"[18].

Tylko w ciągu czterech miesięcy, tj. od kwietnia do lipca 1924 r., władze bezpieczeństwa województw wschodnich odnotowały 83 przypadki aktów terroru z udziałem działaczy komunistycznych i oddziałów dywersyjnych przerzuconych z ZSRR[19]. Szczytowym sukcesem dywersantów był atak na Stołpce, przeprowadzony w nocy z 3 na 4 sierpnia przez oddział Stanisława Waupszasowa[20]. Głównym celem było opanowanie aresztu i uwolnienie zatrzymanych tam komunistów, z członkiem Wydziału Wojskowego KPP, Stanisławem Skulskim i szefem KPZB – Pawłem Korczikiem, na czele. Dywersanci opanowali stację kolejową, udało im się także rozbić posterunek policji. Według autorów monografii o Kominternie, akcja zakończyła się powodzeniem[21]. Polskie źródła natomiast przyznają, że komunistycznemu oddziałowi udało się rozbić

14) Tamże.

15) *Informacja O II DOK V o wysłaniu komunistów z Rosji w celach dywersyjnych do portów polskich,* pismo nr L. 1513/II Tajne z 16.10.1923 r., CAW, SRI DOK V, sygn. I.371.5/A.288.

16) H. Cimek, *Komuniści, Polska*..., s. 22-23 i 41-42.

17) Takie określenie wprowadzili dla bandyckiego oddziału Muchy-Michałowskiego autorzy monografii o Kominternie. J. Linder, S. Czurkin, *Krasnaja Pautina* ..., s. 272.

18) Tamże, s. 278.

19) Zestawienie aktów dywersyjno-bandyckich z 31 lipca 1924 r., CAW, Oddz. II SG, sygn. I.3030.4.2538, k. 1-2.

20) A. Krzak, *Kontrwywiad wojskowy II Rzeczpospolitej przeciwko radzieckim służbom specjalnym 1921--1939*, Toruń 2007, s. 198.

21) J. Linder, S. Czurkin, *Krasnaja Pautina*..., s. 282.

posterunek policji i opanować część miasta wraz ze stacją kolejową, lecz przeciwdziałanie wojsk polskich zmusiło ich do odwrotu, w trakcie którego zastrzelono kilkunastu napastników (schwytano kilku)[22]. Część oddziału dywersyjnego (około piętnastu osób) zdołała jednak zbiec i przekroczyć granicę z ZSRR. Akcja ta wywołała protest polskiego Ministerstwa Spraw Zagranicznych[23]. Z przesłuchań schwytanych terrorystów wynikało, że od dłuższego czasu działali oni w pasie przygranicznym, atakując posterunki policji i polskie dwory. Ponadto, oficerowie defensywy policyjnej i kontrwywiadu uzyskali informacje, iż większość członków oddziału była szkolona w specjalnym obozie pod Mińskiem[24].

Począwszy od września 1924 r. terroryści komunistyczni zaktywizowali swoją działalność, dokonując wielu uderzeń na linie komunikacyjne na Kresach. 24 września zatrzymali pociąg linii Brześć-Łuniniec, rabując pasażerów i wagon pocztowy. Podobna akcja miała miejsce kilka dni później w powiecie pińskim. W październiku dywersanci zniszczyli wiadukt kolejowy w powiecie nieświeskim. Z kolei 3 listopada i później obrabowali kilka pociągów na linii Brześć-Baranowicze[25].

1 lutego 1925 r. KPRP przekształciła się w Komunistyczną Partię Polski (KPP). Jednak zanim to nastąpiło policji politycznej udało się rozbić jej Wydział Wojskowy (dalej: WW)[26]. Prowadzone równocześnie przez jednostki kontrwywiadu wojskowego operacje antyszpiegowskie w kilku Okręgach Korpusu doprowadziły do rozbicia struktur komunistycznych w jednostkach wojskowych na obszarze całego kraju. Największe straty komuniści ponieśli w DOK I. Samodzielny Referat Informacyjny DOK I[27], prowadząc aferę Słabodziana i towarzyszy, doprowadził do aresztowania Stanisława Flataua i Ryfki Kutznerówny[28], która zajmowała się organizacją dywersji ideologicznej w jednostkach wojskowych[29]. W październiku 1925 r. w wyniku kolejnych aresztowań rozbito wojskową organizację ZMK, działającą na obszarze SRI DOK I. W wyniku likwidacji komórek komunistycznych w jednostkach wojskowych aresztowano 29 osób, w tym 14 żołnierzy[30].

„Bombowa wiosna" 1923 r.

Wystąpienia i akty terroru odnotowywano również w ośrodkach miejskich. Od 1923 r. specjalna grupa dywersyjno-terrorystyczna, złożona z profesjonalnie przeszkolonych członków KPP, działająca w Warszawie i powiązana z rezydenturą wywiadu radzieckiego przy Poselstwie ZSRR, przygotowała na 3 maja zamachy bombowe,

---

22) A. Krzak, *Kontrwywiad wojskowy II Rzeczpospolitej*..., s. 198.

23) *Biuletyn Informacyjny Wydziału Wschodniego MSZ* z 22.08.1924 r. Noty rządu polskiego w sprawie napadu na Stołpce, CAW, Oddz. II SG, sygn. 1917/03/30.

24) A. Krzak, *Kontrwywiad wojskowy II Rzeczpospolitej*..., s. 198.

25) Tamże, s. 284-285.

26) Rozpracowanie prowadzone w lutym tego roku w pułku łączności doprowadziło do aresztowania Kazimierza Gryglasa i Antoniego Lipskiego ze ścisłego kierownictwa WW KPRP. Podobna sytuacja miała miejsce w DOK IV i IX.

27) SRI DOK – Samodzielny Referat Informacyjny Dowództwa Okręgu Korpusu – placówka terenowa Oddziału II Sztabu Głównego Wojska Polskiego zajmująca się kontrwywiadem wojskowym.

28) Po aresztowaniu R. Kutznerówna została zwolniona za kaucją i zbiegła do ZSRR.

29) Materiały wywrotowe to inaczej „bibuła", czyli ulotki, odezwy, broszury, książki oraz inne wydawnictwa o treści komunistycznej i charakterze propagandowym.

30) I. Pawłowski, *Polityka i działalność*..., s. 200.

których celem mieli być najwyżsi dostojnicy państwa polskiego[31]. Aby wzmocnić efekt zamachów terrorystycznych w Warszawie, planowano również dokonanie podobnych aktów w Częstochowie i na obszarze Zagłębia. Komunistom z powodzeniem udało się przeprowadzić wiosną 1923 r. kilka zamachów na lokale ugrupowań i czasopism prawicowych, lecz akcja ta nie przyniosła spodziewanych efektów. Według jej inicjatora – rezydenta wywiadu radzieckiego, Łoganowskiego – wystąpienia te miały prowadzić do destabilizacji sceny politycznej i wystąpień ze strony zwolenników ruchu narodowego. W zamyśle Łoganowskiego akcja komórek terrorystycznych miała być przypisana środowisku piłsudczyków. Tak misternie zaplanowane przedsięwzięcie zakończyło się jednak porażką, bowiem szybka reakcja policji politycznej i kontrwywiadu wojskowego doprowadziła do częściowego rozbicia warszawskiej specbojówki terrorystycznej i aresztowania jej czołowych działaczy, w tym oficerów Wojska Polskiego – por. Walerego Bagińskiego i ppor. Antoniego Wieczorkiewicza[32].

W nocy z 13 na 14 października 1923 r. doszło do potężnej eksplozji w Cytadeli, w wyniku której zginęło kilkadziesiąt osób. O udział w zamachu władze policyjne oskarżyły komunistów, przede wszystkim zatrzymanych oficerów WP, choć oni sami od kilku miesięcy przebywali w więzieniu. Sprawa ta nabrała szerszego rozgłosu i stała się obiektem śledztwa prowadzonego przez specjalną komisję sejmową. Bagiński i Wieczorkiewicz faktycznie byli związani z ruchem komunistycznym, lecz ich odpowiedzialność za zamach październikowy jest co najmniej dyskusyjna. Komisja sejmowa stwierdziła, iż sprawa aresztowanych oficerów i ich powiązania z grupą terrorystyczną miały charakter nieudolnie przeprowadzonej prowokacji policyjnej. Jednak zostali oni skazani na karę śmierci, którą prezydent RP ostatecznie zamienił na karę dożywotniego więzienia.

5 listopada działacze KPP, w związku z zaostrzeniem przepisów prawa wobec osób naruszających porządek konstytucyjny, wezwali robotników do akcji protestacyjnej, którą miał rozpocząć wiec przed Domem Robotnika w Krakowie. Władze administracyjne nie wydały zgody na manifestację, ale do wiecu jednak doszło. Nieprofesjonalnie przeprowadzona interwencja policji doprowadziła do ataku tłumu na interweniujących policjantów i starć, które przerodziły się w regularne walki. Aby opanować sytuację w mieście, władze musiały wprowadzić jednostki wojskowe, co doprowadziło do eskalacji konfliktu. Dopiero po trzech dniach, dzięki interwencji posłów – socjalistów na czele z Bobrowskim, doszło do wygaszenia walk. Jak wynika z ustaleń rosyjskich autorów monografii o Kominternie, przywódcy Międzynarodówki byli zainteresowani kontynuowaniem walk w Krakowie, dlatego nakazali, aby KC KPP przystąpił do aktywniejszych działań polegających m. in. na stworzeniu z uzbrojonych grup robotników oddziałów Gwardii Czerwonej[33]. Reakcja KPP była jednak spóźniona, bowiem kiedy jej działacze przybyli do Krakowa, sytuacja była już opanowana.

---

[31] Tamże, 169-270.

[32] Ppor. Antoni Wieczorkiewicz – legionista sympatyzujący ze skrajną lewicą. Był również oficerem informacyjnym, tzn. nieetatowym pracownikiem Oddziału II. Zajmował się m. in. zwalczaniem działalności wywrotowej w Wojsku Polskim. Prawdopodobnie współorganizator „bojówki" KPRP. *Akta osobowe Walerego Bagińskiego i Antoniego Wieczorkiewicza*, AAN, Zespół Oddział VI, t. 205.

[33] J. Linder, S. Czurkin, *Krasnaja Pautina*..., s. 271.

Terroryzm i dywersja komunistyczna na Kresach

Na Kresach Wschodnich RP także prowadzono działania dywersyjne i terrorystyczne, opierając się na kadrach KPZU i KPZB, lecz ich charakter był odmienny od tych, które podjęto w Polsce centralnej. Działacze ukraińscy i białoruscy liczyli się bowiem z możliwością wybuchu konfliktu zbrojnego z ZSRR. Dlatego całość ich działań, obok agitacji, polegała na stworzeniu sieci organizacji terrorystycznych (dywersyjnych), które po otrzymaniu sygnału z Moskwy miały rozpocząć działanie.

Jedną z pierwszych organizacji, która prowadziła działania o charakterze dywersyjno-terrorystycznym był tzw. „Zakordot"[34], który powstał pod koniec 1920 r. Utworzono dwa jego ośrodki centralne: jeden w Moskwie, drugi w Charkowie[35]. Każdy z oddziałów na obszarze będącym w jego zainteresowaniu tworzył trzy obwody (Obłast' Komitety). Z reguły były to krainy geograficzno-historyczne, jak np. Wołyń czy Galicja Wschodnia. Obłast' Komitety z kolei tworzyły tzw. „Trójki" na szczeblach: okręgowym, powiatowym, miejskim i gminnym. „Trójki" bezpośrednio organizowały grupy bojowe – lotne, czyli komórki terrorystyczne, powoływane doraźnie do wykonania pojedynczej akcji (zamachu), następnie rozwiązywane, a przed kolejnym zadaniem z powrotem reaktywowane.

Do wiosny 1921 r. trwała rozbudowa struktur organizacyjnych „Zakordotu" na terenie Rosji i Ukrainy. Od marca 1921 r. terroryści rozpoczęli ich organizację na terytorium Polski. Członkowie „Trójek" mieli za zadanie zorganizowanie punktów przerzutu ludzi, broni, amunicji, materiałów wybuchowych i innych środków. Z rozpoznania policji i kontrwywiadu wojskowego wynikało, że takie punkty zorganizowano m. in. w Sławucie, Zwiahlu oraz Olewsku. Każdy z nich liczył dwóch i więcej członków. Bojówki terrorystyczne i dywersyjne uzbrojone były przeważnie w broń krótką i karabiny oraz granaty.

Pomimo sprawnie przeprowadzonej pierwszej fazy – organizacyjnej, polskim siłom bezpieczeństwa udało się w lipcu 1922 r. rozbić komórki dywersyjno-terrorystyczne Zakordotu na obszarze powiatu równieńskiego, a pod koniec września 1922 r. ten sam los spotkał bojówki zorganizowane na Pińszczyźnie i w powiecie sarneńskim. Mimo poniesionych strat, w omawianym okresie udało się z sukcesem przeprowadzić kilka napadów innym grupom[36]. 9 lipca 1922 r. zamordowano małżeństwo Korensztajnów w Równem, natomiast 19 lipca 1922 r. napadnięto na miasteczko Nizocz, gdzie zniszczono posterunek policji, urząd pocztowy i gminny. We wrześniu tego samego roku zaatakowano posterunek policji w Wysocku, a w październiku zamordowano agenta policji, Szendera. Członkowie oddziałów dywersyjno-terrorystycznych prowadzili również działalność wywiadowczą, jednak z reguły stanowiła ona zadanie drugorzędne. Natomiast Rosjanie często wykorzystywali już zorganizowane siatki dywersyjne do przerzutu agentów i kurierów. Aktywność Zakordotu wygasła po 1926 r.

---

[34] *Informacja O II DOK V o wysłaniu komunistów z Rosji w celach dywersyjnych do portów polskich,* CAW, SRI DOK V, sygn. I.371.5/A.288.

[35] *Dywersja nieprzyjacielska...*, CAW, Oddz. II SG, sygn. 1917/03/52.

[36] Tamże.

W tym samym mniej więcej okresie, co Zakordot, czyli w 1920 r., przy Centralnym Komitecie Komunistycznej Partii Bolszewików Ukrainy powstało Biuro Galicyjskie (Galbiuro), które skupiało komunistów oraz członków nacjonalistycznych organizacji pochodzących z Galicji Wschodniej. Jak wynika z meldunków wywiadowczych oraz sprawozdań kontrwywiadu wojskowego RP, Biuro stanowiło przykrywkę do działalności szpiegowskiej, terrorystyczno-dywersyjnej oraz propagandowej. W 1921 r., po interwencji rządu RP, organizacja została zlikwidowana. Jednak działania strony radzieckiej były pozorne, bowiem już w roku następnym członkowie Biura założyli przy wsparciu Razwiedupru, tajną organizację terrorystyczno-dywersyjną, która miała prowadzić działania destrukcyjne na obszarze Małopolski Wschodniej. W maju 1922 r. do Polski zostali przerzuceni pierwsi instruktorzy i dowódcy grup terrorystycznych. Tymczasem na terytorium Ukrainy trwało werbowanie ochotników do oddziałów dywersyjnych i intensywne ich szkolenie. Z zeznań dywersantów ujętych przez policję polityczną, wynikało, że mieli oni akcentować komunistyczny charakter ruchu. Oddziały dywersyjne miały być zalążkiem przyszłych jednostek powstańczych, reprezentujących walczący lud ukraiński. Bojówki miały dokonywać zamachów na jednostki policji, wojska, niszczyć linie komunikacyjne i infrastrukturę oraz ośrodki administracji państwowej. Ich celem było także podtrzymywanie nastrojów antypolskich wśród chłopów w Małopolsce, doprowadzenie do ogólnonarodowego powstania i oderwania Małopolski Wschodniej od Rzeczypospolitej[37)] oraz stworzenie państwa o ustroju podobnym do tego, jaki miała Ukraina Radziecka.

Od października do listopada 1922 r. wysłano trzy oddziały dywersyjno-terrorystyczne, które uzyskały wsparcie ze strony już istniejących komórek terrorystycznych. Działaniami objęły one obszar województwa tarnopolskiego, dokonując wielu napadów terrorystycznych, mordując i rabując. W efekcie przeprowadzonej operacji antydywersyjnej wszystkie oddziały terrorystyczne do końca listopada 1922 r. zostały rozbite, a większość terrorystów schwytana. Po tej klęsce Biuro praktycznie zaprzestało aktywnej działalności terrorystycznej, skupiając się na szerzeniu propagandy.

W 1924 r. oficerom kontrwywiadu wojskowego udało się rozgromić kolejną grupę terrorystyczną, występującą pod nazwą Ukraińska Czerwona Powstańcza Armia[38)], która została założona przez członków władz centralnych Kominternu w celu przygotowania konspiracyjnych struktur wojskowych mających działać na Zachodniej Ukrainie[39)]. Operację nadzorował radziecki wywiad wojskowy – Razwiedupr. Rozpracowanie związane z organizacją terrorystyczną zostało zainicjowane po doniesieniu jednego z informatorów SRI DOK II o funkcjonowaniu organizacji dywersyjnej w rejonie wsi Michałkowce, Simonów, Żwizów i Sławuty. Zarządzono inwigilację podejrzanych – Iwana Konohczuka i Mikołaja Kołynczuka, która w krótkim czasie przyniosła pozytywne rezultaty. W wyniku prowadzonych działań operacyjno-rozpoznawczych oficerowie kontrwywiadu uzyskali kolejne informacje o organizacji struktur powstańczych,

---

37) Informacja o działalności sowieckiego wywiadu, Pismo nr 138/II. Tj.22 z 24.03.1922 r., CAW, Oddz. II SG, sygn. I.303.4.1705.

38) Informacja dla Dowódcy Okręgu Korpusu nr V dotycząca likwidacji organizacji szpiegowsko-powstańczej p.n. Ukraińska Czerwona Powstańcza Armia, Pismo nr 56/II.Inf.C.T.O. z 10.01.1925 r., CAW, Oddz. II SG, sygn. I.303.4.2538.

39) Opracowanie *Wstępna ocena ruchu terrorystycznego* z 11.11.1922 r., CAW, Oddz. II SG, sygn. I.303.4.6908.

obejmujących zachodnie powiaty Małopolski Wschodniej i Wołynia. Terroryści dokonywali zakupu broni, amunicji i materiałów wybuchowych, dysponując znacznymi środkami finansowymi (głównie dolarami amerykańskimi). W związku z tym, że zachodziła obawa, iż całość obserwowanych działań wymknie się spod kontroli SRI, kierownictwo kontrwywiadu podjęło decyzję o likwidacji rozpoznanych struktur dywersyjno-terrorystycznych, co doprowadziło do rozbicia komórek bojowych.

W tym samym okresie oficerowie SRI DOK IX w Brześciu przeprowadzili podobną operację na Wołyniu, również i tam niszcząc struktury dywersyjne i terrorystyczne, zorganizowane przez ukraińskich komunistów.

W latach 1925-27 dużą aktywność w organizacji i prowadzeniu działalności dywersyjnej wykazywał ośrodek w Kamieńcu Podolskim. Do oddziałów werbowano mężczyzn w wieku od 18 do 30 lat narodowości ukraińskiej. Zabroniono natomiast wstępować do niego członkom partii. Pod koniec 1925 r. ośrodek został podzielony na trzy konne i dwie piesze grupy, które zostały przerzucone do Rumunii i Polski, gdzie miały dokonywać sabotażu obiektów wojskowych oraz rozbudowywać swoje struktury w oparciu o ludność w rejonie działania, jak również prowadzić agitację komunistyczną. Operacja przerzutu na terytorium Polski została przeprowadzona w 1926 r., jednak dalsze działania nie powiodły się, bowiem grupy dywersantów zostały rozbite.

Jak wynika z dokumentów archiwalnych, kontrwywiadowi wojskowemu udało się ustalić, że od 1923 r. na terytorium Białoruskiej Republiki Radzieckiej wywiad (Razwiedupr) i OGPU szkoliły białoruskich i polskich komunistów w specjalnych szkołach dywersantów, które znajdowały się w Puchowiczach, Mińsku, Bobrujsku, Borysowie, Smoleńsku i Homlu. Początkowo byli oni przygotowywani tylko do prowadzenia dywersji ideologicznej, lecz od 1924 r. rozszerzono profil szkolenia, który obejmował również przedmioty wojskowe i wywiadowcze[40]. Kursantów uczono sposobów budowy sieci informacyjnej i uzyskiwania danych wywiadowczych, przygotowywania komórek i grup dywersyjnych (terrorystycznych) oraz podstaw organizacji działań partyzanckich. Grupy dywersyjne formowano w wyznaczonych obozach na Białorusi, tam też były one uzbrajane i ekwipowane, a następnie przerzucane na terytorium Rzeczypospolitej[41]. Zasadniczym celem grup było przygotowanie ludności do powstania przeciw Polsce, zdobywanie funduszy na działania komunistów białoruskich oraz kompromitowanie władz administracyjnych Rzeczypospolitej.

Informacje podobnej treści przekazywał attaché wojskowy RP w Moskwie, mjr Kobylański, który informował o powstawaniu grup dywersyjnych i terrorystycznych na Ukrainie. Działania destrukcyjne prowadzone z inspiracji władz radzieckich miały wywołać na Kresach Wschodnich chaos i spowodować powszechne powstanie, które miało zakończyć się przyłączeniem tych terenów do zachodnich republik ZSRR[42]. Według dyplomaty, kolejnym celem miało być odwrócenie uwagi ludności republik rosyjskich od trudności ekonomicznych i wewnętrznych, jakich doświadczał wówczas ZSRR.

W listopadzie 1928 r., pomimo doświadczeń z nieudanych wystąpień w pierwszej połowie lat dwudziestych, komuniści białoruscy po raz kolejny opowiedzieli się za or-

---

[40] *Organizacja band dywersyjnych*. Informacja dla Ministerstwa Spraw Wewnętrznych z 16 marca 1925 r., CAW, Oddz. II SG, sygn. I.3030.4.2538.

[41] Tamże.

[42] *Organizowanie akcji dywersyjnej przez Sowiety*. Informacja Attaché wojskowego RP w Moskwie z 1925 r., CAW, Oddz. II SG, sygn. I.3030.4.2538.

ganizacją i wybuchem powstania, które doprowadziłoby do oderwania ziem zachodniej Białorusi i przyłączenia ich do Białoruskiej SRR. W swojej naiwności nie wykluczali oni udziału w zamieszkach nawet Armii Czerwonej[43]. KPP początkowo odniosła się krytycznie do zamierzeń KPZB i KPZU, jednak w miarę rozwoju akcji terrorystycznych i partyzanckich dążyła do przejęcia nad nimi koordynacji i kontroli. Wobec natychmiastowej i dobrze skoordynowanej akcji policji, KOP i wojska, większość grup terrorystycznych i niewielkich oddziałów partyzanckich została rozbita i rozproszona. Nie oznaczało to jednak, że komuniści zaniechali prowadzenia działalności destrukcyjnej na polskich Kresach Wschodnich. W kolejnych latach kontynuowali bowiem akcje terrorystyczne i dywersyjne, jednocześnie na dużą skalę prowadząc pracę agitacyjną wśród ludności ukraińskiej i białoruskiej.

Działalność wywrotowa komunistów po przewrocie majowym

W latach 1925-26, po rozbiciu wojskówki KPP[44], Komitet Centralny KPP podjął uchwałę o utworzeniu tymczasowego Wydziału Agitacji w wojsku przy Sekretariacie KC, który na nowo miał zorganizować Wydziały Wojskowe przy komitetach okręgowych i obwodowych partii komunistycznej. Wydział Agitacji poprzez Centralny Podwydział WW[45] miał kierować działalnością komórek w jednostkach wojskowych, jednak ta struktura nigdy nie rozpoczęła działalności. Do kolejnych zmian doszło w 1927 r., kiedy utworzono Centralny Wydział Wojskowy (dalej: CWW) KPP oraz rozpoczęto organizowanie struktur terenowych[46]. Kadry dla WW były kształcone w Wojskowej Szkole Politycznej KPP w Moskwie[47]. W ten sposób zaczął się zupełnie nowy okres w politycznej działalności ruchu komunistycznego, który charakteryzował się wzmożoną pracą agitacyjną w siłach zbrojnych, organizowaniem struktur konspiracyjnych oraz dalszym zacieśnianiem związków z radzieckimi służbami specjalnymi. Podczas II Plenum KPP posunięto się nawet do uchwalenia zadań, z których wynikało, że komuniści w przypadku konfliktu będą traktować armię polską jako wojska okupacyjne[48]. Chociaż organom bezpieczeństwa kilkakrotnie udało się rozbić struktury wojskowe KPP, to odradzały się, zasilane przez komunistów przerzucanych z ZSRR. Działalność ta trwała nieprzerwanie aż do upadku państwa polskiego, nawet wtedy, gdy KPP jako partia została rozwiązana, a większość kierownictwa ściągnięto do ZSRR i rozstrzelano.

Kolejna fala intensyfikacji działalność dywersyjnej i dywersyjno-wywiadowczej przypadła na przełom lat 1931-32, kiedy część działaczy KPZU zorganizowała sieć ko-

---

43) H. Cimek, *Komuniści, Polska...*, s. 58-59.

44) Potoczna nazwa wydziałów wojskowych KPP.

45) H. Cimek, *Komuniści, Polska...*, s. 205-06.

46) I. Pawłowski, *Polityka i działalność...*, s. 208.

47) Wojskowa Szkoła Polityczna powstała w Moskwie. Jej zadaniem było przygotowanie wykwalifikowanych kadr komunistycznych do działalności w strukturach Sił Zbrojnych. W szkole prowadzono sześciomiesięczne kursy. Kierownikiem politycznym był Leon Purman, a wojskowym Stefan Żbikowski. Przedmioty wojskowe wykładali m. in. Feliks Kon, Karol Świerczewski, Jan Unszlicht, Stefan Bortnowski. Byli to albo oficerowie Armii Czerwonej, albo ludzie związani z IV Oddziałem Sztabu RKKA. Z przedmiotów wojskowych uczono: taktyki i organizacji armii polskiej, teorii powstania organizacji i prowadzenia walk partyzanckich, taktyki i organizacji walk w ośrodkach zurbanizowanych. Ponadto wykładano naukę o broni, minerstwie i topografii wojskowej. Szkoła ta była klasycznym ośrodkiem szkolenia wywiadowczo-dywersyjnego, Tamże, s. 211.

48) H. Cimek, *Komuniści, Polska...*, s. 73.

mórek dywersyjnych na Wołyniu i rozpoczęła działania terrorystyczne[49]. Nie miały one jednak charakteru masowego wystąpienia zbrojnego, lecz były raczej próbą destabilizacji tej części Rzeczypospolitej. Grupy te zostały dość szybko rozbite przez oddziały policji i KOP. Nie powstrzymało to jednak naszego wschodniego sąsiada przed kolejnymi próbami zorganizowania siatek o takim charakterze.

Na początku 1932 r. na terytorium Polski został przerzucony doświadczony komunista Antoni Suszko, który otrzymał zadanie zorganizowania struktur dywersyjno-terrorystycznych w oparciu o członków partii komunistycznej – Polaków – byłych żołnierzy Armii Czerwonej oraz członków grup dywersyjnych z lat 1924-26[50]. Suszko nawiązał również kontakt z członkami białoruskich oddziałów dywersyjnych o charakterze nacjonalistycznym. Miał stworzyć sieć grup, które pozostałyby „uśpione" aż do wybuchu konfliktu polsko-radzieckiego[51].

A. Suszko okazał się dość sprawnym organizatorem i wytrawnym konspiratorem. Udało mu się bowiem zwerbować, a następnie przeszkolić kilkunastu członków swojej organizacji. Następnie podzielił przydzielony mu teren na rejony i podrejony oraz wyznaczył poszczególnym osobom obszary odpowiedzialności, na których mieli organizować siatki dywersyjne. Zwerbowanych członków siatki przerzucał do ZSRR, gdzie przechodzili specjalistyczny kurs dywersyjno-wywiadowczy. Suszko rozpoczął również organizowanie struktur konspiracyjnych na obszarze Wołkowyska, Białowieży i Słonimia, lecz jego działalność została przerwana kontrakcją policji politycznej.

Dopiero postępująca normalizacja w stosunkach polsko-radzieckich oraz prowadzone od 1933 r. rozmowy w sprawie podpisania układu o nieagresji[52] doprowadziły do pewnego osłabienia aktywności organizacji komunistycznych. Zresztą, władze Kominternu już w 1931 r. wydały polecenie, aby KPP odcięła się od wystąpień terrorystycznych na Wołyniu. Podobnie było w latach 1924–25, gdy ZSRR, nie chcąc wszczynać konfliktu z Polską, nakazał władzom Kominternu wycofanie KPP i jej przybudówek z oficjalnego wsparcia działań dywersyjnych na Kresach oraz przygotowań do zbrojnych wystąpień na terytorium Polski[53]. Poprawa w stosunkach polsko-radzieckich nie doprowadziła jednak do zaprzestania destrukcyjnej działalności komunistów.

Komórki „wojskówki" partii komunistycznej i metody działania w jednostkach Wojska Polskiego

Centralny Wydział Wojskowy był częścią składową KPP. Miał zajmować się przygotowaniem wojskowych kadr komunistycznych oraz kadr partii do powstania zbrojonego, a także prowadzić działalność destrukcyjną w jednostkach wojskowych i po-

[49] Tamże, s. 59-60.

[50] Referat Kierownika SRI DOK IX, kpt. F. Nowaka, wygłoszony 15 grudnia 1934 r. na konferencji prokuratorów w Wilnie, na temat *Ruch komunistyczny na terenie DOK IX*, CAW, SRI DOK IX, sygn. I.371.9/A.891.

[51] Tamże.

[52] 25 lipca 1932 r. został podpisany w Moskwie polsko-radziecki pakt o nieagresji (parafowany 25 stycznia 1932 r.). Układ ten pierwotnie został zawarty na trzy lata. 5 maja 1934 r., po kolejnych rozmowach, przedłużono jego obowiązywanie o 10 lat. J. Ślusarczyk, *Polska a państwo radzieckie. Kalendarium 1918--1939*, Warszawa 1996, s. 108-109.

[53] H. Cimek, *Komuniści, Polska...*, s. 60.

zyskiwać dane wywiadowcze o systemie obronnym Rzeczypospolitej. Podlegały mu Wydziały Wojskowe i Wydział Techniki Wojennej[54]. Te z kolei dzieliły się na komórki wojskowe, działające w jednostkach wojskowych, sztabach, instytucjach wojskowych oraz zakładach przemysłu zbrojeniowego[55]. Komórka składała się z dwóch do pięciu członków. Poza komórkami w jednostkach wojskowych istniały tzw. „separatki". Prowadziły one samodzielną pracę wywiadowczo-ideologiczną w oparciu o zadania wcześniej postawione w wydziale okręgowym. Komórki komunistyczne uzyskiwały dane o liczbie żołnierzy, ich morale i stanie gotowości bojowej jednostki oraz o ilości i typach uzbrojenia, a także o stanie zapasów mobilizacyjnych. Dane te były przesyłane okręgowym WW. Oprócz działalności wywiadowczej członkowie komórek organizowali pogadanki oraz kolportaż tzw. bibuły. Brali również udział w aktywnych formach walki ideologicznej (dywersji), na przykład w wywieszaniu haseł o treściach komunistycznych i antypaństwowych oraz czerwonych sztandarów. Ponadto, członkowie wojskowych struktur konspiracyjnych mieli uczestniczyć w działaniach prowadzących do wywoływania antagonizmów na tle narodowościowym i buntów wśród żołnierzy. W trakcie mobilizacji wojennych mieli również organizować bojkot procesu mobilizacyjnego, unieruchamiać pracę w fabrykach zbrojeniowych oraz tworzyć oddziały dywersyjne, prowadzące walkę z jednostkami policji i wojska[56].

Szczególnie ważna z punktu widzenia kierownictwa kompartii była działalność wśród poborowych, a następnie żołnierzy służących w jednostkach wojskowych. Zwracano uwagę na ich przygotowanie do prowadzenia działalności wywrotowej w wojsku. Starano się zakonspirować szczególnie aktywnych członków KZM i KPP, którzy po wcieleniu mieli przystąpić do organizowania komórek komunistycznych w pododdziałach i oddziałach. W tym celu komuniści otrzymywali dane, z kim mają się skontaktować po wcieleniu, jakich haseł rozpoznawczych używać (tj. jak nawiązać łączność z innymi członkami partii)[57].

Od połowy lat trzydziestych część poborowych (członków i sympatyków partii komunistycznej) otrzymywała polecenie ucieczki do ZSRR. Tam zgłaszali się pod wskazany adres i byli szkoleni w zakresie prowadzenia działalności agitacyjno-propagandowej oraz szpiegowskiej, a następnie z powrotem przerzucano ich do Polski. Za przykład może posłużyć sprawa działacza komunistycznego Jana Jakowlewa vel Jakuba Żukowa vel Jana Rutkowskiego, który zeznał, że na terytorium ZSRR prowadzono szkolenie z zakresu dywersji i sabotażu dla działaczy KPZB[58].

---

[54] Wydział Techniki Wojennej podlegał bezpośrednio pod CWW, ale posiadał odrębne struktury organizacyjne na szczeblu okręgu, dzielnic miast (garnizonów) i jednostek. Zajmował się przygotowaniem wyposażenia i materiałów dla WW. Członkowie tego pionu organizowali składy materiałów wybuchowych, broni i amunicji oraz przygotowywali akcje terrorystyczno-dywersyjne. Mieli również zapewnić łączność poszczególnym komórkom i wydziałom wojskowym.

[55] *Referat SRI DOK II dotyczący akcji Kominternu na terenie wojska*, Pismo nr L. Dz. 4664/Inf.NR.tj.36. z 25.08.1936 r., CAW, SRI DOK II, sygn.I.371/2/A.96.

[56] Uchwała II Plenum KC KPP głosiła, że „w takich wypadkach partia ujmuje w swoje ręce ten ruch, organizuje na gruncie oporu przeciw mobilizacji walkę masową do walki partyzanckiej włącznie", *Raport kontrwywiadowczy...*, CAW Oddz. II SG, sygn. I.303.4.2630.

[57] Raport kontrwywiadowczy..., CAW, Oddz. II SG, sygn. I.303.4.2630.

[58] *Informacja dot. Jakowlewa Jana vel Żukowa Jakuba vel Rutkowskiego Jana z 27.02.1935 r.*, CAW, SRI DOK IX, sygn. I.371.9/A.865.

W 1931 r. policji politycznej udało się przejąć opracowanie pt. *Przyczynek do sprawy powstania zbrojnego*, opublikowane nakładem KC KPZB i opracowane przez G. Rwala[59]. Dzięki temu uzyskano szereg interesujących danych dotyczących organizacji oraz form i metod działań obowiązujących w kompartii. G. Rwal dokonał bowiem analizy warunków, w jakich KPP mogłaby zorganizować i przeprowadzić powstanie. Uważał, iż powstanie zbrojne stanowi jedną z form walki politycznej, dlatego też kompartia musi się do niego dobrze przygotować, zarówno w sferze wyszkolenia oddziałów, jak i zaopatrzenia. Walka powinna zostać zainicjowana przez działania terrorystyczne i dywersyjne oraz ogólnopolską akcję strajkową, co powinno doprowadzić do powszechnego chaosu i destrukcji administracji państwowej. I dopiero po zdezorganizowaniu życia wewnętrznego i porządku publicznego miało dojść do powszechnego powstania, które objęłoby całe terytorium Rzeczypospolitej[60].

Opracowanie G. Rwala daje teoretyczne podstawy do stwierdzenia, iż rozruchy, jakie miały miejsce na przełomie 1931 i 1932 r. na Wołyniu, Polesiu i w Małopolsce[61] mogły stanowić próbę możliwości powstańczych ludności i struktur komunistycznych[62].

Po 1936 r. działalność KPP była już jednak schyłkowa. Rozpoczęły się bowiem pierwsze przesłuchania wybitnych działaczy partii w Moskwie, choć struktury komunistyczne nadal prowadziły aktywną działalność konspiracyjną[63]. Wyrazem tego były m. in. *Wytyczne Kompartii do roboty w wojsku* z lutego 1937 r.[64] W 1937 r. działacze KPP spodziewali się konfliktu zbrojnego (najprawdopodobniej z udziałem ZSRR). Nakazywali w związku tym Komitetom Dzielnicowym i Okręgowym partii tworzenie Wydziałów Wojskowych Czerwonej Pomocy. Ponadto, na wypadek wojny członkom zlecono gromadzenie informacji o obozach dla internowanych i stworzenie wojennego systemu łączności.

Z materiałów Oddziału II wynika, że mimo rozwiązania KPP, działalność struktur szczebla podstawowego tej partii nie ustała[65]. Komintern nadal bowiem utrzymywał łączność z komórkami KPZU i KPZB. Informacje uzyskane przez Wydział Bezpieczeństwa Białostockiego Urzędu Wojewódzkiego w lutym 1939 r. wskazują,

---

59) Pismo Wydziału Bezpieczeństwa Publicznego Białostockiego Urzędu Wojewódzkiego nr BP III-242/31 T z 17.01.1931 r., CAW, SRI DOK IX, sygn. I.371.9/A.98.

60) Tamże. s. 3-4.

61) Na przełomie 1932 i 1933 r. w wyniku starć z policją w walkach ulicznych i wiejskich zginęło ponad 70 robotników i chłopów, a kilkudziesięciu zostało rannych. W rozruchach ponieśli śmierć również policjanci, A. Próchnik (H. Swoboda), *Pierwsze piętnastolecie Polski Niepodległej. Zarys dziejów politycznych*, Warszawa 1983, s. 379-380.

62) Tamże, s. 376-378, s. 380.

63) Było to wyrazem przejścia wszelkich legalnych i półlegalnych struktur KPP do konspiracji. Stało się tak na mocy otrzymanej z Kominternu instrukcji o zmianach struktur i zasad działalności partii komunistycznych. Akcja przechodzenia do konspiracji została przeprowadzona na wiosnę 1937 r. Członkowie KPP mieli uczestniczyć w ćwiczeniach wojskowych oraz starać się nawiązywać kontakty z żołnierzami. Pismo SRI DOK IX dotyczące przygotowań kompartii do wystąpień zbrojnych oraz akcji na wypadek wojny nr L. dz. 1521/Inf.tj.Nar. z 05.03.1937 r., CAW, SRI DOK IX, sygn. I.371.9/A.891.

64) Opracowanie dotyczące reorganizacji roboty wojskowej w kompartii nr L. dz. 246/Inf.tj.Nar. z 06.02.1937 r., CAW, SRI DOK IX, sygn. I.371.9/A.891.

65) KPP została rozwiązana wiosną 1938 r., lecz jej kierownictwo było likwidowane praktycznie od 1933 r. (Jerzy Czeszejko-Sochacki). Większość kierownictwa i liczących się członków KPP została ściągnięta do ZSRR w 1937 r. i w sfingowanych procesach skazana na karę śmierci i stracona. red. J. Tazbir, *Polska na przestrzeni wieków*, Warszawa 1995, s. 609.

że na obszarze Białoruskiej SRR organizowano kursy dywersyjne dla członków partii komunistycznych[66]. Byli oni ściągani na terytorium ZSRR po podaniu określonego hasła w jednym z programów radzieckiego radia. Kursy trwały kilka miesięcy, a po ich zakończeniu mieli być przerzuceni z powrotem do Polski. Zarówno ta informacja, jak i poprzednie wskazują, iż po rozwiązaniu organizacji partyjnych KPP przez władze Kominternu, członkowie tej partii zostali przejęci przez radziecki wywiad wojskowy, który przeprowadził ich specjalistyczne szkolenie dywersyjne i szpiegowskie.

Zakończenie

Nie ulega wątpliwości, że część struktur komunistycznych była przygotowywana do działań wywiadowczo-dywersyjnych na rzecz ZSRR. Przystąpienie do Kominternu Komunistycznej Partii Polski było świadomym podporządkowaniem się komunistów polskich instytucjom państwowym ZSRR, bowiem Komintern był jeszcze jedną agendą radzieckich służb specjalnych. Należy jednak pamiętać, iż część działaczy KPP sprzeciwiała się prowadzeniu działalności wywiadowczej i dywersyjnej przeciwko państwu polskiemu. Ta część została jednak dość szybko wyeliminowana. Działania wywiadowcze i terrorystyczne jej członków zagrażały bezpieczeństwu państwa i miały, obok celów destrukcyjnych, olbrzymi wpływ na utrzymanie porządku publicznego. Afery Płatka, Buchty, Feiwla, Mühlrada i towarzyszy czy Cyli Khol[67] są najlepszym przykładem powiązań polskich komunistów z radzieckimi służbami specjalnymi. I nie są to odosobnione przypadki, gdyż spraw kontrwywiadowczych o charakterze szpiegowskim, dywersyjnym i terrorystycznym z udziałem komunistów Defensywa Polityczna (a później policja polityczna) i Wydział II b oraz jego jednostki terenowe prowadziły rocznie po kilkaset. Świadczy to nie tylko o możliwościach KPP i jej satelitów, ale przede wszystkim o determinacji i masowym charakterze działalności wywiadowczo-dywersyjnej i terrorystycznej prowadzonej przez ZSRR.

Kontrwywiad wojskowy oraz defensywa policyjna przywiązywały dużą wagę do rozpoznawania i likwidacji zagrożenia ze strony ruchu komunistycznego, słusznie uważając, że był on wykorzystywany przez obce służby specjalne do prowadzenia działalności destrukcyjnej, zagrażającej bezpieczeństwu państwa polskiego. Należy jednak stwierdzić, że wypracowywana przez szereg lat metodyka i zaangażowanie pojedynczych oficerów kontrwywiadu i policji politycznej w przeciwdziałanie wywiadowczej i terrorystycznej działalności komunistów przynosiły pożądane efekty. Trudno jednak w pełni ocenić zaangażowanie komunistów z KPP w działalność antypolską ze względu na brak dostępu do archiwów radzieckich wojskowych i cywilnych służb specjalnych. Można natomiast stwierdzić, że destrukcyjna działalność komórek komunistycznych wymuszała konieczność utrzymywania w gotowości dużej ilości sił i środków służb bezpieczeństwa II RP.

---

[66] Informacja nr PB.II.15-M-4/39 z 10.02.1939 r. dotycząca kursów partyzanckich w ZSRR, CAW, SRI DOK IX, sygn. I.371.9/A.874.

[67] Na temat wymienionych rozpracowań kontrwywiadowczych więcej u: A. Krzak, *Kontrwywiad wojskowy II Rzeczypospolitej*..., s. 229–236.

ABSTRACT

The article covers the outline of the extremely left – oriented parties and their activity in the framework of the Komintern. At the breakthrough of the 1918 – 1919 the Polish communists began to create the structures of the Delegates' Councils copied from the Soviet communists. They tried to implement their program leading to the initiation of the revolutionary process. The activity of communists was intensified with the outbreak of the Polish – Soviet war. The activity of KPRP was divided: on the one hand that communist party conducted legal political activity taking part in the parliamentary elections and was a member of Parliament and on the other hand it prepared canvassers and social spheres to revolutionary performances. Simultaneously, the counteracting the diversion groups and the activity of communist parties and organizations was one of the most important tasks of counterintelligence service of the II Polish Republic. Following the documents of II Administration of General Staff, the Polish Army paid attention to identification of the internal structures of KPP, KPZU, KPZB, KZM and other organizations conducting the agitation and diversionary activity. There was a considerable series of successes often leading to destruction of the communist cells and stopping their activity even for dozens of months.

II.
ANALIZY

Agata Furgała
Damian Szlachter
Anna Tulej
Paweł Chomentowski

System antyterrorystyczny Wielkiej Brytanii. Wybrane zagadnienia[1)]

Wstęp

Wielka Brytania od kilku dekad boryka się z kolejnymi falami współczesnego terroryzmu skierowanymi przeciwko jej obywatelom oraz narodowym interesom. Obecna „ponowoczesna" aktywność (ang. *postmodern*) zdominowana jest przez skrajnie radykalne jednostki, wykorzystujące wypaczoną i niszową wersję islamskiej wiary do usprawiedliwiania popełniania aktów przemocy, jako metody osiągnięcia celów politycznych.[2)] Na bazie wieloletnich doświadczeń, kraj ten stworzył najbardziej kompleksowy antyterrorystyczny system prawny w Unii Europejskiej oraz wypracował spójną narodową strategię walki ze zjawiskiem terroryzmu, realizowaną przez szereg podmiotów wplecionych w wielopoziomowy system instytucjonalno – prawny, który został przedstawiony poniżej.

CONTEST – narodowa strategia walki z terroryzmem

CONTEST (ang. *The United Kingdom's Strategy for Countering International Terrorism*[3)]) strategia opierająca się ona na 4 niżej przedstawionych filarach (ang. 4P's), realizowanych wewnątrz państwa oraz poza jego granicami, tj.:

Filar I. **Present** – zapobieganie czynnikom oraz przyczynom powstania terroryzmu;

Filar II. **Pursue** – ściganie terrorystów wraz z osobami wspierającymi ich aktywność;

Filar III. **Protect** – skuteczna ochrona obywateli oraz obiektów użyteczności publicznej stanowiących element narodowej infrastruktury krytycznej, przed skutkami ataków terrorystycznych;

Filar IV. **Prepare** – przygotowanie do konsekwencji zaistniałych zamachów terrorystycznych, czyli budowanie zdolności reagowania kryzysowego oraz likwidacji skutków takich zdarzeń.

[1)] Tekst został przygotowany na potrzeby projektu rozwojowego nr OR00004007 finansowanego ze środków Ministerstwa Nauki i Szkolnictwa Wyższego przeznaczonych na naukę w latach 2009-2011.

[2)] Charakterystyczne dla działalności terrorystycznej są czasowe fazy nasilenia i ograniczenia aktów przemocy – tzw. „fale terroryzmu". Okres końca lat sześćdziesiątych do połowy lat osiemdziesiątych został nazwany „trzecią falą" w dotychczasowej historii terroryzmu. Na terenie Europy przejawiała się ona w postaci klasycznej działalności skrajnie lewicowych, skrajnie prawicowych oraz nacjonalistyczno-separatystycznych grup terrorystycznych. Zob. Borkowski R., *Terroryzm ponowoczesny*, Wydaw. Adam Marszałek, Toruń 2006 r., s. 50. Por. Laqueur W., *Postmodern*, „Foreign Affairs" nr 5, 1996, s. 24-36.

[3)] W marcu 2009 r. weszła w życie nowa wersja strategii, tzw. CONTEST II.

Brytyjska strategia walki z terroryzmem podlega okresowej ocenie, w której uwzględniane są postępy w realizacji wszystkich czterech filarów oraz prezentowane nowe zadania oraz inicjatywy przygotowywane w tym obszarze.

Legislacja antyterrorystyczna

Brytyjskie przepisy antyterrorystyczne zawarte są w czterech ustawach kierunkowych:

1. *Terrorism Act 2000,*
2. *Anti-Terrorism Crime and Security Act 2001,*
3. *Prevention of Terrorism Act 2005,*
4. *The Terrorism Act 2006.*

Powyższe akty prawne wprowadziły następujące uprawnienia oraz rozwiązania systemowe:

a) listę proskrypcyjną organizacji terrorystycznych (lista organizacji nielegalnych) – wprowadza ona zakaz działania wskazanych podmiotów na terytorium Wielkiej Brytanii;
b) nowe uprawnienia dla służb policyjnych, np. prawo do zatrzymywania osób podejrzanych o terroryzm na okres 28 dni bez nakazu sądu;
c) penalizację przestępstw kryminalnych kluczowych dla walki z terroryzmem:
   - podżeganie do popełniania aktów terroryzmu,
   - gloryfikowanie terroryzmu lub pośrednie namawianie do stosowania takich metod,
   - dystrybucja terrorystycznych materiałów propagandowych,
   - czyny mające na celu przygotowanie ataku terrorystycznego,
   - szukanie możliwości szkolenia lub szkolenie terrorystów na terytorium kraju albo poza jego granicami,
   - dostarczanie wiedzy lub szkolenie dotyczące użycia broni, materiałów wybuchowych, substancji chemicznych, biologicznych lub nuklearnych.
d) wzmocnienie prawa dotyczącego zwalczania finansowania terroryzmu, poprzez stworzenie możliwości gromadzenia i wymiany informacji koniecznych do przeciwdziałania terroryzmowi pomiędzy instytucjami rządowymi;
e) rozbudowanie procedur imigracyjnych;
f) podwyższenie norm bezpieczeństwa przemysłu lotniczego i nuklearnego;
g) zwiększenie rygoru dostępu i ochrony wobec niebezpiecznych substancji, które mogą zostać użyte przez terrorystów;
h) wprowadzenie tzw. „nakazów kontrolnych" w stosunku do osób podejrzanych o aktywność o charakterze terrorystycznym (zarówno obywateli Wielkiej Brytanii, jak i obcokrajowców) – prawo to daje możliwość ograniczania swobód obywatelskich osób, od zakazu dostępu do konkretnych rzeczy lub usług, poprzez zakaz spotykania się z konkretnymi osobami, aż do ograniczeń w przemieszczaniu się.

Brytyjski system instytucjonalny do walki z terroryzmem

Każda sytuacja kryzysowa wywołana na terenie Zjednoczonego Królestwa przez międzynarodowy terroryzm staje się sprawą wagi państwowej i jest koordynowana na poziomie rządowym. Złożoność systemu antyterrorystycznego Wielkiej Brytanii powoduje, iż w mechanizmie tym uczestniczy szereg opisanych poniżej organów ad-

ministracji państwowej oraz gremia powołane do współpracy międzyinstytucjonalnej, takie jak:

1. **Urząd Premiera Zjednoczonego Królestwa** (ang. *the United Kingdom Cabinet Office*) **–** pełni funkcję koordynacyjną wobec wszelkiej aktywności administracji państwowej związanej z walką z terroryzmem, wykorzystując w tym celu następujące struktury i mechanizmy decyzyjne:
   a) **Rządowe Biuro Koordynacji** (ang. *Cabinet Office Briefing Room* – tzw. COBRa) – miejsce koordynacji działań rządu Zjednoczonego Królestwa w sytuacjach kryzysowych o charakterze ogólnonarodowym, zapewniające funkcjonowanie wysokich przedstawicieli struktur administracji państwowej w trybie 24/7. Rządowemu Biuru Koordynacji przewodniczy minister, właściwy w zakresie reagowania na zamachy terrorystyczne, czyli minister spraw wewnętrznych. Natomiast w momencie bezpośredniego zagrożenia bezpieczeństwa państwa COBRa zbiera się pod przewodnictwem premiera (Rządowe Biuro Koordynacji posiada własny bezpieczny system łączności umożliwiający m. in. przeprowadzenie wideokonferencje);
   b) **Wiodący Resort Rządowy** (ang. *Lead Government Department* – LGD's) – struktura sprawująca kierowniczą rolę w kwestiach decyzji podjętych przez rząd w związku z wystąpieniem sytuacji kryzysowych;
   c) **Rządowy Sekretariat ds. Sytuacji Nadzwyczajnych** (ang. *Cabinet Civil Contingency Secretary* – CCS) – identyfikuje oraz analizuje rodzaje zagrożeń dla narodowej infrastruktury krytycznej (ang. *UK's Critical National Infrastructure* – CNI), a następnie przygotowuje krajowe plany reagowania na wytypowane zagrożenia. CCS koordynuje jednocześnie pracę kluczowych działów administracji rządowej oraz innych kierunkowych instytucji w czasie sytuacji kryzysowej. Aktywność Rządowego Sekretariatu ds. Sytuacji Nadzwyczajnych nadzoruje Stały Sekretarz ds. Wywiadu, Bezpieczeństwa i Przywracania Ciągłości Funkcjonowania Państwa – (ang. *Permanent Secretary for Intelligence, Security and Resilience*);
   d) **Strategiczne Centrum Koordynacji** (ang. *Strategic Coordination Center – Gold*) to rządowy punkt kontaktowy znajdujący się w miejscu wystąpienia sytuacji kryzysowej, dowodzony przez wysokiego przedstawiciela sił policyjnych – (tzw. *Gold Commander*)[4];
   e) **Centrum Koordynacji Informacyjnej** (ang. *News Coordination Centre* – NCC) – aktywowane[5] jest w sytuacji nadzwyczajnej, na bazie personelu zajmującego się komunikacją w ramach *Cabinet Office*. Odpowiada za:
      - zbieranie informacji ze Strategicznego Centrum Koordynacji,
      - rozpowszechnianie pozyskanej wiedzy (z zachowaniem poufności wybranych danych) w ramach rządu oraz kluczowych instytucji państwowych,

[4] Przy Strategicznym Centrum Koordynacji działa Punkt Kontaktowy dla Prasy (ang. *Press Liaison Point),* przy którym akredytowani przedstawiciele mediów otrzymują oficjalne komunikaty o bieżącej sytuacji.

[5] NCC osiąga zdolność do działania w ciągu 90 min. od momentu powołania przez Biuro ds. Komunikacji przy Urzędzie Premiera – (ang. *Cabinet Office Communication Group*). Funkcjonuje w trybie 24/7.

- przekazywanie regularnych komunikatów do opinii publicznej za pośrednictwem specjalistycznych rządowych portali internetowych[6] oraz innych mass-mediów[7], zgodnie z wytycznymi LGD;
- przygotowanie oceny relacji dziennikarzy prezentujących dane wydarzenie.

NCC funkcjonuje na potrzeby Wiodącego Resortu Rządowego i w tym celu blisko współpracuje od strony technicznej i merytorycznej z reprezentantami Rządowej Sieci Informacyjnej (ang. *Government News Network* – GNN[8]), m. in. na miejscu zdarzenia terrorystycznego (poza Londynem);

f) Rządowy Zespół Łącznikowy (ang. *Government Liaison Team* – GLT) to multidyscyplinarna jednostka, dowodzona przez Oficera Łącznikowego Rządu (ang. *Government Liaison Officer* – GLO), odpowiadająca za zapewnienie kanału łączności pomiędzy COBR, a Strategicznym Centrum Koordynacji na miejscu zdarzenia nadzwyczajnego;

g) Połączony Komitet Wywiadu (ang. *Joint Intelligence Committee* – JIC) – harmonizuje bieżącą pracę i wytycza priorytety dla kierunkowych służb specjalnych w zakresie m. in. pracy analityczno-informacyjnej w ramach tzw. Wspólnoty Wywiadowczej (ang. *UK Intelligence Community Online*[9]). Zapewnia również dostarczanie informacji wywiadowczych dotyczących zagrożeń na potrzeby Premiera oraz właściwych ministrów;

2. Ministerstwo Spraw Wewnętrznych (ang. *Home Office*) – centralny punkt reagowania na zagrożenia terrorystyczne w kraju, kształtujący politykę antyterrorystyczną państwa. MSW, w zakresie swoich kompetencji odpowiada za walkę z terroryzmem na terenie Anglii, Walii i Szkocji. Z kolei obszar Irlandii Północnej podlega w tej materii Ministerstwu ds. Irlandii Północnej (ang. *Northern Ireland Office*). W *Home Office* umiejscowiono **Biuro ds. Bezpieczeństwa i Walki z Terroryzmem** (ang. *Office for Security and Counter-Terrorism* – OSCT) – jednostkę właściwą

---

[6] W celu zwiększenia skuteczności informacyjnej programu rządowego - *UK Resilience Programm* i kampanii – *Preparing for Emergencies* lub *London Prepared* (przygotowane specjalnie dla aglomeracji londyńskiej) realizowanych przez szereg wybranych organów administracji państwa oraz instytucji partnerskich, uruchomiono trzy tematyczne portale internetowe (http://www.ukresilience.info/; http://www.preparingforemergencies.gov.uk/; http://www.londonprepared.gov.uk/). Na co dzień służą one m.in. jako baza wiedzy z zakresu przygotowań na zagrożenia dla bezpieczeństwa obywateli, natomiast w momencie sytuacji kryzysowej zamieniają się w bieżące (aktualizacja co 30 min.) źródło informacji. NCC umieszcza na wyżej wymienionych stronach internetowych wystąpienia z briefingów prasowych, wskazówki, instrukcje i plany działania, mapy, statystyki, alarmy lub inne ostrzeżenia.

[7] Współpraca z mediami w sytuacjach kryzysowych powinna następować zgodnie z wcześniej uzgodnionym protokołem dwustronnych kontaktów, przygotowanym przez Medialne Forum ds. Sytuacji Nadzwyczajnych - (MEF) lub Brytyjską Korporację Nadawczą – (ang. *British Broadcasting Corporation* – BBC). W wypadku BBC jest to inicjatywa – tzw. *Connecting in a Crisis*.

[8] GNN to agencja informacyjna stanowiąca lokalne ramię centralnej administracji państwowej. Specjalizuje się w zapewnianiu eksperckiego poziomu komunikacji regionalnej i jest zaufanym pośrednikiem podmiotów rządowych w kontaktach z mediami, szczególnie na wypadek zaistnienia sytuacji nadzwyczajnych.

[9] Brytyjska Wspólnota Wywiadowcza działająca w ramach *Cabinet Office* składa się z przedstawicieli następujących instytucji: Służby Wywiadu, zwanej często MI6 (ang. *Secret Intelligence Service* – SIS), Służby Bezpieczeństwa, zwanej często MI5 (ang. *UK's Security Service*), Połączonego Centrum Analiz Terroryzmu (ang. *Joint Terrorism Analysis Centre* – JTAC), Jednostki Wywiadu Wojskowego (ang. *Defense Intelligence Staff* – DIS), Ministerstwa Obrony (*Ministry of Defense* – MOD), Centrum Łączności Rządowej (ang. *Government Communication Headquarters* – GCHQ). Za: *National Intelligence Machinery*, The UK Stationery Office, 2006.

do wspierania i koordynowania codziennej aktywności poszczególnych resortów oraz instytucji wchodzących w skład systemu bezpieczeństwa państwa w realizacji obowiązków związanych z zapobieganiem i zwalczaniem terroryzmu, ze szczególnym uwzględnieniem zadań przypisanych im w ramach Strategii CONTEST. Do szczegółowych zadań OSCT należy m. in.:

- ocena reagowania administracji państwowej na incydenty o charakterze terrorystycznym,
- wspieranie rozwoju legislacji antyterrorystycznej w kraju i poza jego granicami,
- zapewnianie społeczeństwu niezbędnych środków ochrony przed terroryzmem,
- zapewnianie odpowiedniego poziomu zabezpieczenia infrastruktury krytycznej państwa (z uwzględnieniem podatności na ataki z wykorzystaniem urządzeń teleinformatycznych),
- dbałość o przygotowanie administracji państwowej do skutecznego reagowania oraz odpowiedzi na ataki i incydenty terrorystyczne z wykorzystaniem broni masowego rażenia.

a) Policja Metropolitarna (ang. *Metropolitan Police Service/Scotland Yard/Met*) – w swojej strukturze posiada wysoce wyspecjalizowaną komórkę do walki z terroryzmem, w postaci Dowództwa Antyterrorystycznego (ang. *Counter Terrorism Command* – SO13/CTC)[10]. Do statutowych zadań *Scotland Yard* CTC należy m. in.:
- zbieranie i dystrybucja, w ramach posiadanej jurysdykcji, informacji na temat terroryzmu, ekstremizmu oraz innych przestępstw im towarzyszących,
- dostarczanie specjalistycznych porad z zakresu bezpieczeństwa publicznego w kraju i za granicą,
- udział w budowaniu społecznego zaufania oraz partnerskiej współpracy z mieszkańcami stolicy Wielkiej Brytanii,
- prowadzenie punktu kontaktowego dla międzynarodowej współpracy policyjnej w sprawach antyterrorystycznych (np. wymiana tzw. *best practices*);

b) Służba Bezpieczeństwa, zwana często MI5 (ang. *UK's Security Service*) to podległa Ministerstwu Spraw Wewnętrznych krajowa służba specjalna, której zadaniem jest ochrona bezpieczeństwa Zjednoczonego Królestwa przed zagrożeniami wewnętrznymi, stwarzanymi m. in. przez terroryzm. Sprawy dotyczące terroryzmu międzynarodowego w ramach MI5 prowadzi kierunkowa komórka organizacyjna o nazwie *International Counter Terrorism Branch*. Zaś terroryzmem nacjonalistyczno – separatystycznym występującym w Irlandii Północnej zajmuje się Northern *Ireland Counter Terrorism*.

c) Połączone Centrum Analiz Terroryzmu (*Joint Terrorism Analysis Centre* – JTAC) to ustanowiona w czerwcu 2003 r. przy MI5, multinstytucjonalna jednostka analityczna zajmująca się zakresem działań terroryzmu międzynarodowego[11], które stanowią bezpośrednie zagrożenie dla obywateli i interesów Wielkiej Brytanii, zarówno na jej obszarze, jak i poza granicami. JTAC zapewnia przekrojowe analizy i bieżące informacje niezbędne do wspieania procesu decyzyjnego

[10] Dowództwo Antyterrorystyczne Policji Metropolitarnej zostało utworzone 2 października 2006 r. z połączenia dwóch wewnętrznych specjalistycznych struktur *Scotland Yard* zajmujących się przestępstwami terrorystycznymi, czyli tzw. *Anti-Terrorist Branch oraz Special Branch*.

[11] Warto w tym miejscu zaznaczyć, iż Połączone Centrum Analiz Terroryzmu nie sporządza oceny poziomu zagrożenia terroryzmem wewnętrznym, powodowanego aktywnością irlandzkich separatystów oraz lojalistów. Kwestia ta wciąż leży w gestii kierunkowego departamentu MI5.

na każdym poziomie administracji państwowej, odpowiada również za określenie aktualnego poziomu zagrożenia w narodowym systemie wczesnego ostrzegania przed terroryzmem (tzw. *Threat levels: The system to assess the threat from international terrorism*). JTAC zatrudnia na stałe ponad 100 specjalistów z kilkunastu instytucji i ministerstw rządowych. Korzysta przy tym również z wiedzy naukowej niezależnych fachowców. Jednostka działa w trybie 24/7.

3. **Ministerstwo Obrony** (ang. *Ministry of Defence*) – odpowiada za prowadzenie prewencji oraz fizyczne zwalczanie zagrożeń o charakterze terrorystycznym (tzw. „wyprzedzające misje bojowe"), jak również wspiera w tym zakresie wysiłki sojusznicze.
   a) **Wojskowa Jednostka Specjalna SAS** (ang. *The Special Air Service*) – wykorzystywana do wykonywania działań kontrterrorystycznych w kraju oraz poza jego granicami. W celu zwiększenia skuteczności realizacji zadań taktycznych podejmowanych w Zjednoczonym Królestwie SAS wspomagany jest przez antyterrorystyczne pododdziały policji metropolitarnej. Decyzję o użyciu wojskowych sił specjalnych podejmuje premier Wielkiej Brytanii. Z kolei, całość akcji koordynowana jest na poziomie strategicznym w **COBR** przez ministra spraw wewnętrznych lub premiera Zjednoczonego Królestwa, w zależności od skali powstałego zagrożenia.
4. **Ministerstwo Spraw Zagranicznych** – (ang. *Foreign and Commonwealth Office*) odpowiada za ochronę interesów oraz obywateli Wielkiej Brytanii za granicą oraz koordynuje i promuje (m. in. poprzez prowadzenie szkoleń i wsparcie informacyjne dla krajów partnerskich) antyterrorystyczną współpracę międzynarodową[12]:
   a) **Służba Wywiadu, zwana często MI6** (ang. *Secret Intelligence Service* – SIS) – podległa Ministerstwu Spraw Zagranicznych służba wywiadu, pozyskująca niezbędne informacje w celu zapewnienia ochrony przebywającym poza krajem obywatelom Zjednoczonego Królestwa oraz zabezpieczająca zagraniczne interesy państwa, także na wypadek wystąpienia zagrożeń terrorystycznych.
5. **Ministerstwo Skarbu Państwa** – (ang. *Her Majesty's Treasury*) odpowiada za zapobieganie finansowania terroryzmu, wykorzystując w tym celu prawo do zamrażania aktywów pieniężnych wobec podmiotów podejrzanych o ten proceder. Prerogatywa ta stosowana jest przez ministerialny **Zespół ds. Zamrażania Środków Finansowych** (ang. *Asset Freezing Unit*). Z kolei, koordynacją działań podejmowanych przez Ministerstwo Skarbu Państwa w celu realizacji zadań przypisanych temu resortowi w ramach CONTEST zajmuje się **Grupa ds. Przestępstw Finansowych** (ang. *Financial Crime Team*).
6. **Ministerstwo Sprawiedliwości** – (ang. *Ministry of Justice* – MoJ)[13] podejmuje wszelkie niezbędne kroki, w celu zwiększenia efektywności, skuteczności i bezpieczeństwa systemu sprawiedliwości w sprawach o terroryzm oraz w postępowaniach dotyczących przemocy stosowanej przez radykalnych ekstremistów. W tym

---

[12] Za: Media Emergency Forum, *Joint glossary of official and media terms and acronyms*, August 2004; *NaCTSO Glossary* zob. w: http://nactso.gov.uk/glossary.php, 10.09.2009 r.; *National Intelligence Machinery*, The UK Stationery Office, 2006; http://www.cabinetoffice.gov.uk/government_communication, 09.09.2009 r.

[13] Ministerstwo Sprawiedliwości zostało wyodrębnione z MSW 9 maja 2007 r. jako nowy rządowy resort skupiający w swojej właściwości system sprawiedliwości, składający się z sądownictwa, więziennictwa i kurateli sądowej.

celu umiejscowiony w MoJ **Krajowy Urząd ds. Wykroczeń** (ang. *National Offender Management Service* – NOMS)[14], prowadzi bliską współpracę z policją i służbami specjalnymi.

7. **Centrum Łączności Rządowej** – (*Government Communication Headquarters* – GCHQ) jest służbą specjalną prowadzącą rozpoznanie elektroniczne w celu dostarczenia administracji państwowej informacji istotnych z punktu widzenie centralnego procesu decyzyjnego dotyczącego bezpieczeństwa narodowego, m. in., na polu walki z terroryzmem. GCHQ zabezpiecza również, pod kątem technicznym, integralność rządowego systemu komunikacji oraz informacji przed zagrożeniami zewnętrznymi.
8. **Stowarzyszenie Szefów Policji** – (ang. *Association of Chief Police Officers* – ACPO) koordynuje działania Policji z 43 służb (Anglii i Walii) w zakresie walki z terroryzmem i innymi zagrożeniami dla bezpieczeństwa obywateli. Współpracuje bezpośrednio z rządem, szczególnie w trakcie zaistniałych incydentów terrorystycznych oraz innych sytuacji nadzwyczajnych.
9. **Centrum Ochrony Infrastruktury Krytycznej** – (ang. *Centre for Protection of National Infrastructure* – CPNI) to międzyresortowa jednostka, wypracowująca kompleksowe porady i ekspertyzy dotyczące zasady ochrony narodowej infrastruktury krytycznej, w celu zredukowania jej podatności na zagrożenia terrorystyczne. Docelowymi odbiorcami produktów NSAC (wysokiej klasy usługi doradczo-analityczne, kursy specjalistyczne, informacje *on-line*, poradniki) są liczne organizacje, sektor publiczny oraz środowiska biznesu[15]:
   a. **Narodowy Urząd ds. Ochrony Antyterrorystycznej** (ang. *National Counter Terrorism Security Office* – NaCTSO) – jednostka policyjna działająca przy CPNI w imieniu ACPO(TAM)[16] oraz we współpracy z MI5 zajmująca się kwestią obniżenia poziomu oddziaływania terroryzmu na ciągłość funkcjonowania aparatu państwowego. Do jej statutowych zadań należy:
      - podnoszenie świadomości na temat zagrożeń terrorystycznych oraz środków służących przeciwdziałaniu i łagodzeniu skutków ataku,
      - kształtowanie i rozwój kierunku polityki antyterrorystycznej w ujęciu krajowym oraz międzynarodowym (w ramach filaru *Protect* i *Prepare* z CONTEST),
      - koordynacja prac, przygotowanie merytoryczne oraz nadzór nad aktywnością instytucji odpowiedzialnych za dystrybucję porad dotyczących ochrony przed terroryzmem, poprzez sieć krajowych **Doradców ds. Bezpieczeństwa Antyterrorystycznego** – (ang. *Counter Terrorism Security Advisers* CTSA[17]),

---

[14] NOMS został utworzony 1 czerwca 2004 r. i obecnie funkcjonuje jako departament Ministerstwa Sprawiedliwości z właściwością dla Anglii i Walii. Odpowiedniki niniejszego urzędu działają niezależnie w Szkocji i Irlandii Północnej.

[15] CPNI powstało 1 lutego 2007 r. z fuzji Narodowego Centrum Doradztwa ds. Bezpieczeństwa Służby Specjalnej MI5 (ang. *Security Service's National Security Advice Centre* – NSAC) oraz Centrum Koordynacji Bezpieczeństwa Infrastruktury Narodowej (ang. *National Infrastructure Security Co-ordination Centre* – NISCC).

[16] ACPO(TAM) (ang. *Association of Chief Police Officers for Terrorism and Allied Matters)* specjalna podgrupa w ramach Stowarzyszenia Szefów Policji zajmująca się problematyką terroryzmu i przestępstw z nim powiązanych.

[17] W skład *Counter Terrorism Security Advisers* wchodzą wysokiej klasy specjaliści z lokalnej policji. Nadrzędną rolą tej jednostki jest zapewnienie pomocy, porad oraz wskazówek szerokiej gamie podmiotów prywatnych i państwowych we wszystkich aspektach ochrony antyterrorystycznej.

- budowanie partnerskiej współpracy informacyjnej pomiędzy społeczeństwem, policją, a kluczowymi instytucjami administracji państwowej[18].

Inicjatywy służące rozwojowi sieci antyterrorystycznej oraz współpracy pomiędzy obywatelami i środowiskiem biznesu, a instytucjami państwowymi:

1. Narodowy system wczesnego ostrzegania przed terroryzmem (tzw. *The system to assess the threat from international terrorism*), w którym jeden z pięciu określonych poziomów zagrożenia (z ang. *Threat levels)* determinuje wprowadzenie jednego z trzech scenariuszy mechanizmów działania dla instytucji stanowiących narodowy system do walki z terroryzmem. Nowy, uproszczony system wczesnego ostrzegania przed zagrożeniami o charakterze terrorystycznym, został uruchomiony 1 sierpnia 2006 r. Instytucją odpowiedzialną za dokonywanie zmian poszczególnych stopni systemu jest JTAC. Informacje na temat aktualnego poziomu zagrożenia są dostępne na bieżąco, m. in., *on-line* na stronach *Home Office* lub MI5[19].
   Pięć poziomów zagrożenia przeprowadzenia ataku terrorystycznego to:
   I. Poziom **„Niski"** (ang. *Low*) – atak jest wątpliwy;
   II. Poziom **„Umiarkowany"** (ang. *Moderate*) – atak jest możliwy, ale mało prawdopodobny;
   III. Poziom **„Poważny"** (ang. *Substantial*) – atak ma wysokie prawdopodobieństwo;
   IV. Poziom **„Ciężki"** (ang. *Severe*) – atak jest bardzo możliwy;
   V. Poziom **„Krytyczny"** (ang. *Critical*) – atak jest oczekiwany w niedalekim czasie.
2. Pakiet informacji dotyczących ryzyka wystąpienia zagrożeń dla bezpieczeństwa osobistego w trakcie podróży zagranicznej na danym obszarze geograficznym (ang. *The Risk of Terrorism when Travelling Overseas*)**,** udostępniany jest za pośrednictwem ministerstwa odpowiedzialnego za politykę zagraniczną (*Foreign and Commonwealth Office*) i we współpracy z JTAC.
3. Bezpłatna i całodobowa linia telefoniczna rejestrująca informacje dotyczące terroryzmu (ang. *Anti-Terrorist Hotline 0800-789321*), uruchomiona została w celu umożliwienia anonimowego zgłaszania nietypowych lub podejrzanych zachowań, zaobserwowanych przez obywateli w swoim najbliższym otoczeniu (inicjatywa: *Home Office* i *Metropolitan Police*)[20].

---

[18] Za: Media Emergency Forum, *Joint glossary of official and media terms and acronyms*, August 2004; http://www.nactso.gov.uk/missionstatement.php, 21.09.2009; *NaCTSO Glossary* zob. w: http://nactso.gov.uk/glossary.php, 20.09.2009 r.; *National Intelligence Machinery*, The UK Stationery Office, 2006; http://www.met.police.uk/so/counter_terrorism, 21.09.2009; http://www.ukresilience.info/nscwip.aspx, 21.09.2009 r.

[19] Za: UK Government Home Office*, Threat levels: The system to assess the threat from international terrorism,* Stationery Office, July 2006.

[20] Wspomniana linia telefoniczna była promowana w mediach, m. in. pod hasłami: „Terroryzm: Jeśli coś podejrzewasz, zgłoś to" – (ang. *Terrorism: If you suspect it report it*) oraz „Ratujący życie" – (ang. *Life Savers*). Za: P. Piasecka, K. Liedel, *Government and society partnership in terrorism combating* w: S. Wojciechowski (red.), *The modern terrorism and its forms*, Wydaw. Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Adama Mickiewicza, Poznań 2007, s. 31; K. Liedel, P. Piasecka, *Jak przetrwać w dobie zagrożeń terrorystycznych – elementy edukacji antyterrorystycznej,* Wydaw. Trio i Collegium Civitas, Warszawa 2008, s. 51-54.

4. Porady i zalecenia z zakresu bezpieczeństwa antyterrorystycznego w strefach zatłoczonych, miejscach pracy, budynkach mieszkalnych dostarczane przez rozbudowaną ogólnokrajową sieć policyjnych doradców ds. przeciwdziałania terroryzmowi (*Counter Terrorism Security Advisers – CTSA*) na potrzeby sektora prywatnego**;**
5. Inicjatywa *Community Safe* – prowadzony przez policję oraz administrację lokalną centralny punkt wczesnego ostrzegania, zaopatrujący za pomocą łączności elektronicznej, (telefony komórkowe, pagery, poczta e-mail), obywateli zarejestrowanych dobrowolnie na danym obszarze, w aktualne i oficjalne dane oraz zalecenia, m. in., na wypadek zaistnienia zdarzenia o charakterze terrorystycznym (tzw. system *real-time*).
6. Specjalistyczne poradniki skierowane zarówno do poszczególnych obywateli, jak i środowisk biznesu, np:
   a) *Protecting against Terrorism* – szczegółowy, nowoczesny poradnik na temat zasad ochrony przed terroryzmem, opublikowany przez brytyjską służbę specjalną MI5 (na bazie międzyresortowej współpracy z kierunkowymi instytucjami państwowymi (ang. *Cabinet Office, Home Office, ACPO*). Poradnik porusza m. in. następujące zagadnienia:
      - sposoby tworzenia, rozwijania i udoskonalania zasad bezpieczeństwa w miejscu pracy,
      - środki ochrony bezpieczeństwa - od obiektów fizycznych, poprzez wrażliwe dane informatyczne (podatne na przestępstwa popełniane przy użyciu sieci informatycznych), po właściwy dobór personelu,
      - metody rozpoznawania oraz zapobiegania atakom terrorystycznym z użyciem ładunków wybuchowych, środków chemicznych, biologicznych lub radioaktywnych,
      - zasady przeszukiwania oraz ewakuacji z pomieszczeń na wypadek zaistnienia sytuacji kryzysowych w miejscu pracy.
   b) *Preparing for Emergencies* – modelowy poradnik, stworzony w ramach szerszej społecznej kampanii *Home Office* mającej na celu propagowanie przystępnej wiedzy z zakresu metod zapobiegania sytuacjom kryzysowym oraz sposobów radzenia sobie z ich skutkami, m.in. pod kątem zagrożeń o charakterze terrorystycznym, z wykorzystaniem materiałów pirotechnicznych, chemicznych, biologicznych lub radioaktywnych[21)];
   c) Pakiet czterech kompleksowych poradników dotyczących bezpieczeństwa na wypadek zaistnienia zagrożeń o charakterze terrorystycznym (ang. *Counter Terrorism Protective - Security Advice*) [22)] w dużych skupiskach publicznych (I – stadiony i obiekty sportowe, II – puby i dyskoteki, III – centra handlowe,

[21)] Kampania społeczna pod tytułem: *Przygotowanie na sytuacje nadzwyczajne – co musisz wiedzieć* (ang. *Preparing for Emergencies - what you need to know*) prowadzona jest przez *Home Office* na wielu szczeblach administracji państwowej za pośrednictwem sieci inicjatyw o zasięgu regionalnym i lokalnym (jak np. promowanie systemu: *Go in*, *Stay in*, *Tune in)*. Jeden z jej istotnych elementów stanowi projekt pt. *Planowanie Ciągłości Działania w Biznesie* (ang. *Business Continuity Management* – BCM), którego zadanie polega na przygotowaniu sektora prywatnego do ograniczenia lub całkowitego wyeliminowania negatywnych skutków zdarzeń kryzysowych, w tym zamachów terrorystycznych, dla prowadzonej działalności gospodarczej. Więcej na ten temat w podręczniku sygnowanym przez *Home Office* pt. *Jak jesteś przygotowany – Narzędzia Planowania Ciągłości Działania w Biznesie* (ang. *How prepared are you - Business Continuity Management Toolkit*).

[22)] Za: http//:www.nactso.gov.uk/crowdedplaces.php, 21.09.2008 r.

IV – atrakcje dla zwiedzających), przygotowany przez NaCTSO we współpracy ze środowiskami biznesu oraz pod egidą *Home Office,* CPNI, ACPO(TAM) oraz MI5.

Podsumowanie

Wielka Brytania wypracowała dotychczas jeden z najbardziej skutecznych na świecie systemów walki z terroryzmem, który został wpisany w IV priorytety aktywności państwowej, tj.: zapobieganie czynnikom oraz źródłom powstawania terroryzmu, ściganie terrorystów oraz ich aktywnych sympatyków; ochronę obywateli oraz obiektów użyteczności publicznej, należących do narodowej infrastruktury krytycznej przed skutkami ataków terrorystycznych; budowanie zdolności reagowania kryzysowego oraz likwidacji skutków zamachów terrorystycznych. System ten stanowi kompilację rozbudowanego mechanizmu koordynacji międzyinstytucjonalnej oraz adekwatnej do skali zagrożenia legislacji. Wszystkie narodowe mechanizmy antyterrorystyczne poddawane są regularnej ocenie, a w konsekwencji stale aktualizowane i udoskonalane w oparciu o wnioski z przeprowadzanych ćwiczeń oraz analiz trendów współczesnego terroryzmu. Zaawansowana forma tej multilateralnej antyterrorystycznej kooperacji okazuje się kluczową dla ograniczenia efektów działania, bądź całkowitego wyeliminowania poszczególnych elementów terrorystycznej sieci zagrażającej interesom oraz obywatelom Wielkiej Brytanii.

Bibliografia:

1. Aleksandrowicz T., *Terroryzm międzynarodowy*, Wydawnictwo Akademickie i Profesjonalne, Warszawa 2008.
2. Borkowski R., *Terroryzm ponowoczesny*, Wydawnictwo Adam Marszałek, Toruń 2006.
3. CONTEST - *the United Kingdom's Strategy for Countering International Terrorism 2009.*
4. *Encyklopedia PWN – Fakty i Liczby*, Warszawa 2006.
5. Hołyst. B., *Encyklopedia Terroryzmu*, Tom I i II, Lexis Nexis, Warszawa 2009.
6. Kowalczyk K., Wróblewski W., *Terroryzm – globalne wyzwanie*, Adam Marszałek, Toruń 2006.
7. *How prepared are you - Business Continuity Management Toolkit* – UK Home Office.
8. Jałoszyński K., *Współczesny wymiar antyterroryzmu*, Wydawnictwo Trio, Warszawa 2008.
9. *Joint glossary of official and media terms and acronyms*, Media Emergency Forum, August 2004.
10. Laqueur W., *Postmodern*, „Foreign Affairs" nr 5, 1996.
11. Liedel K., *Terroryzm – Anatomia Zjawiska*, Wydawnictwo Naukowe Scholar i Collegium Civitas Press, Warszawa 2006.
12. Liedel K., Piasecka P., *Jak przetrwać w dobie zagrożeń terrorystycznych – elementy edukacji antyterrorystycznej,* Wydawnictwo Trio i Collegium Civitas, Warszawa 2008.
13. Malinowski M. J., Ożarowski R., Grabowski W., *Ewolucja terroryzmu na przełomie XX i XXI wieku,* Wydawnictwo Uniwersytetu Gdańskiego, Gdańsk 2009.
14. *National Intelligence Machinery*, The UK Stationery Office, 2006.

15. Polko R., *Grom w działaniach przeciwterrorystycznych*, Biblioteka „Bezpieczeństwa Narodowego" t. VI, Warszawa 2008.
16. Szafrański J., Kosiński J., *Współczesne zagrożenia terrorystyczne oraz metody ich zwalczania*, Wydaw. Wyższej Szkoły Policji, Szczytno 2007.
17. *Threat levels: The system to assess the threat from international terrorism,* Stationery Office, UK Government Home Office.
18. Wojciechowski S., *The modern terrorism and its forms*, Wydawnictwo Instytutu Nauk Politycznych i Dziennikarstwa Uniwersytetu Adama Mickiewicza, Poznań 2007.
19. Zeszyt Biura Bezpieczeństwa Narodowego, *Przeciwdziałanie terroryzmowi*, nr 2, Warszawa 2008 r. – materiały z konferencji zorganizowanej przez Biura Bezpieczeństwa Narodowego 27 listopada 2007.
20. Czasopismo „Terroryzm" – z lat 2007-2009.
21. Portale internetowe:
http://www.acpo.police.uk/about.html/,
http://www.cabinetoffice.gov.uk/,
http://www.justice.gov.uk/,
http://www.met.police.uk/so/counter_terrorism/,
http://www.londonprepared.gov.uk/,
http://nactso.gov.uk/glossary.php/,
http://www.preparingforemergencies.gov.uk/,
http://www.ukresilience.info/.

ABSTRACT

The present paper aims at presenting the British counterterrorism system considered as one of the most effective systems in the world. It was build on the basis of three decades of the UK experiences related to:

- counteracting the factors and sources of terrorism;
- investigating terrorist activities, as well as their active supporters;
- protecting citizens and public utility installations being part of the national critical infrastructure against the consequences of terrorist attacks;
- building capacities of crisis management and eliminating the consequences of terrorist attacks.

The paper concentrates on obligations and tasks imposed on a number of competent national authorities, namely:

- the United Kingdom Cabinet Office (Cabinet Office Briefing Room);
- Metropolitan Police Service - Counter Terrorism Command - SO13/CTC, UK's Security Service - Joint Terrorism Analysis Centre - JTAC);
- Ministry of Defence (The Special Air Service);
- Foreign and Commonwealth Office (Secret Intelligence Service – SIS);
- Her Majesty's Treasury;
- Ministry of Justice;
- Government Communication Headquarters;
- Centre for Protection of National Infrastructure;

as well as on the mechanisms of their interinstitutional cooperation and the provisions of the legislation applicable in the United Kingdom at present. The paper refers also to initiatives aimed at developing counterterrorist networks, as well as cooperation between citizens, businesses and public administration institutions.

Katarzyna Laskowska

Współczesne zagrożenia bezpieczeństwa Rosji w ujęciu kryminologicznym

Przez kilka dziesięcioleci obywatele ZSRR żyli w kraju, który był potęgą pod względem militarnym, politycznym, terytorialnym i demograficznym. Owa sytuacja zmieniła się wraz z rozpadem Związku Radzieckiego, w rezultacie czego powstały samodzielne, niezależne państwa, a wśród nich i Rosja. Obecnie kraj ten, po przejściach w znaczeniu gospodarczym, politycznym i społecznym, wprawdzie pretenduje do miana mocarstwa, ale z różnych przyczyn nie może nim być. Powodem tego jest, między innymi, wiele zagrożeń uniemożliwiających spokojne, bezpieczne i dostatnie funkcjonowanie państwa rosyjskiego.

Celem niniejszego opracowania jest ukazanie tych zagrożeń w aspekcie kryminologicznym. W związku z tak zakreślonym problemem, istotne wydaje się udzielenie odpowiedzi na następujące pytania:

- jakie zagrożenia dla bezpieczeństwa państwa występują we współczesnej Rosji?
- jakie są ich przyczyny?
- jakie instrumenty stosuje państwo w celu ograniczania lub eliminowania tych zagrożeń?

Podstawą rozważań będą akty prawne i inne dokumenty dotyczące omawianej problematyki, a także opracowania wyników badań kryminologicznych prowadzonych w tym zakresie przez rosyjskich kryminologów, w tym wywiad z czołowym kryminologiem rosyjskim, J. I. Gilinskim[1)].

1. Podstawowe zagadnienia dotyczące bezpieczeństwa Rosji

Przystępując do rozważań należy sprecyzować pojęcie „bezpieczeństwo". Określa je *Ustawa o bezpieczeństwie* z 1992 r.[2)] W świetle art. 1 „bezpieczeństwo" jest to *stan obrony życiowo ważnych interesów jednostki, społeczeństwa i państwa przed zagrożeniami wewnętrznymi i zewnętrznymi*. Przez „życiowo ważne interesy" należy rozumieć całokształt potrzeb, których zaspokojenie w wystarczającym stopniu zabezpiecza funkcjonowanie i możliwości progresywnego rozwoju jednostki, społeczeństwa i państwa" (art. 1), a „zagrożenia bezpieczeństwa" to *całokształt warunków i czynników stwarzających niebezpieczeństwo dla życiowo ważnych interesów jednostki, społeczeństwa i państwa* (art. 3).

W świetle art. 2 tej ustawy podmiotami zobowiązanymi do zapewnienia bezpieczeństwa na terytorium Federacji Rosyjskiej (FR) są głównie państwo i obywatele. Zapewnienie to ma być realizowane na zasadzie praworządności, zachowania równowagi między ważnymi życiowo interesami jednostki, społeczeństwa i państwa, a także wzajemnej odpowiedzialności tych podmiotów oraz integracji z międzynarodowymi systemami bezpieczeństwa (art. 5). Podstawy prawne dotyczące kwestii zapewnienia

---

[1)] Prof. J.I. Gilinskij jest pracownikiem Rosyjskiej Akademii Nauk i Akademii Prokuratury Generalnej w Sankt-Petersburgu.

[2)] Zakon o biezopasnosti z dnia 25.12.1992 r., N 3235-1(w redakcji z dnia 02.03.2007 r., N 24-FZ), http://www.internet-law.ru/law/inflaw/sec.htm.

bezpieczeństwa stanowią: Konstytucja FR, ustawa *O bezpieczeństwie* z 1992 r., inne ustawy regulujące stosunki w dziedzinie bezpieczeństwa oraz umowy międzynarodowe ratyfikowane przez Rosję (art. 6).

W celu zagwarantowania bezpieczeństwa państwa i obywateli stworzono system bezpieczeństwa Federacji Rosyjskiej, którego głównym elementem, w świetle art. 8, ustanowiono organy władzy ustawodawczej, wykonawczej i sądowniczej oraz organizacje i instytucje państwowe i społeczne, a także obywateli. Przyjęto, że główne zadania tego systemu to: ujawnianie i prognozowanie zagrożeń wewnętrznych i zewnętrznych, a także utrzymywanie w gotowości sił i środków do zapewnienia bezpieczeństwa, zarządzanie nimi w sytuacjach powszechnych i nadzwyczajnych (art. 9). Owe środki i siły, na podstawie art. 12, zagwarantowane są w szczególności przez: Siły Zbrojne, federalne organa bezpieczeństwa, organa spraw wewnętrznych i wywiadu wewnętrznego, Państwową Służbę Przeciwpożarową, organa służby likwidacji skutków następstw sytuacji nadzwyczajnych, formacje obrony cywilnej, wojska wewnętrzne, służby z zakresu energetyki, transportu, telekomunikacji, służby celne, ochrony przyrody i zdrowia.

W Rosji konstytucyjnym organem przygotowującym dla Prezydenta Federacji Rosyjskiej akty prawne dotyczące bezpieczeństwa jest Rada Bezpieczeństwa. Jej status, zadania i tryb wydawania decyzji określiła ustawa w szczególności w art. 13-19.

Zatem, jak wynika z powyższych informacji, podstawowe kwestie dotyczące bezpieczeństwa Rosji reguluje ustawa *O bezpieczeństwie*. Jest ona zbiorem przepisów o charakterze organizacyjnym i porządkowym. Ma też charakter kompetencyjny, gdyż zawiera prawne podstawy funkcjonowania szeroko pojętego systemu bezpieczeństwa w Rosji. Ustawa ta nie wskazuje konkretnych zagrożeń dla tego kraju.

Pojęcie bezpieczeństwa określa też *Koncepcja narodowego bezpieczeństwa Federacji Rosyjskiej* z 1997 r.[3)] (zwana dalej *Koncepcją*). Posługuje się ona pojęciem „narodowe bezpieczeństwo Federacji Rosyjskiej", pod którym rozumie *bezpieczeństwo jej wielonarodowościowego narodu jako nosiciela suwerenności i jedynego źródła władzy w Federacji Rosyjskiej*. Należy uznać, że pojęcie „bezpieczeństwa" z ustawy *O bezpieczeństwie* ma szerszy zakres niż określenie „bezpieczeństwa narodowego" zawartego w *Koncepcji*.

2. Diagnoza i etiologia zagrożeń bezpieczeństwa państwa rosyjskiego

Diagnoza zagrożeń bezpieczeństwa państwa rosyjskiego zostanie dokonana w oparciu o wymienioną *Koncepcję* i wyniki badań kryminologicznych.

W *Koncepcj*i dokonano podziału zagrożeń na wewnętrzne i międzynarodowe. Jako zagrożenia wewnętrzne w wskazano w niej:

- stan gospodarki państwa, charakteryzujący się w szczególności obniżaniem się PKB, niewielką liczbą inwestycji, wzrostem długu państwowego, osłabieniem systemu finansowo-bankowego, spadkiem produkcji,
- obniżenie potencjału naukowo-technicznego i technologicznego kraju,
- socjalne zróżnicowanie społeczeństwa, upadek jego wartości moralnych,

[3)] *Koncepcija nacjonalnoj biezopasnosti Rossijskoj Federaciji* z 17 XII 1997 r., (przyjęta Dekretem Prezydenta FR Nr 1300), *Sobranije zakonodatielstwa RF* 2000, Nr 2, art. 170.

- etnocentryzm, szowinizm oraz religijny ekstremizm, a także niekontrolowaną migrację, która sprzyja narastaniu konfliktów społecznych i politycznych,
- wzrost przestępczości zorganizowanej i korupcji, których rozwojowi sprzyja kryminalizacja społeczeństwa, słaba kontrola państwa, brak odpowiedniej bazy prawnej i polityki państwa w tym zakresie. Wzrost ten następuje wskutek zmian w strukturze własności w Rosji, zaostrzenia się walki o władzę na bazie interesów grupowych i nacjonalistycznych, niedostatecznego zabezpieczenia materialno-technicznego, fluktuacji kadr organów zajmujących się ochroną bezpieczeństwa oraz w skutek nihilizmu prawnego,
- podział społeczeństwa na bogatych i biednych, słabe zabezpieczenie społeczne obywateli, znaczny procent ludzi biednych w społeczeństwie, wzrost bezrobocia,
- zagrożenia dla zdrowia fizycznego, kryzys służby zdrowia i socjalnej ochrony społeczeństwa, wzrost spożycia alkoholu i narkotyków, spadek narodzin, skrócenie długości życia obywateli, deformacja demograficznego systemu społeczeństwa, upadek rodziny, spadek potencjału duchowego, moralnego i twórczego społeczeństwa.

Za zagrożenia o charakterze międzynarodowym uznano:

- narzucanie przez inne państwa i organy międzynarodowe swoich mechanizmów gwarancji bezpieczeństwa międzynarodowego,
- osłabienie politycznych, gospodarczych i wojskowych wpływów Rosji wobec rozszerzania się NATO na wschód,
- możliwość umieszczania przez inne państwa baz wojskowych i wojsk w pobliżu granic z Rosją,
- rozprzestrzenianie się broni masowego rażenia,
- osłabienie procesów integracyjnych w ramach Wspólnoty Niepodległych Państw (WNP),
- narastanie konfliktów wokół granic państw WNP,
- terroryzm, w tym o charakterze międzynarodowym, który może doprowadzić do destabilizacji sytuacji w Rosji,
- dążenie innych państw do dominacji w światowej przestrzeni informacyjnej, pozbycie się Rosji z rynku informacyjnego, dążenie do uzyskania dostępu do sieci systemów telekomunikacyjnych Rosji,
- dążenie niektórych państw do stworzenia nowej techniki wojskowej, sprzyjającej nowemu etapowi wyścigu zbrojeń,
- aktywizację działalności zagranicznych służb specjalnych na obszarze Rosji,
- niedostateczne finansowanie systemu obronności wobec wyżej wymienionych zagrożeń, nieodpowiednia baza prawna w tym zakresie, niski poziom przygotowania Sił Zbrojnych i innych jednostek odpowiedzialnych za bezpieczeństwo Rosji,
- ekspansję gospodarczą, demograficzną i kulturowo-religijną obywateli innych państw na terytorium FR,
- wzrost aktywności transgranicznej przestępczości zorganizowanej i zagranicznych organizacji terrorystycznych,
- niską kulturę ekologiczną, niekontrolowany rozwój paliwowo-energetycznych gałęzi przemysłu, brak przepisów prawnych skutecznie chroniących ekologię, wykorzystywanie Rosji jako miejsca przerobu niebezpiecznych materiałów i środków, co może doprowadzić do katastrofy o charakterze ekologicznym.

W *Koncepcji* wskazano zatem na zagrożenia o charakterze gospodarczym, społecznym, kryminalnym, politycznym, duchowym, moralnym, organizacyjnym, prawnym, zdrowotnym, ekologicznym, wojskowym, socjalnym i demograficznym. Stanowią one szerokie spektrum niebezpieczeństw. Mają różny wymiar, skierowane są wobec

różnych kategorii dóbr i mają różny ciężar gatunkowy. Jednakże, jedno co je łączy, to naruszanie poczucia bezpieczeństwa państwa, społeczeństwa i obywateli. Jako zagrożenia o charakterze kryminalnym wymieniono w *Koncepcji* głównie przestępczość zorganizowaną, korupcję i terroryzm.

Występowanie analogicznych zagrożeń w rzeczywistości ustalono na podstawie analizy literatury kryminologicznej, w tym opracowań wyników wielu badań prowadzonych w Rosji w tym zakresie. Zostaną one krótko scharakteryzowane.

A. Zagrożenia wynikające z przestępczości zorganizowanej

Poprzez przenikanie w sferę działalności gospodarczej przestępczość zorganizowana wpływa na kształtowanie kierunków reform. W ten sposób następuje kryminalizacja gospodarki, przejawiająca się w dążeniu do ustanowienia kontroli nad jej strategicznymi gałęziami lub przejęcia niektórych dochodowych przedsiębiorstw. Powoduje to poważne straty w dziedzinie obrotu surowcami, metalami kolorowymi i nośnikami energii. W ramach zorganizowanej działalności następuje dokonywanie wielu nielegalnych transakcji, na których tracą jednostki i państwo[4)]. Narusza to bezpieczeństwo obrotu gospodarczego[5)] poprzez przejmowanie przez struktury przestępcze majątku państwowego i społecznego.[6)] Powodowane są poważne straty materialne dla państwa i społeczeństwa, poprzez zrastanie się struktur przestępczych z legalnym biznesem i gospodarką państwa.[7)]

W niektórych regionach Rosji przestępczość zorganizowana sprzyja nawiązywaniu współpracy liderów grup przestępczych z przywódcami klanów, dążących do realizacji własnych interesów politycznych; dąży do nawiązywania i rozwoju korupcyjnych powiązań z przedstawicielami różnych szczebli władzy oraz do udziału w życiu politycznym.[8)]

Przestępczość zorganizowana sprzyja rozwojowi narkomanii, dostarczając na rosyjski rynek środki odurzające, powodując wzrost uzależnienia od nich i wzrost przestępstw narkotykowych oraz rozwój międzynarodowych struktur zajmujących się narkobiznesem. Powoduje również internacjonalizację przestępczości[9)], narusza autorytet Rosji poprzez udział w międzynarodowej zorganizowanej działalności, wpływa na dyskredytację Rosji jako kraju mafijnego[10)]. Przestępczość zorganizowana wciąga w orbitę swej działalności dużą liczbę osób[11)], wpływa na upadek systemu wartości duchowych społeczeństwa, ukazuje „piękne, lekkie życie", kultywuje przemoc, stymuluje i aktywizuje elementy przestępcze, jednoczy je do nielegalnych celów[12)], sprzyja tworzeniu ideologii świata przestępczego, szczególnie widocznej na początku lat 90.[13)]

---

4) Szeroko na ten temat: J.A. Mochow, *FSB: borba s organizowannoj priestupnostju*, Moskwa 2006, s. 33-41.
5) N.F. Kuzniecowa, W.W.Łuniejew, *Kriminołogija*, Moskwa 2004, s. 400.
6) W.S. Owczinskij, W.J. Eminow, N.P. Jabłokow (red.), *Osnowy borby s organizowannoj priestupnostju,* Moskwa 1996, s. 131.
7) A.W. Gyske, *Sowriemiennaja rossijskaja priestupnost' i probliemy biezopasnosti obszcziestwa. Politiczieskij analiz*, Moskwa 2000, s.84-85.
8) J.A. Mochow, op. cit., s. 34, 36-37.
9) A.W. Gyske, op. cit., s. 85.
10) J.A. Mochow, op. cit., s. 33.
11) A.W. Gyske, op. cit., s. 85.
12) N.F. Kuzniecowa, W.W. Łuniejew, op. cit., s. 401.
13) W.S. Owczinskij, W.J. Eminow, N.P. Jabłokow (red.), op. cit., s. 131.

Walki między grupami o strefy wpływów powodują spadek poczucia bezpieczeństwa.[14] Zagrożone są w ten sposób swobody i wolności obywatelskie[15].

Należy podkreślić też wyrządzenie szkód przez przestępczość zorganizowaną w systemie politycznym i gospodarczym poprzez dezorganizację i niszczenie przy pomocy korupcji organów władzy. Tego typu działalność kształtuje negatywny stosunek społeczeństwa do władzy.[16] Szczególnie demoralizujące jest tworzenie przez funkcjonariuszy organów państwowych systemu ochrony dla struktur przestępczych[17]. Przestępczość zorganizowana wykazuje powiązania nie tylko z korupcją, ale i terroryzmem.

Na zagrożenia wynikające z przestępczości zorganizowanej wskazuje również J.I. Gilinskij[18]. Uważa on, że *W tej dziedzinie przestępczości zaszły w ostatnich latach zmiany. Przestępczość z lat 90., w której młodzi ludzie „kryszowali"*[19] *sklepy, restauracje czyli prowadzili działalność przestępczą typu gangsterskiego, przeszła ewolucję. Dzisiaj część prywatnego małego i średniego biznesu „kryszują" przedstawiciele milicji, co zresztą sami potwierdzają. Zepchnęli oni w ten sposób, zmusili do odwrotu, drobną przestępczość zorganizowaną. Liderzy grup przestępczych weszli już do gospodarki lub polityki lub w oba miejsca naraz. I dlatego dawni przywódcy nielegalnych struktur są dziś urzędnikami, deputowanymi, ich asystentami, merami miast, gubernatorami, biznesmenami. Szczególnie jest to widoczne na południowym wschodzie Rosji. Oczywiście, drobne grupy nadal istnieją. Np. w Sankt – Petersburgu, na bazarach owocowo-warzywnych, „kryszują" Azerowie, a ich „kryszuje" milicja. Z wywiadów przeprowadzonych z nimi wynika, że każdy nowy handlowiec, który chce prowadzić sprzedaż na rynku musi opłacić taką możliwość przedstawicielowi owej grupy. Po przyjeździe powinien się do niego zgłosić i uiścić opłatę. Jeśli strony nie porozumieją się, to wówczas wkracza milicjant, który jako następny negocjuje stawkę. Warto podkreślić, że między organami ochrony porządku publicznego dochodzi do konkurencji. Np. w Sankt – Petersburgu seksbiznes „kryszuje" milicja, ale są również agencje działające pod przykrywką Federalnej Służby Bezpieczeństwa (FSB). To już jest wyższy poziom „kryszy". Podobnie jest z narkotykami i hazardem, czyli większy biznes „kryszuje" FSB, mniejszy – milicja.*

Z informacji uzyskanych z wywiadu wynika, że przestępczość typu bandyckiego, gangsterskiego w Rosji odchodzi w przeszłość. Przestępcy przechodzą na wyższy poziom nielegalnej działalności, ingerując lub przejmując władzę w biznesie lub polityce. A udział w tej kategorii przestepczości funkcjonariuszy państwowych świadczy o mafijnym jej charakterze oraz o bezradności władzy wobec tego zjawiska.

---

[14] J.A. Mochow, op. cit., s. 44.

[15] W.S. Owczinskij, W.J. Eminow, N.P. Jabłokow (red.), op. cit., s. 130.

[16] N.F. Kuzniecowa, W.W. Łuniejew, op. cit., s. 399-400.

[17] W.S. Owczinskij, W.J. Eminow, N.P. Jabłokow (red.), op. cit., s. 132.

[18] Informacje pochodzą z wywiadu z profesorem J.I. Gilinskim, który został przeprowadzony w dniu 13.05 2009r. podczas jego pobytu na Wydziale Prawa Uniwersytetu w Białymstoku na potrzeby realizacji zadania badawczego realizowanego w ramach projektu Nr PBZ - MNiSW- DBO-01/I/2007 pt.: *Monitoring, identyfikacja i przeciwdziałanie zagrożeniom bezpieczeństwa obywateli* kierowanego przez Prof. zw. dr. hab. Emila W. Pływaczewskiego.

[19] „Kryszować" oznacza w języku rosyjskim „ochraniać". Słowo użyte w tekście w cudzysłowie wskazuje na ochronę przestępczą, czyli nielegalną eksploatację, pobieranie haraczu od podmiotów „ochranianych".

B. Zagrożenia wynikające z korupcji

Współcześnie *korupcja w Rosji stała się normą, a nie wyjątkiem, przede wszystkim wśród elity politycznej, rządzącej i gospodarczej*[20]. Rozwija się ona, zatem, wśród urzędników wszystkich szczebli najważniejszych instytucji w państwie (milicji, partii politycznych, parlamentu i sądów, organów celnych i oświatowych, organów podatkowych i prasy oraz służby zdrowia i resortów wojskowych, służb migracyjnych, komunalnych, organizacji religijnych).[21] Jej obecny stan, skala, formy i przejawy różnią się znacznie od poprzednio występujących w historii Rosji[22]. Obecnie korupcja przybiera zawoalowane formy (np. lobbing i protekcjonizm[23]), a wysoka wartość i duża skala wręczanych łapówek[24] dla polityków i urzędników rządowych kształtuje negatywny obraz władzy nie tylko w Rosji, ale i w świadomości społeczności międzynarodowej.[25] Korupcja podważa wiarygodność Rosji w oczach partnerów biznesowych, odstrasza inwestorów, prowadzi do rozwoju „szarej" gospodarki, naruszenia mechanizmów rynkowych[26]; narusza zasady wolności, równości i sprawiedliwości w społeczeństwie[27], wywiera negatywny wpływ na gospodarkę państwa[28]. Wykazuje także powiązania z przestępczością zorganizowaną.[29]

Według J. I. Gilinskiego, właśnie korupcja, jak to określił, *„totalna korupcja", jest najpoważniejszym zagrożeniem we współczesnej Rosji. Jest ona zagrożeniem numer jeden. Jej zakres obecnie jest ogromny, należy bowiem płacić wysokie łapówki za przyjęcie do przedszkola, dobrej szkoły, uczelni, za leczenie w dobrym szpitalu, u dobrego lekarza, inspektorom GAI na drogach itd. Powoduje to, że trudno jest żyć w Rosji bez pieniędzy. Bardzo poważny problem stanowi korupcja na najwyższych szczeblach władzy. Potwierdzają to wyniki badań prowadzonych przez niezależną fundację Satarowa – INDEM. W domu zgromadziłem duże ilości wycinków z gazet, w których podawane są konkretne ceny za konkretne usługi, tzn., ile trzeba dać, by zostać deputowanym, jego asystentem, ile kosztuje umorzenie sprawy w prokuraturze, ile war-*

---

[20] W.W. Łuniejew, *Priestupnost' XX wieka. Mirowyje, riegionalnyje i rossijskije tiendienciji*, Moskwa 2005, s. 523.

[21] Zob. N.F. Kuzniecowa, *Korrupcija i wziatocznicziestwo,* w: N.F. Kuzniecowa (red.), Kriminołogija, Moskwa 2006, s. 166.

[22] O.W. Łupaina, *Korrupcija w sistemie gosudarstwiennoj służby – ugroza nacjonal'noj biezopasnosti i cełostnosti Rossiji*, Sliedowatiel' 2008, nr 3, s. 42

[23] A.W. Gyske, op. cit., s. 136.

[24] Zob. N.F. Kuzniecowa, *Korrupcija i wziatocznicziestwo...,* s. 165.; W.D. Małkow (red.), *Kriminołogija*, Moskwa 2004, s. 327.; W.W. Kolesnikow, W.N. Bykow, O.A. Borisow, *Korrupcija kak ugroza nacjonal'noj biezopasnosti: o spiecifikie kriminołogiczieskowo podchoda*, „Kriminołogiczieskij Żurnał Bajkalskowo Gosudarstwiennowo Uniwiersitieta Ekonomiki i Prawa" 2007, nr 3-4, s. 51.

[25] G. Miszin, *Nieobchodim zakon o borbie s korrupcijej w wysszich eszełonach własti*. *Ugołownoje Prawo* 2002, nr 2, s. 132.; B.W. Wołżenkin, *Korrupcija w Rossiji,* w: W.N. Burłakow**,** W.P. Salnikow (red.)**,** *Kriminołogija XX wiek*, Sankt Petersburg 2000, s. 364.

[26] J.W. Golik, W.I. Karasiew, *Korrupcija kak miechanizm socjal'noj degradaciji,* Sankt Petersburg 2005, s. 248.

[27] W.W. Kolesnikow, W.N. Bykow, O.A. Borisow, op. cit., s. 55.

[28] A.G. Chabibulin, *Korrupcija kak ugroza nacjonalnoj biezopasnosti: mietodołogija, problemy i puti ich rieszienija*, „Żunał rossijskowo prawa" 2007, nr 2, s. 45.

[29] A.W. Gyske, op. cit., s. 151.; A.I. Dołgowa (red.), *Priestupnost' w Rossiji nacziała XXI wieka i reagirowanije na niejo*, Moskwa 2004, s.61-62.

te jest wszczęcie procesu wobec konkurenta w biznesie, przeciwnika politycznego, ile kosztuje podpis gubernatora, np. w sprawach z zakresu budownictwa. Szczególnie jest to widoczne w Sankt Petersburgu, w mieście, w którym wyburza się wiele starych budynków, by zbudować luksusowe hotele. Decyzji w tym zakresie wydaje się wiele, ale trzeba je opłacić odpowiednim urzędnikom, najczęściej 20% wartości kontraktu budowlanego (tzw. „otkat"). Jego wysokość zależy od zakresu i miejsca wykonywanych usług (na terenie miasta, regionu). Taki „otkat" płacony jest też w innych sytuacjach, np. przy kontrabandzie – od wartości przemycanego towaru, od wartości zleceń na różne prace, w tym projekty badawcze. Za wszystko należy płacić. Przy obecnym poziomie korupcji nie da się w Rosji rozwiązać żadnych problemów. Bowiem ważne jest tylko to, komu, ile i za co należy zapłacić. Jest to straszne, to niszczy kraj, społeczeństwo.

W kraju panuje przekonanie, że w Rosji wszyscy chcą walczyć z korupcją. Powstają plany, akty, komisje, ale to i tak nic nie zmienia. Tylko stawki rosną. Jeśli kilka lat temu przyjęcie na uniwersytet moskiewski kosztowało 8 tys. dolarów, to obecnie 30-40 tys. „Ucieczka" przed odbyciem służby wojskowej kosztowała niegdyś ok. 10 tys. dolarów, dziś ok. 100 tys. dolarów.

Informacje podane przez J.I. Gilinskiego przekonują o poważnym zagrożeniu ze strony korupcji, zarówno dla państwa, jak i społeczeństwa. Utrudnia ona przede wszystkim życie przeciętnego, niezamożnego obywatela, podważa jego wiarę w równość. Uwikłanie w ten proceder funkcjonariuszy organów ścigania i wymiaru sprawiedliwości - organów stojących na straży sprawiedliwości - pozostawia obywateli samych sobie w tym państwie.

C. Zagrożenia wynikające z terroryzmu

Zagrożenia związane z terroryzmem wynikają z celów, jakie chce się osiągnąć, tj. z: dążenia do zmiany ustroju i polityki państwa, naruszenia terytorialnej integralności państwa, spowodowania dezorganizacji władzy państwowej, uzyskania ustępstw od władzy, wywołania wojny lub konfliktu wojennego, stworzenia nowych (narodowościowych, religijnych) standardów stosunków społecznych.[30)]

Wynikają one również z metod działania terrorystów zmierzających, przede wszystkim, do wywołania strachu i napięcia poprzez użycie przemocy lub jej groźby, z wykorzystaniem mediów[31)], do powodowania poważnych następstw zarówno o charakterze materialnym, jak i niematerialnym (uszczerbek na zdrowiu lub śmierć ludzi). Na ofiary wybierane są osoby przypadkowe, czego przykładem był, np. zamach na Dubrowce czy w Biesłanie. Ponadto, drastyczność aktów terrorystycznych, bezkompromisowość działań terrorystów, zastosowanie najnowszych technologii, globalny charakter[32)] działalności terrorystycznej powoduje poczucie destabilizacji państwa[33)]. Przyczynia się do tego wysoki stopień zorganizowania i konspiracji działań oraz trudności w prognozowaniu aktów terrorystycznych[34)].

---

30) W.D. Małkow (red.), op. cit., s.299.

31) Tamże, s. 300.

32) A.A. Matwiejewa, *Tierrorizm,* w: N.F. Kuzniecowa (red.), *Kriminołogija*, Moskwa 2006, s.130-131, 133--134.; R..H. Makujew, *Tierrorizm w usłowijach globalizaciji,* „Gosudarstwo i Prawo" 2007, nr, 3, s. 44.

33) W.D. Małkow (red.), op. cit., s. 301.

34) A.A. Matwiejewa, op. cit., s. 130-131, 133-134.

Poważne zagrożenie wynika z powiązań terroryzmu z przestępczością zorganizowaną, dzięki której uzyskuje on środki finansowe na swoją działalność. Jest to ważne, gdyż pieniądze potrzebne są terrorystom na logistyczne przygotowanie zamachów.[35)]

Oceniając problem terroryzmu w Rosji, J.I.Gilinskij stwierdził, że *Obecnie w Rosji najczęściej mają miejsce indywidualne akty terroru. Teraz nie dochodzi do wybuchów domów, ale do zabójstw konkretnych ludzi, zwłaszcza w Moskwie. Często mają one podłoże polityczne lub religijne. Dużo jest zabójstw dziennikarzy, którzy piszą prawdę, za co giną.*

Jak widać, terroryzm w Rosji przechodzi ewolucję. Zmiany związane są, z pewnością, z normowaniem się sytuacji w Czeczenii, mniejszym nasileniem konfliktów narodowościowych i religijnych w tym kraju.

Poza wyżej wymienionymi zagrożeniami w sferze przestępczości J.I. Gilinskij zwraca też uwagę na inne niebezpieczeństwa. *Na drugim miejscu wśród zagrożeń* [po korupcji – przyp. K.L.] *należy umieścić alkoholizm społeczeństwa rosyjskiego. Jest to stara przypadłość Rosjan, ale takiej skali, jaka jest dzisiaj, jeszcze nie było. Szczególny problem stanowi alkoholizm, zwłaszcza, wśród ludności małych miasteczek i wsi. Rozpiła się cała wieś rosyjska. Związane jest to z dużym bezrobociem w małych miasteczkach, wokół upadłych kombinatów. Swój smutek ludzie bez pracy topią w wódce, samogonie, perfumach i różnorodnych wynalazkach alkoholopodobnych. Alkoholizm rozwija się zarówno wśród ludzi starych, jak i młodych. Przykładem jest znany mi kazus 6-letniego dziecka leczonego z uzależnienia od piwa, nabytego w wyniku rozpijania go przez ojca. Niepokojące jest, że młodzież łączy nieraz piwo z narkotykami. Taki masowy alkoholizm jest prawdziwym zagrożeniem dla Rosji.*

Co się tyczy zwykłych ludzi, to problem stanowi przemoc, w tym zabójstwa, zgwałcenia, pobicia. To nie są zagrożenia dla państwa, a dla społeczeństwa.

Profesor zastrzegł, że nie lubi pojęcia „bezpieczeństwo narodowe", gdyż *często posługują się nim politycy, wykorzystując je do własnych celów. To, co się politykom nie podoba, nazywają zagrożeniem dla bezpieczeństwa państwa, społeczeństwa.*

W tym miejscu warto zastanowić się, jakie są przyczyny wyżej wymienionych zagrożeń. Według A.I. Dołgowej, stanowią je:

- niesystemowe przemiany stosunków społecznych i nasilanie się sprzeczności między interesami różnych grup społecznych,
- niskie zarobki powodujące niewysoki standard życia i nasilanie się agresji oraz potrzebę poszukiwania nowych źródeł dochodów,
- upadek lub kryzys wartości, związany z brakiem lub niedostateczną kontrolą państwa w sferze społecznej i duchowej,
- dobór nieodpowiedniej, słabo przygotowanej i zabezpieczonej technicznie kadry do przeciwdziałania i zwalczania różnych przejawów przestepczości,
- nieadekwatność, słabość i inne mankamenty ustawodawstwa[36)].

---

35) A.I. Dołgowa, *Priestupnost' tierroristiczieskowo charaktiera,* w: A. I. Dołgowa (red.), Kriminołogija, Moskwa 2007, s.612.; J.A. Stiepanowa, *Rol' narkobizniesa w politekonomii konfliktow i tierrorizma*, Moskwa 2005, s. 258-259., J.I. Awdiejew, A.J. Guśkow, *Problemy organizowannosti sowriemiennowo tierrorizma,* w: A.I. Dołgowa (red.), *Organizowannyj tierrorizm i organizowannaja priestupnost'*, Moskwa 2002, s. 31.

36) A.I. Dołgowa, *Organizowannaja priestupnost', terrorizm i korrupcija: tiendienciji i sowierszenstwowanije bor'by s nim*, „Prokurorskaja i Sliedstwiennaja Praktika" 2005, nr 3-4, s. 169-170.; Zob. też G.G. Gorszenkow, *Prawowoj aspiekt nacjonalnoj biezopasnosti*, „Rossijskij kriminołogiczieskij wzgliad" 2006, nr s. 110-113.

J.I. Gilinskij uznał, że nie ma wspólnego mianownika w etiologii tak różnych niebezpieczeństw. Uważa on, że *Różne są przyczyny tych wszystkich zagrożeń. Jeśli chodzi o zachowania o charakterze terrorystycznym, to przyczyną jest walka o władzę, o to, by władza mogła spokojnie funkcjonować. Np. śmierć Anny Politkowskiej to przykład śmierci w walce nie o władzę (bo ona nigdy nie chciała być u władzy), ale walka o to, by inni mogli utrzymać swoje bezpieczne pozycje.*

Co do korupcji – to nie ma jednej przyczyny. Odkąd pojawiły się w Rosji wszelkie dobra, których nie można było wcześniej nabyć, odtąd korupcja zaczęła się jeszcze intensywniej rozwijać. Za wypłatę nie da się kupić jachtów czy willi we Francji. Podstawową przyczyną jest więc niskie uposażenie urzędników państwowych. Np. oficer milicji zarabia bardzo mało, starszy oficer nieco więcej, ale stawki ich wynagrodzenia oscylują wokół wysokości minimalnej płacy w Rosji. Stąd pomysły, by podnieść pensje, jednakże trzeba wiedzieć, że w warunkach rosyjskich wraz z podwyżkami wzrosną też stawki łapówek. Jest to więc zamknięty krąg, z którego nie ma wyjścia.

Jeśli chodzi o ogólną przestępczość i przemoc, to tak jak wskazywał, np. K. Marks czy R. Merton, ich przyczyną są nierówności społeczne i ekonomiczne.

Przyczyny przestępczości w Rosji , zatem, są skutkiem nierozwiązanych od lat problemów związanych z transformacją, problemów o charakterze politycznym, gospodarczym, organizacyjnym, prawnym i społecznym. Mają one zarówno wewnętrzny, jak i zewnętrzny charakter.

3. Przedsięwzięcia podejmowane przez państwo rosyjskie w celu ograniczania lub eliminacji zagrożeń

W świetle *Koncepcji*, w sferze walki z przestępczością w Rosji (w tym zorganizowaną, korupcyjną, terrorystyczną) konieczne jest w szczególności:

- *ujawnianie, likwidowanie i przeciwdziałanie przyczynom i warunkom rodzącym przestępczość, zwiększenie roli państwa jako gwaranta bezpieczeństwa jednostki i społeczeństwa, stworzenie bazy prawnej i jej efektywne stosowanie,*
- *wzmocnienie systemu organów ochrony porządku publicznego, w szczególności struktur odpowiedzialnych za przeciwdziałanie przestępczości zorganizowanej i terroryzmowi, umożliwienie im skutecznej działalności*,
- *rozwój współpracy w zakresie ochrony porządku publicznego, zwłaszcza z krajami WNP.*

Jak podkreślono w przedmiotowej *Koncepcji*, „środki i decyzje podejmowane przez władze w zakresie walki z przestępczością powinny być jawne, konkretne i zrozumiałe dla każdego obywatela, mieć wyprzedzający charakter, gwarantować równość wszystkich przed prawem, nieuniknioną odpowiedzialność, mieć poparcie społeczne".

W *Koncepcji* założono, że do przeciwdziałania zagrożeniom mają służyć regulacje prawne uwzględniające międzynarodowe zobowiązania Rosji, gwarantujące prawa człowieka. Przykładowo, w celu przeciwdziałania korupcji należy stworzyć warunki uniemożliwiające legalizację kapitałów zdobytych w sposób nielegalny, stworzyć system kontroli finansowej, wykorzystywać środki o charakterze administracyjnym, cywilnym i karnym, mechanizm kontroli dochodów urzędników i pracowników instytucji o różnych formach własności. Powinno się podejmować środki przeciwdziałające i zwalczające terroryzm, narkobiznes i przemyt. Należy współpracować z organami innych państw, stworzyć mechanizmy przeciwdziałające nielegalnemu obrotowi bronią,

materiałami wybuchowymi i ich napływowi z zagranicy, ścigać i inwigilować osoby prowadzące na terytorium Rosji działalność terrorystyczną.

W tym miejscu rozważań należałoby sprawdzić, jak w praktyce wygląda owo przeciwdziałanie i zwalczanie zagrożeń.

Należy stwierdzić, że zwłaszcza od początku lat 90. państwo podejmowało wiele działań o charakterze prawnym.

W zakresie zwalczania przestępczości zorganizowanej należy wskazać: Dekret Prezydenta FR *O niezbędnych sposobach ochrony ludności przed bandytyzmem i innymi przejawami przestepczości zorganizowanej* z 1994 r., ustawę *O walce z przestępczością zorganizowaną* z 1995 r., *Kodeks karny* z 1996 r., ustawę *O działalności operacyjno-dochodzeniowej* z 1995 r., ustawę *O przeciwdziałaniu legalizacji (praniu) dochodów uzyskanych w sposób nielegalny* z 2001 r.

Akty prawne o charakterze antykorupcyjnym stanowią: Dekret *o walce z korupcją w systemie służby państwowej* z 1992 r., ustawa *o podstawach służby państwowej Federacji Rosyjskiej* z 1995 r., Dekret Prezydenta FR *O środkach zwiększenia dyscypliny w systemie służby państwowej* z 1996 r., *Kodeks Karny* z 1996 r., ustawa *O przeciwdziałaniu korupcji* z 2008 r., ustawę *O wniesieniu zmian do poszczególnych aktów prawnych Federacji Rosyjskiej w związku z przyjęciem ustawy federalnej «o przeciwdziałaniu korupcji»* z 2008r. oraz ustawa *O wniesieniu zmian do poszczególnych aktów prawnych Federacji Rosyjskiej w związku z ratyfikacja konwencji Organizacji Narodów Zjednoczonych przeciwko korupcji* z 2003r. i *Konwencji o odpowiedzialności karnej za korupcję* z 1999 r. oraz *przyjęciem ustawy federalnej «o przeciwdziałaniu korupcji»* z 2008 r.

W zakresie zwalczania terroryzmu należy wskazać: ustawę *O walce z terroryzmem* z 1998 r., *Kodeks Karny* z 1996 r., ustawę *O przeciwdziałaniu terroryzmowi* z 2006 r.

Można zatem wymieniać szereg aktów dotyczących poszczególnych problemów[37]. Owo ustawodawstwo kształtowało się przez wiele lat. Powstawało na fali ważnych i poważnych wydarzeń oraz zjawisk negatywnych. Poza tym, uchwalano wiele koncepcji i programów, których założeniem było dążenie do ograniczania lub eliminowania omówionych zagrożeń. Powoływano też szereg organów i służb, których działalność nie zawsze była jednak efektywna.

J.I. Gilinskij uważa, że w Rosji reakcja państwa na zagrożenia *jest prosta, jedna – zwiększenie kar. Fakt, że podłożem tych zagrożeń są nierówności społeczne, nikogo nie martwi. Podwyżki pensji, czy emerytur są tak niewielkie, że pokrywają jedynie inflację, więc nigdy nie wyeliminują tych nierówności.*

Zatem, jaka jest przyszłość przedstawionych zagrożeń, w tym przestępczości? W ocenie J.I. Gilinskiego, (To) *zależy od reżimu politycznego. Niski poziom przestępczości w Rosji miał miejsce po II wojnie światowej, w okresie odwilży chruszczowowskiej i pierestrojki, czyli w czasach choćby niewielkiej liberalizacji, demokratyzacji życia społecznego i politycznego. Zatem, jak wynika z doświadczeń historycznych, pozytywne rezultaty daje w szczególności zmniejszenie wysokości orzekanych kar i surowości władzy wobec społeczeństw.*

[37] O.A. Stiepanow postuluje, by w warunkach globalizacji zagrożeń stworzyć prawo ponadpaństwowe, międzynarodowe jako reakcję na zagrożenia o charakterze globalnym. Zob. O.A. Stiepanow, *Usłowija formirowanija prawa biezopasnosti*, „Gosudarstwo i Prawo" 2007, nr 2, s. 82 i nast.

Czy głos profesora zostanie wysłuchany, pokaże czas. Zatem, przed władzami Rosji stoją poważne zadania w zakresie oddziaływania na omawiane zagrożenia. Ich realizacja ze względu na mentalność Rosjan nie szanujących prawa i pozostających z władzą w specyficznych relacjach będzie zapewne trudna.

Odpowiadając na pytania postawione na początku rozważań należy stwierdzić, że w Rosji, w aspekcie kryminologicznym, podstawowe zagrożenia stanowi przestępczość o charakterze zorganizowanym, korupcyjnym i terrorystycznym. Zjawiska te są głęboko zakorzenione w społeczeństwie, stąd też niełatwo poddają się oddziaływaniu państwa. Pomimo podejmowanych przedsięwzięć, zmierzających do ich ograniczania nadal stanowią poważne zagrożenie ze względu na skalę, przejawy i tendencje przemian zachodzących w Rosji. Ich eliminacja wymaga wspólnych wysiłków państwa i społeczeństwa.

ABSTRACT

The paper by Katarzyna Laskowska shows the criminological aspects of the present threats to Russia's security. The author starts by identifying the threats. Based on the 1997 "National security concept of the Russian Federation," and an interview with J. I. Gilinsky, the author determines that in their nature the threats are both internal (such as social and economic problems and growth of organized crime and corruption) and external (such as proliferation of weapons of mass destruction, expansion of foreign espionage, and growth of terrorist and international criminal organizations). The common feature of the threats is their damaging impact on the sense of security of the Russian state, society, and citizens. The author emphasizes the fact that the key criminal threats are organized crime, corruption, and terrorism. She also describes the negative consequences of the presence of such threats and determines the factors contributing to their growth, such as changes in the Russian society, involving most of all the collapse of a value system and the bad financial situation of the citizens, shortcomings of the laws, and low efficiency of the Russian state's law enforcement agencies.

In the paragraphs following the stipulation of threats and their sources, the author presents a number of examples of laws aimed to fight corruption, terrorism, and organized crime. She emphasizes the fact that the efforts made by the Russian government are not always effective, as the phenomena in question are often deeply rooted in the society and are not easy to change by the government's actions. Only joint efforts by both the Russian state and the Russian society may lead to success in this area.

Andrzej Makarski

Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego. Geneza, zasady działania oraz doświadczenia po pierwszym roku funkcjonowania

I. GENEZA

Przeprowadzona pod koniec 2007 r. analiza porównawcza rozwiązań systemowych w państwach UE, realnie zagrożonych atakiem terrorystycznym, z funkcjonującą wówczas strukturą w Polsce wykazała, że:

- w wielu krajach Wspólnoty istnieją rozwiązania pozwalające na koordyncję działalności służb i instytucji państwowych w zakresie przeciwdziałania terroryzmowi;
- w zależności od zastosowanych systemów, ich działanie dotyczy sfery analityczno-informacyjnej, czynności operacyjno-rozpoznawczych, prewencyjnych lub reagowania po dokonaniu zamachu terrorystycznego;
- uplasowanie struktur i osób koordynujących działania jest różnorodne – niejednokrotnie są to członkowie Rad Ministrów, jednostki organizacyjne Ministerstw Spraw Wewnętrznych albo podmioty funkcjonujące w lub przy wewnętrznych służbach specjalnych;
- pomimo rekomendacji Wspólnoty[1)] oraz wcześniejszych prób opracowania rozwiązań systemowych w tym zakresie, w Polsce brakuje struktury, która koordynowałaby działalność krajowych służb i instytucji w zakresie zwalczania terroryzmu;
- w zakresie czterech filarów UE zajmujących się przeciwdziałaniem terroryzmowi (zapobieganie, ochrona, ściganie i reagowanie[2)]) w RP funkcjonuje znaczna liczba organów państwowych podległych Prezesowi Rady Ministrów, ministrom spraw wewnętrznych i administracji, finansów, obrony narodowej, spraw zagranicznych oraz

---

[1)] Zgodnie z zaleceniem nr 2 Rady do Spraw Wymiaru Sprawiedliwości i Spraw Wewnętrznych UE, opracowanym na podstawie oceny rozwiązań antyterrorystycznych o charakterze prawnym, administracyjnym i technicznym (ang. *peer evaluation*) krajów członkowskich UE, należy powołać podmiot, którego zadaniem będzie koordynacja działań instytucji rządowych, organów ochrony prawa oraz służb specjalnych w zakresie zwalczania terroryzmu. Szczegółowe zalecenia przedstawiono w załączniku do opracowania.

[2)] W zakresie zwalczania terroryzmu kierunki działania państw UE wyznaczają:
- przyjęta przez Radę UE w dniach 1-2 grudnia 2005 r. *Strategia UE w zakresie zwalczania terroryzmu*,
- zaakceptowany w czerwcu 2004 r. i zaktualizowany w 2005 r. *Plan działania dotyczący zjawiska terroryzmu*.

Podstawą ich stworzenia było wskazanie czterech filarów zwalczania terroryzmu:
- **zapobieganie** *(Prevent)* – przeciwdziałanie wstępowaniu osób w szeregi organizacji terrorystycznych poprzez eliminację czynników powodujących radykalizację postaw i rekrutację do ugrupowań o charakterze terrorystycznym zarówno w Europie, jak i na całym świecie;
- **ochrona** *(Protect)* – zabezpieczanie obywateli i infrastruktury przed zagrożeniem terrorystycznym, m.in. poprzez zwiększenie skuteczności ochrony granic, bezpieczeństwa transportu oraz obiektów o znaczeniu strategicznym;
- **ściganie** *(Pursue)* – zwalczanie działalności terrorystycznej zarówno na terenie UE, jak i poza granicami państw członkowskich, poprzez rozbicie grup i organizacji terrorystycznych, a także pozba-

infrastruktury. Ich działania nie są w pełni koordynowane, a efektem tego stanu są różne – niejednokrotnie skrajnie rozbieżne – oceny poziomu zagrożenia terrorystycznego RP oraz identyfikacji czynników oddziałujących na ten stan.

W związku z taką diagnozą stworzona została koncepcja rozdziału zadań wynikających ze strategii UE dotyczącej zwalczania terroryzmu pomiędzy instytucje państwowe oraz powołania struktury o charakterze operacyjnym – Centrum Antyterrorystycznego ABW. Koncepcja ta została zaakceptowana 16 stycznia 2008 r. przez wicepremiera, wcyesnego ministra spraw wewnętrznych i administracji Grzegorza Schetynę oraz Szefa ABW ppłk. Krzysztofa Bondaryka. Następnie, projekt ten przedstawiony został członkom Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych, którzy na styczniowym posiedzeniu poparli zawarte w nim idee[3)], dotyczące przede wszystkim:

- rozdziału kompetencji i wskazania podmiotów koordynujących realizację zadań na terenie Polski:

Rys. 1. Rozdział kompetencji i wskazanie podmiotów koordynujących realizację zadań w RP.

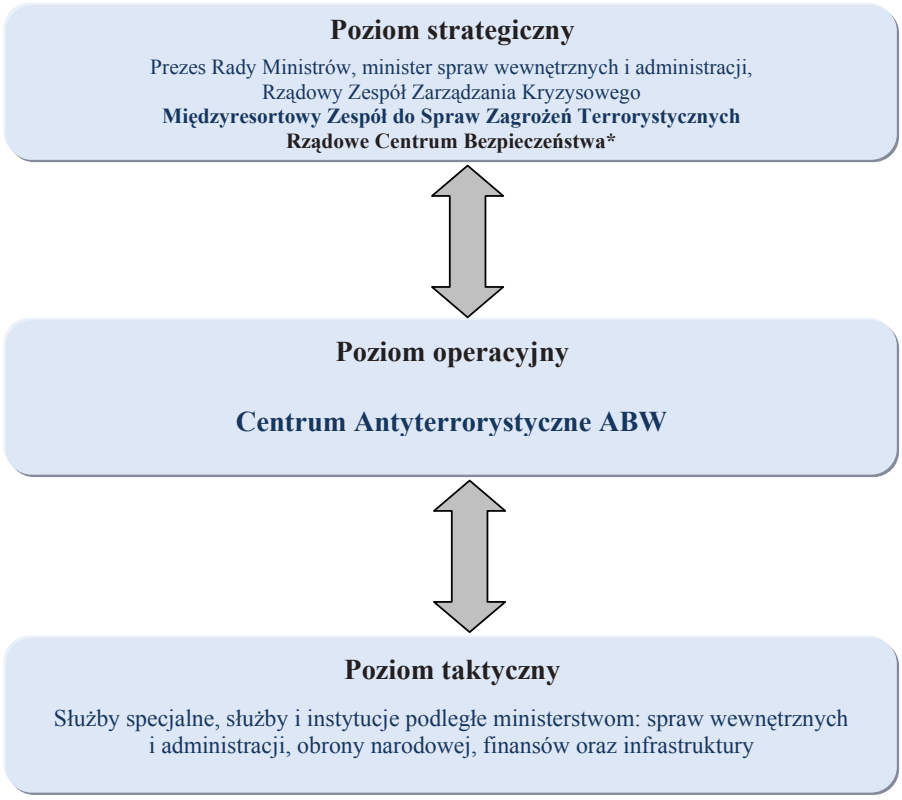
wianie ich członków zaplecza logistycznego (broń, fundusze, łączność, środki transportu) i stawianie przed wymiarem sprawiedliwości;

– **reagowanie** *(Respond)* – stworzenie efektywnego programu zarządzania kryzysowego i minimalizacji skutków zamachu terrorystycznego, obejmującego, m.in., koordynację działań po ataku, a także zapewnienie pomocy ofiarom.

Omówione cztery filary zwalczania terroryzmu znajdują swoje odzwierciedlenie w schemacie przedstawionym na rysunku 1.

[3)] Zespół został powołany na podstawie Zarządzenia Prezesa Rady Ministrów nr 162 z 26 października 2006 r. (z późn. zm.). W jego pracach uczestniczą: przewodniczący – minister spraw wewnętrznych i administracji, ministrowie: finansów, spraw zagranicznych, sprawiedliwości, obrony narodowej, koordynator do spraw służb specjalnych (jeżeli został powołany); zastępcy przewodniczącego oraz sekretarze i podsekretarze stanu w MSWiA, sekretarz Kolegium do Spraw Służb Specjalnych, Generalny Inspektor Informacji Finansowej, Generalny Inspektor Kontroli Skarbowej; szefowie: Służby Celnej, ABW, AW, SWW, SKW, Sztabu Generalnego WP, BOR; komendanci: Główny Policji, Główny Straży Granicznej, Główny Państwowej Straży Pożarnej, Żandarmerii Wojskowej, Obrony Cywilnej Kraju; dyrektor Rządowego Centrum Bezpieczeństwa – członkowie. Ponadto na posiedzenia zapraszany jest Szef BBN.

• struktury krajowego systemu zwalczania terroryzmu:



* stan po 2008 roku

Rys. 2. Struktura systemu zwalczania terroryzmu w RP.

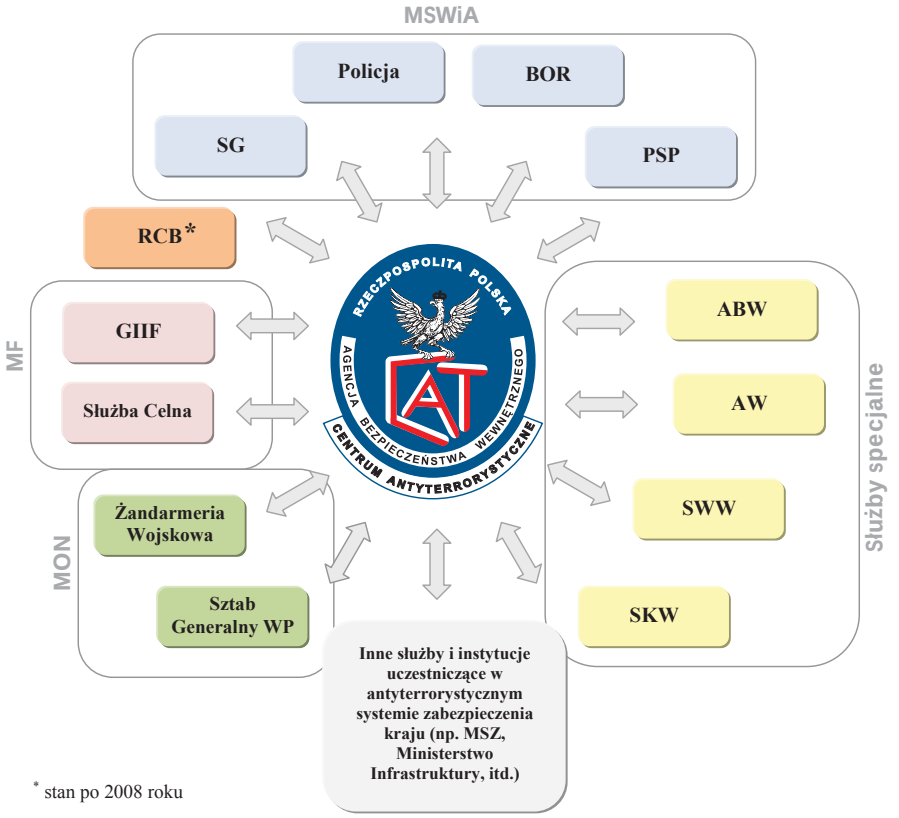
Poziom strategiczny realizowany jest przez Prezesa Rady Ministrów i podległe mu organa, w tym: Rządowy Zespół Zarządzania Kryzysowego i Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych (MZdsZT), kierowany przez ministra spraw wewnętrznych i administracji. Strukturą wspomagającą funkcjonowanie Zespołu jest Stała Grupa Ekspercka. Ustalenia MZdsZT mają bezpośrednie przełożenie na działania jego członków tworzących **poziom taktyczny.** Zadania szczebla strategicznego obejmują w szczególności:

• wytyczanie kierunków i obszarów działań antyterrorystycznych krajowych służb i instytucji odpowiedzialnych za bezpieczeństwo;
• koordynację przepływu informacji na szczeblu rządowym.

Poziom operacyjny służy stałemu, szybkiemu i syntetycznemu informowaniu kierownictwa państwa o zagrożeniach oraz działaniach w związku z nimi podejmowanych przez służby państwowe. Na tym poziomie odbywa się również koordynacja działań – na płaszczyźnie analityczno-informacyjnej – służących identyfikacji i przeciwdziałaniu zagrożeniom terrorystycznym, prowadzonych przez krajowe służby i instytucje.

Poziom taktyczny (wykonawczy) – realizowany przez krajowe służby i instytucje uczestniczące, zgodnie z ustawami kompetencyjnymi, w antyterrorystycznej ochronie kraju:

- dwukierunkowego obiegu informacji o zagrożeniach terrorystycznych w ramach Centrum Antyterrorystycznego ABW:



Rys. 3. Obieg informacji w CAT ABW.

Wspólna koncepcja MSWiA i ABW przedstawiona została następnie do zaopiniowania oraz akceptacji Sejmowej Komisji do Spraw Służb Specjalnych (w marcu i czerwcu 2008 r.), Kolegium do Spraw Służb Specjalnych (w kwietniu i lipcu 2008 r.) oraz Rządowemu Centrum Legislacyjnemu (w marcu 2008 r.). Ostatecznie projekt uzyskał akceptację Prezesa Rady Ministrów Donalda Tuska, który 17 września 2008 r. w Zarządzeniu nr 102 (M.P. z 2008 r. nr 69, poz. 622) zmienił statut Agencji Bezpieczeństwa Wewnętrznego i powołał od 1 października 2008 r. nową jednostkę organizacyjną – Centrum Antyterrorystyczne ABW.

II. ZADANIA

Głównym zadaniem Centrum Antyterrorystycznego ABW jest koordynacja działań służb i instytucji uczestniczących w zabezpieczeniu kraju przed zagrożeniem terrorystycznym w zakresie analityczno – informacyjnymoraz wspieranie na bazie pozy-

skanych i przeanalizowanych informacji procesu decyzyjnego kierownictwa państwa. Centrum wypełnia to zadanie poprzez realizację następujących działań:

1. Wspomaganie procesów decyzyjnych w przypadku realnego zagrożenia atakiem terrorystycznym CAT, niezwłocznie po uzyskaniu wiedzy o możliwym zamachu, przekazuje wszelkie dane pozwalające na przygotowanie i zabezpieczenie sił i środków niezbędnych do prawidłowego reagowania kryzysowego m.in. prezydentowi, prezesowi Rady Ministrów, ministrowi spraw wewnętrznych i administracji oraz dyrektorowi Rządowego Centrum Bezpieczeństwa.
2. Koordynację działań operacyjno – rozpoznawczych w zakresie zwalczania terroryzmu, realizowaną m.in. poprzez:
   - cykliczne lub doraźne narady osób szczebla decyzyjnego, w trakcie których określane są zadania do realizacji w ramach rozpoznawanych zagrożeń oraz wytyczane perspektywiczne kierunki i obszary aktywności służb i instytucji państwowych;
   - przekazywanie sygnałów o potencjalnych zagrożeniach w celu podejmowania, na bieżąco, działań zgodnie z algorytmami reagowania w sytuacjach zagrożenia;
   - monitoring aktywności organizacji terrorystycznych i ich członków oraz struktur wspierających działalność fundamentalistów na terenie RP;
   - monitoring poziomu bezpieczeństwa obiektów mogących stanowić potencjalne cele ataku terrorystycznego.
3. Wykonywanie czynności analityczno-informacyjnych w zakresie:
   - sporządzania raportów sytuacyjnych – aktualnych, syntetycznych i pełnych informacji dla kierownictwa państwa (prezydenta RP, prezesa Rady Ministrów) na temat poziomu zagrożenia terrorystycznego kraju oraz działań podejmowanych przez służby i instytucje państwowe w celu zniwelowania niebezpieczeństw;
   - długo – i krótkookresowych prognoz poziomu zagrożenia terrorystycznego Polski;
   - analiz zagrożenia terrorystycznego w innych państwach w kontekście bezpieczeństwa strategicznych interesów RP oraz polskich obywateli;
   - udziału w sporządzaniu ocen funkcjonowania systemów ochrony elementów infrastruktury krytycznej kraju pod kątem usunięcia ewentualnych nieprawidłowości.
4. Udział w opracowywaniu i nowelizacji procedur reagowania kryzysowego na wypadek ataku oraz sporządzanie algorytmów działań przed zamachem.
   Centrum Antyterrorystyczne uczestniczy w działaniach mających na celu weryfikację skuteczności aktualnie stosowanych schematów postępowania w sytuacjach kryzysowych oraz wykrywanie i analizę słabych punktów zarządzania kryzysowego przy jednoczesnym wskazaniu potencjalnych strategii i kierunków dalszych działań.
5. Monitoring radykalnych mediów.
   Systematycznie prowadzony monitoring mediów obcojęzycznych, w tym arabskich i kaukaskich, pozwala na regularne opracowywanie raportów zawierających zestawienie prezentowanych w nich treści, które mogą wskazywać na istnienie zagrożenia dla obywateli lub interesów Rzeczypospolitej.
6. Wspomaganie po ewentualnym zamachu terrorystycznym działań służb i instytucji uczestniczących w ochronie antyterrorystycznej Polski.
   Pozyskiwane przez Centrum Antyterrorystyczne ABW sygnały – zarówno pochodzące ze źródeł otwartych, jak i operacyjnych – gromadzone są w specjalistycz-

nej bazie danych, stworzonej specjalnie na potrzeby Centrum przez ekspertów Departamentu Bezpieczeństwa Teleinformatycznego ABW. W bazie tej dokonuje się również podziału informacji na jednostki analityczne, tak by można było przeszukiwać zasoby przez różne typy rekordów. W ten sposób stworzona sieć powiązań, w przypadku rozpracowywania grupy ekstremistycznej lub ewentualnego zaistnienia ataku terrorystycznego, służy do budowania analiz kryminalistycznych powiązań sprawców z osobami udzielającymi im logistycznego wsparcia. Jednym z takich przykładów są analizy opracowane na potrzeby śledztwa w sprawie uprowadzenia i zamordowania przez terrorystów polskiego geologa w Pakistanie.

7. Współpraca zagraniczna

Współpraca zagraniczna CAT ABW prowadzona jest zarówno na płaszczyźnie dwustronnej, jak i wielostronnej. Obejmuje, przede wszystkim, wymianę informacji, wspólną analizę globalnych zagrożeń oraz korzystanie z doświadczeń i wiedzy innych państw. Wszelkie aspekty tej aktywności omawiane są zarówno w trakcie regularnych, jak i doraźnych spotkań, seminariów, warsztatów oraz za pośrednictwem systemów bezpiecznej łączności.

Centrum współpracuje m.in. ze strukturami Unii Europejskiej, NATO, Rady Europy i OBWE oraz gremiami zrzeszającymi służby specjalne innych krajów. W ramach tej współpracy uczestniczy w pracach:

- międzynarodowej grupy antyterrorystycznej (ang. *Counter-Terrorist Group – CTG*), utworzonej w następstwie wydarzeń z 11 września 2001 r.;
- grupy roboczej UE ds. terroryzmu (ang. *Working Party on Terrorism – WPT*) w ramach współpracy policyjnej i sądowej w sprawach karnych;
- grupy zwanej Klubem Berneńskim, która skupia służby wywiadu i bezpieczeństwa Państw Członkowskich UE oraz Norwegii i Szwajcarii;
- Komitetu Specjalnego NATO (AC/46), utworzonego w 1952 r., który doradza organowi decyzyjnemu NATO oraz przygotowuje raporty dotyczące zagrożeń bezpieczeństwa, wynikających m.in. z działalności terrorystycznej;
- Konferencji Europy Środkowej (ang. *Middle Europe Conference – MEC*), powstałej w 1994 r. z inicjatywy holenderskiej.

CAT ABW podejmuje również współpracę na zasadach dwustronnych, na podstawie porozumień określających ramy współdziałania w zakresie obronności, wspierania pokoju, zapobiegania przestępczości i zwalczania terroryzmu. Takie porozumienia strona polska podpisała m.in. z Austrią, Belgią, Białorusią, Czechami, Estonią, Finlandią, Gruzją, Hiszpanią, Litwą, Niemcami, Słowacją, Szwecją, Ukrainą, Węgrami. Rozwija też współdziałanie ze swoimi odpowiednikami na świecie, szczególnie w państwach europejskich. Obecnie współ-pracuje z: Wielką Brytanią – JTAC (ang. *Joint Terrorism Analysis Centre*), USA – NCTC (ang. *National Counterterrorism Center*), Niemcami – GTAZ (niem. *Gemeinsames Terrorismusabwehrzentrum*), Danią – CTA (ang. *Centre for Terrorism Analysis*) oraz Ukrainą – ATC (ang. *Anti – Terrorist Centre*) i in.

III. FUNKCJONOWANIE

Centrum Antyterrorystyczne ABW funkcjonuje w systemie całodobowym, przez 7 dni w tygodniu. Oprócz funkcjonariuszy ABW służbę w nim pełnią oddelegowani funkcjonariusze, żołnierze i pracownicy m.in. Policji, Straży Granicznej, Biura Ochrony Rządu, Agencji Wywiadu, Służby Wywiadu Wojskowego, Służby Kontrwywiadu Wojskowego oraz Służby Celnej. Realizują oni zadania w ramach kompetencji insty-

tucji, którą reprezentują. Ponadto, z Centrum Antyterrorystycznym ABW aktywnie współpracują inne podmioty uczestniczące w systemie ochrony antyterrorystycznej RP, takie jak Ministerstwo Spraw Wewnętrznych i Administracji, Ministerstwo Spraw Zagranicznych, Państwowa Straż Pożarna, Generalny Inspektor Informacji Finansowej, Sztab Generalny Wojska Polskiego, Żandarmeria Wojskowa, Urząd Lotnictwa Cywilnego, Państwowa Agencja Atomistyki, Rządowe Centrum Bezpieczeństwa itp.

IV. DOŚWIADCZENIA PO ROKU DZIAŁALNOŚCI CENTRUM ANTYTERRORYSTYCZNEGO ABW

1. KATALOG ZDARZEŃ I SYTUACJI ZGŁASZANYCH DO CENTRUM ANTYTERRORYSTYCZNEGO ABW

Jedną z pierwszych kwestii wymagających szybkiego rozwiązania tuż po utworzeniu CAT ABW było zapewnienie właściwego obiegu i dopływu informacji do Centrum, a następnie – po ich weryfikacji i analizie – wdrożenie stosownych procedur reagowania i informowania kierownictwa państwa o możliwych zagrożeniach. Stąd też dokonano kategoryzacji monitorowanych sytuacji na:

1. Zdarzenia terrorystyczne zaistniałe na terenie Polski i mające wpływ na bezpieczeństwo RP i jej obywateli;
2. Zdarzenia terrorystyczne zaistniałe poza granicami Polski i mające wpływ na bezpieczeństwo RP i jej obywateli;
3. Uzyskanie informacji o potencjalnych zagrożeniach mogących wystąpić na terenie Polski i poza granicami RP;
4. Uzyskanie informacji dotyczących prania pieniędzy lub transferów środków finansowych mogących świadczyć o finansowaniu działalności terrorystycznej.

Stworzenie czterech kategorii zdarzeń związanych z zagrożeniami o charakterze terrorystycznym pozwoliło na przygotowanie analogicznej liczby schematów działań krajowych służb i instytucji odpowiedzialnych za przeciwdziałanie terroryzmowi. Przy pracach tych uwzględniono również bardzo ważną rolę, jaką w przypadku dokonania lub planowania przez ekstremistów zamachu terrorystycznego spełnia urząd prokuratora.

Kolejnym etapem było opracowanie katalogu zdarzeń zgłaszanych do Centrum Antyterrorystycznego ABW przez współpracujące w jego ramach służby i instytucje. Decyzją Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych – na podstawie opinii i wkładów wszystkich członków tego gremium – wdrożona została do stosowania lista 104 typów zdarzeń (podzielonych na 15 kategorii), o których powinno być informowane Centrum.

2. SZYBKA WYMIANA I WERYFIKACJA INFORMACJI

Równolegle z pracami zmierzającymi do precyzyjnego i przejrzystego określenia zakresu zadań Centrum, siłami ABW prowadzone są działania zmierzające do uruchomienia rozległej sieci teleinformatycznej (IT CAT) dopuszczonej do przetwarzania informacji objętych tajemnicą państwową. Istotą tego przedsięwzięcia jest skrócenie do zaledwie kilku sekund czasu przekazania sygnału o zagrożeniu, by w odpowiednim czasie móc podejmować skuteczne i efektywne działania zapobiegawcze. Ponadto, uruchomiony został (aktualnie w fazie ostatecznych testów) system informowania o zdarzeniach o charakterze terrorystycznym wykorzystujący szyfrowany kanał łączności mobilnej. Planowany termin zakończenia wszystkich prac wdrożeniowych w sferze teleinformatyki przewidziany jest na I półrocze 2010 r.

Oprócz przedsięwzięć służących zbudowaniu bezpiecznych kanałów przesyłu informacji, w pierwszym roku funkcjonowania Centrum prowadzono działania zmierzające do uruchomienia w CAT ABW jednolitego systemu obrazowania aktualnego stanu bezpieczeństwa m.in. w sferze komunikacji lądowej, morskiej i lotniczej (zwłaszcza w aspekcie przewozu materiałów niebezpiecznych) oraz poziomu promieniowania materiałów rozszczepialnych. Wszystkie te elementy składowe bezpośrednio przekładają się na podwyższanie poziomu pracy w zakresie monitorowania aktualnej skali zagrożenia terrorystycznego RP.

3. NAJWAŻNIEJSZE DZIAŁANIA I PROJEKTY CAT ABW

a) monitorowanie incydentów i zdarzeń o charakterze terrorystycznym.

Utworzenie CAT ABW (1 października 2008 r.) zbiegło się w czasie z uprowadzeniem przez islamskich terrorystów polskiego geologa z firmy „Geofizyka Kraków", pracującego w Pakistanie na kontrakcie (28 września 2008 r.). Już w dniu porwania funkcjonariusze tworzonego wówczas Centrum, na płaszczyźnie informacyjno – analitycznej, zainicjowali wspieranie polskich służb i instytucji operujących za granicą w ich działaniach, zmierzających do uwolnienia Polaka. Materiały uzyskiwane równolegle przez różne instytucje przekazywane były na bieżąco Prokuratorowi Generalnemu, w celu włączenia ich do wszczętego w tej sprawie śledztwa. Tragiczny finał porwania naszego rodaka nie zakończył działań, które CAT ABW prowadził w tej sprawie. Wszelkie naprowadzenia i dowody wskazujące na sprawców tego morderstwa są nadal na bieżąco włączane do toczącego się postępowania, w celu doprowadzenia przed wymiar sprawiedliwości terrorystów, którzy dopuścili się tego czynu.

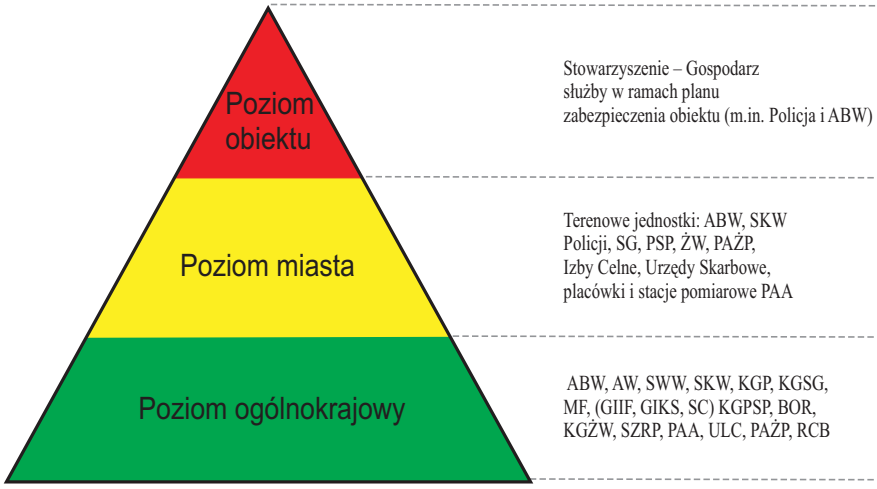
W pierwszym roku działalności CAT ABW zajmowało się również kilkuset aktami piractwa morskiego. Kilka z nich bezpośrednio dotyczyło obywateli RP pływających na statkach pod różnymi banderami, a porywaczami byli niejednokrotnie ekstremiści powiązani z islamskimi organizacjami terrorystycznymi, aktywnymi w rejonie Zatoki Adeńskiej i Oceanu Indyjskiego. Również te incydenty były monitorowane przez Centrum, a efekty monitoringu były wykorzystywane w prowadzonych za granicą przedsięwzięciach zmierzających do uwolnienia uprowadzonych oraz w działaniach procesowych w ramach toczących się postępowań karnych.

Oprócz kilku ważnych zdarzeń o charakterze terrorystycznym, dotyczących obywateli RP, a zaistniałych za granicą, również w Polsce miały miejsce incydenty, które skutkowały wszczęciem przez CAT ABW procedur reagowania kryzysowego oraz równolegle z nimi działań wykrywczych w ramach postępowań przygotowawczych.

b) antyterrorystyczne zabezpieczenie UEFA EURO 2012

Jednym z ważniejszych zadań realizowanych obecnie przez CAT ABW jest przygotowanie antyterrorystycznego zabezpieczenia Mistrzostw Europy w Piłce Nożnej. W ramach tego przedsięwzięcia sporządzono plan dotyczący rozpoznawania, zapobiegania i zwalczania zagrożeń terrorystycznych do Krajowej Strategii Zabezpieczenia UEFA EURO 2012 (koordynatorem prac nad tym dokumentem jest Ministerstwo Spraw Wewnętrznych i Administracji), który w czerwcu 2009 r. zaakceptowany został przez władze UEFA. Oprócz działań planistycznych, wdrożono również prace nad wspólnym dla wszystkich służb uczestniczących w ochronie antyterrorystycznej kraju projektem zbudowania mapy zagrożeń

terrorystycznych dla obiektów Mistrzostw. Obejmuje on trzy poziomy zabezpieczenia terenu (obiektu, miasta organizatora i państwa), uwzględnia czynniki wpływające na wzrost lub obniżenie poziomu zagrożenia (polityczne, społeczne, infrastrukturalne i inne) oraz rozdziela zadania i kompetencje na poszczególnych poziomach zabezpieczenia.



Rys. 4. System ochrony strefy publicznej i prywatnej.

4. PODSUMOWANIE

Centrum Antyterrorystyczne Agencji Bezpieczeństwa Wewnętrznego jest unikatową w skali kraju strukturą odpowiedzialną za jedną ze sfer bezpieczeństwa państwa i obywateli RP. Realizowana w ramach CAT ABW bezpośrednia współpraca oddelegowanych przedstawicieli instytucji zaangażowanych w antyterrorystyczne zabezpieczenie Polski i obywateli RP daje wymierne efekty w postaci:

- znacznego przyspieszenia wymiany informacji o zagrożeniach terrorystycznych,
- stworzenia skutecznego systemu weryfikacji danych,
- raportów przedstawiających całość wiedzy o incydencie i podjętych w związku z nim przedsięwzięciach zapobiegawczych przez podmioty krajowe.

Zapewniona systemowa ochrona informacji niejawnych, a jednocześnie transparentność działań realizowanych przez służby i instytucje współpracujące w ramach CAT ABW przyczyniają się do wzrostu zaufania i zmniejszenia rywalizacji między uczestnikami krajowego systemu ochrony antyterrorystycznej.

Tworząc koncepcję polskiego Centrum Antyterrorystycznego, skorzystano z doświadczeń innych państw, m.in.:

- z brytyjskich rozwiązań (J-TAC) przetransponowano w polskie realia sferę działań w zakresie pracy analityczno-informacyjnej,
- na podstawie rozwiązań niemieckich (GTAZ) stworzono system koordynacji działań operacyjno-rozpoznawczych,
- korzystając z wzorca brytyjskiego (J-TAC) oraz ukraińskiego (ATC) ulokowano Centrum Antyterrorystyczne przy wewnętrznej służbie specjalnej, jaką jest Agencja Bezpieczeństwa Wewnętrznego.

Wyłącznie polskim wkładem w koncepcję działań CAT ABW są zastosowane założenia teleinformatyczne, które – jak niejednokrotnie stwierdzali przedstawiciele zagranicznych centrów – spowodowały, że w polskim Centrum Antyterrorystycznym wdrożone zostały rozwiązania na miarę XXI wieku. Funkcjonalność, jaką już osiągnęło CAT ABW, docenił również Koordynator UE do spraw Zwalczania Terroryzmu, Gelles de Kerchove, który w jednym ze swoich raportów wskazał, że analogiczne rozwiązania należałoby wdrożyć w innych państwach Wspólnoty.

Zalecenia UE dotyczące działań antyterrorystycznych

W wyniku przeprowadzonej przez Radę do Spraw Wymiaru Sprawiedliwości i Spraw Wewnętrznych UE oceny rozwiązań antyterrorystycznych o charakterze prawnym, administracyjnym i technicznym (ang. *peer evaluation*) krajów członkowskich UE opracowano zbiór zaleceń dla państw Wspólnoty. Wytyczne te mają na celu usprawnienie działań oraz zapewnienie nowych instrumentów organom ochrony prawa, służbom specjalnym i innym instytucjom państwowym, które posiadają kompetencje umożliwiające zwalczanie terroryzmu. Wdrożenie zaleceń uzależniono od aktualnego stanu zagrożeń terrorystycznych oraz wszelkich implikacji politycznych w poszczególnych państwach członkowskich.

KLUCZOWE ZALECENIA DZIAŁAŃ NA POZIOMIE KRAJOWYM

Zalecenie nr 1: Koordynacja politycznych wysiłków w zwalczeniu terroryzmu poprzez stworzenie na poziomie ministerialnym struktury odpowiedzialnej za opracowanie ogólnokrajowego planu przeciwdziałania terroryzmowi, prawnego ścigania terrorystów, ochrony infrastruktury krytycznej i zarządzania kryzysowego.
Zalecenie nr 2: Powołanie Koordynatora ds. Zwalczania Terroryzmu, którego zadaniem będzie koordynacja w tym zakresie działań instytucji rządowych, organów ochrony prawa oraz służb specjalnych.
Zalecenie nr 3: Koordynacja ścigania poprzez powołanie urzędu (np. Prokuratora Krajowego), do którego obowiązków będzie należała koordynacja działań organów sprawiedliwości, a także wymiany informacji pomiędzy władzami sądowniczymi i organami ochrony porządku publicznego i służbami bezpieczeństwa.
Zalecenie nr 4: Współpraca między instytucjami oraz dostęp do potrzebnych informacji i danych wywiadowczych poprzez stworzenie planu prowadzonej na bieżąco krajowej koordynacji w zakresie wymiany informacji pomiędzy wszystkimi służbami bezpieczeństwa i wywiadu oraz organami ochrony porządku publicznego, zajmującymi się zwalczaniem terroryzmu.
Zalecenie nr 5: Wielośródłowe oceny zagrożeń terrorystycznych na podstawie wszystkich dostępnych informacji, dostarczane w czasie umożliwiającym podjęcie stosownych decyzji.
Zalecenie nr 6: Gromadzenie informacji polegające m. in. na optymalizacji procesów pozyskiwania i wymiany informacji dotyczących wszystkich aspektów terroryzmu zarówno w kraju, jak i za granicą, według klucza ustalonego adekwatnie do potrzeb danego państwa.
Zalecenie nr 7: Stworzenie odpowiednich podstaw prawnych umożliwiających służbom specjalnym uzyskanie dostępu do baz danych organów ochrony prawa i innych instytucji państwowych. Dostęp ten, jednak, ograniczony zgodnie z zasadą *need to know* oraz zgodny z wymogami ochrony informacji niejawnych.

Zalecenie nr 8: Siły policyjne, w tym również lokalne, powinny być w pełni zaangażowane w walkę z terroryzmem, przejść odpowiednie przeszkolenia oraz być na bieżąco powiadamiane o poziomie zagrożenia.

INNE WAŻNE ZALECENIA

Zalecenie nr 9: Kontrola graniczna powinna uwzględniać aspekty związane z przeciwdziałaniem terroryzmowi, w tym warunki pozyskiwania i wymiany informacji z organami ochrony porządku i służbami specjalnymi.

Zalecenie nr 10: Umożliwienie użycia informacji wywiadowczych jako dowodu w sądzie, co zwiększyłoby możliwości państwa w ściganiu i pociąganiu do odpowiedzialności karnej osób oskarżonych o terroryzm.

Zalecenie nr 11: Zapewnienie podstawy prawnej działania służb i instytucji, która umożliwiałaby pełne wykorzystanie szeregu technik dochodzeniowych, zarówno związanych z wykorzystaniem sprzętu technicznego, jak i innych[4)].

Zalecenie nr 12: Stworzenie systemu bezpiecznej łączności umożliwiającej komunikację krajową i międzynarodową**. Wprowadzenie certyfikatów bezpieczeństwa** dla osób, które dysponują informacjami niejawnymi, również podczas pracy w instytucjach unijnych.

Zalecenie nr 13: Stworzenie systemu zarządzania kryzysowego łączącego działania wszystkich właściwych instytucji i urzędów w celu szybkiego, skoordynowanego reagowania na ataki terrorystyczne. Krajowe centra powinny nawiązać ścisłą współpracę ze swoimi zagranicznymi odpowiednikami, aby przygotować się i odpowiednio zareagować na wypadek przygranicznej sytuacji kryzysowej.

ZALECENIA DZIAŁAŃ NA POZIOMIE UNIJNYM

Zalecenie nr 14: Współpraca z Europolem i Eurojustem, korzystanie z informacji dotyczących terroryzmu z istniejących archiwów Europolu oraz optymalizacja wymiany informacji, również poprzez krajowe biura Europolu. Tam, gdzie istnieją przeszkody, państwa członkowskie powinny rozważyć stworzenie *ad hoc* grup roboczych na poziomie krajowym, z udziałem przedstawicieli właściwych organów oraz reprezentantów Europolu i Eurojustu. Powinna też być wzięta pod uwagę możliwość stworzenia wspólnych zespołów śledczych z udziałem członków tych instytucji.

Zalecenie nr 15: Współpraca z Centrum Sytuacyjnym poprzez optymalizację wkładów przekazywanych do SitCen, w celu poprawy dokonywanych tam analiz strategicznych. W przypadku istnienia przeszkód w przekazywaniu informacji, kraje członkowskie powinny rozważyć stworzenie ad hoc grup roboczych na poziomie krajowym, w skład których będą wchodzili przedstawiciele SitCen.

Zalecenie nr 16: Współpraca z Kolegium Policji Europejskiej (CEPOL), które wspólnie z Europolem powinno przygotować dla urzędników organów ochrony prawa z całej UE szkolenia oraz programy informacyjne na temat przeciwdziałania terroryzmowi. Działanie to promowałoby wzajemne zaufanie pomiędzy krajowymi organa-

[4)] W raporcie sporządzonym po dokonaniu oceny przygotowań Polski w zakresie profilaktyki antyterrorystycznej, Grupa Ewaluacyjna UE wskazała jako jedną z „dobrych praktyk" fakt, iż ABW realizuje swoje ustawowe zadania, posiadając pełnię uprawnień przypisywanych strukturom policyjnym. W ocenie kontrolerów, to rozwiązanie wydaje się być jednym z najskuteczniejszych narzędzi walki z terroryzmem.

mi ochrony porządku publicznego. CEPOL powinien rozważyć możliwości wspierania wymiany pracowników stosownych instytucji krajów członkowskich.

ABSTRACT

During the first year of ABW Antiterrorist Centre activity, it has been proved that its existence as well as its place in the national antiterrorist protection system is fully justifiable. The experience gained so far has taken a direct effect on improving the managing procedures in the national services and institutions, which can be of use in case of obtaining information concerning a terrorist threat to Poland or its citizens. The functioning of the warning system in Poland has been greatly improved by IT solutions applied, which – on one hand – allows for quick gathering and analysis of information, and – on the other hand – makes it possible to transmit data in the appropriate time.

Remigiusz Rosicki

Chiny i Indie a bezpieczeństwo energetyczne Europy

Energia i energetyka

Wzrost zapotrzebowania na energię jest trendem światowym. Przewiduje się, że do 2030 r. popyt na energię wzrośnie o ok. 60%. Ma to szczególne znaczenie ze względu na pojawienie się większej ilości podmiotów, które będą energii potrzebowały. W przyszłości najbardziej znaczącymi konkurentami UE w wyścigu do rynku surowców i energii będą Chiny i Indie. Konsumpcja energii, w podziale na regiony, przedstawia się następująco: państwa OECD (47,3%), Chiny (15%), Azja bez Chin (11,5%), byłe państwa ZSRR (8,1%), Afryka (5,6%), Ameryka Łacińska (5,1%), Bliski Wschód (4,3%)[1)].

Obecnie Chiny cierpią na ciągły głód energii. W 2003 r. przesunęły się na drugie miejsce w światowej konsumpcji ropy naftowej, a trend zwiększającego się uzależnienia od importu tego surowca widoczny jest szczególnie od 1993 r. Należy przypomnieć, że jeszcze w okresie 1998 – 1999 w Chinach mieliśmy do czynienia z nadwyżką energii. Dochodziło do takiej sytuacji, że elektrownie o małej mocy państwo zamykało[2)]. Ówczesna sytuacja gospodarcza uległa pogorszeniu w związku z tzw. „kryzysem azjatyckim", choć nie był on tak dotkliwy, jak w przypadku państw Azji Południowo – Wschodniej, co wynikało ze specyfiki reglamentacji działalności gospodarczej podmiotów międzynarodowych w Chinach[3)].

Bezpieczeństwo energetyczne UE

W problemie bezpieczeństwa energetycznego UE zwraca się uwagę na aspekt uzależnienia od dostaw surowców z Rosji. Trzeba jednak zaznaczyć, że nie wszystkie państwa unijne rozpatrują problem dostaw rosyjskich surowców jako zagrożenie. Wynika to z innej struktury importu surowców. Przykładowo, dla Francji dostawy z obszaru Federacji Rosyjskiej, w gruncie rzeczy będą stanowiły rzeczywistą dywersyfikację dostaw. Wzrost znaczenia Indii i Chin zmusza do refleksji nad przyszłością UE w świecie globalnym – w globalnej gospodarce. Skutki rozwoju gospodarczego tych państw – a nie wykluczone, że w przyszłości także innych – doprowadzą do większej konkurencyjności na rynku surowców, a więc i do możliwości wzrostu ich cen w związku z niewystarczającą podażą. UE zmuszona będzie, a nawet już jest, do rywalizacji o dostęp do surowców. W tym zakresie nie ma wielu rozgrywających, jest za to wiele interesów – zarówno interesów państw, jak i korporacji zajmujących się wydobyciem

---

1) *Key World Energy Statistics 2008*, IEA, Paris 2008, s. 30.

2) P. Olszowiec (oprac.), *Energetyka w Chinach – czas reform*, „Energia Gigawat" 2003, nr 1, (http://www.gigawat.net.pl/article/articleview/120/1/9/, 31 sierpień 2008).

3) B. Drelich – Skulska, *Bezpośrednie inwestycje zagraniczne w gospodarce Chin w latach 1997 – 2005*, w: J. Rymarczyk, B. Drelich – Skulska, W. Michalczyk (red.), *Regionalizacja a globalizacja we współczesnym świecie.* Tom 1, AE Wrocław, Wrocław 2007, s. 220 – 229.

i przetwarzaniem surowców. Już teraz azjatyccy przedsiębiorcy pojawiają się na innych kontynentach, poszukując złóż surowców, eksploatując je lub wykupując inne przedsiębiorstwa, które się tym zajmowały.

Do 2020 r. uzależnienie UE od importu surowców wzrośnie do 60%. Obecnie ponad 75% zapotrzebowania na ropę naftową pokrywa import, w tym ok. 26% tego surowca pochodzi z Rosji. Rosyjski Gazprom pokrywa ok. 30% zapotrzebowania Europy na gaz. Procent ten ulegnie zmianie po realizacji budowy gazociągów Nord Stream i South Stream[4]. Dyskusyjna jest też dywersyfikacja dostaw gazu dzięki budowie gazociągów Nabbucco i Transkaspijskiego. Pozycja Europy w stosunku do Chin i Indii jest uprzywilejowana ze względu na istniejącą infrastrukturę gazociągów i ropociągów. Oznacza to, że naturalnym rynkiem zbytu dla gazu i ropy naftowej jest Europa. Niedługo może się to zmienić w związku planami budowy sieci przesyłowych, które będą łączyć Rosję, Chiny i inne państwa azjatyckie. To, co teraz jest przewagą w aspekcie globalnym, jest również przekleństwem w aspekcie regionalnym. Bowiem, tak silne uzależnienie UE od importu surowców energetycznych z obszaru Federacji Rosyjskiej implikuje możliwość wpływania przez Rosję na politykę UE, co zresztą nie jest ukrywane przez władze rosyjskie, które uznają surowce i biegnące rury za przedłużenie dyplomacji.

Środowisko, rozwój i energia

Przewiduje się, że do 2030 r. ok. 60 % społeczeństwa chińskiego będzie zamieszkiwać na terenach miejskich, co w przypadku państwa chińskiego oznacza, że więcej niż 0,5 miliarda ludzi będzie należeć do skupisk miejskich[5]. Obecnie 20% populacji światowej to mieszkańcy Chin. Podobny procent charakteryzuje populację Indii. Sam rozwój infrastruktury determinuje wzrost zapotrzebowania na energię. Tak więc, nie tylko rozwój gospodarczy i związana z nim zwiększona produkcja, ale i urbanizacja determinuje zwiększone zapotrzebowanie na energię. Ma to swoje konsekwencje we wzroście zanieczyszczenia powietrza. Obecnie Państwo Środka i USA są głównymi „producentami" gazów GHG. Z tego też względu ta dwójka nie ratyfikowała Protokołu z Kioto. Chiny odpowiadają za 20% światowej emisji CO_2, a sama Azja, bez Chin, za prawie 10%[6]. Widoczny spadek emisji CO_2 można było obserwować mniej więcej w okresie „kryzysu azjatyckiego". Od 2002 r. widoczny jest ponowny trend wzrostu w emisji CO_2. Zanieczyszczenie środowiska w Chinach staje się jednym z głównych problemów społecznych, nie licząc ubóstwa, migracji, dysproporcji społecznych czy innych negatywnych skutków transformacji. Zrównoważony rozwój jest obecnie nierealny, a dominacja elementu gospodarczego nad społecznym i ekologicznym jest aż nadto widoczna. Problemy ekologiczne wzmogły się wraz z rozwojem gospodarczym, począwszy od końca lat 70. XX wieku. Poważnym problemem jest zanieczyszczenie powietrza i degradacja środowiska, związana z wydobyciem i wykorzystywaniem węgla jako surowca. Węgiel jest w dalszym ciągu najważniejszym źródłem energii w Chinach. Ok. 80 % wytwarzanej energii pochodzi z tego surowca[7]. Energetyka indyjska

[4] M. Honczar, *Gazowy blitzkrieg ?*, „Wprost" 2006, nr 12, s. 54 – 57.

[5] J. Li, *Towards a low – carbon future in China's building sector – A review of energy and climate models forecast*, Energy Policy, no 36, 2008, s. 1736 – 1747.

[6] *Key World Energy Statistics 2008*, IEA, Paris 2008, s. 45.

[7] A. Bolesta, *Chiny w okresie transformacji*, Dialog, Warszawa 2006, s. 64 – 78.

w znacznym stopniu również opiera się na węglu. Indie znajdują się na trzecim miejscu pod względem wydobycia węgla (licząc razem węgiel brunatny i kamienny). Oparcie gospodarki, jak i samej energetyki na węglu determinuje wysoki poziom zanieczyszczenia powietrza. Emisja samego CO_2 w Chinach i Indiach w 2006 r. wynosiła odpowiednio 5606,54 i 1249,74 Mt[8]. Żeby znaleźć odniesienia do skali zanieczyszczenia, można te liczby porównać z emisją CO_2 przez wysoko uprzemysłowione Niemcy – 823,46 Mt. Same Niemcy ok. 50% energii uzyskują z węgla kamiennego i brunatnego. Na zanieczyszczenie powietrza w Indiach i Chinach wpływa również rozwój transportu i wzrost ilości pojazdów.

Unia Europejska, stojąc na stanowisku promocji zrównoważonego rozwoju, kładzie nacisk na zwiększenie efektywności energetycznej oraz wspieranie zróżnicowanych form energii. Istotne znaczenie ma zmniejszenie emisji gazów cieplarnianych do atmosfery. UE chce zmniejszyć emisję CO_2 pochodzącego z produkcji energii o 60% do 2050 r. Wspieranie energetyki odnawialnej nie jest jedynym rozwiązaniem, choć szczególnie widocznym i podkreślanym. UE zakłada, że do 2020 r. nastąpi wzrost udziału energii odnawialnej do 20%, a do 2030 r. – do 30%. Założenia te mogą być nie do osiągnięcia ze względu na różne poziomy rozwoju, rożne struktury energetyczne państw członkowskich, a także ze względu na problemy techniczne[9]. Inną drogą uzyskania zmniejszenia emisji GHG jest rozwój energetyki jądrowej. Niektóre kraje unijne są pod tym względem w światowej czołówce. Francja zajmuje drugie miejsce na świecie, jeśli chodzi o produkcję energii w elektrowniach jądrowych (Niemcy – czwarte) i pierwsze, jeśli chodzi o udział w produkcji krajowej energii z tego źródła (Niemcy – szóste).

Jak powiedziane było wcześniej, głównym surowcem energetycznym dla Chin jest węgiel. Przykładowo, w 2006 r. jego wydobycie wynosiło 2.38 miliarda ton, co dawało temu państwu pierwsze miejsce na świecie (stanowi to ok. 47% światowego wydobycia). Natomiast zainstalowana moc elektrowni wyniosła 622 GW – 2 miejsce po USA[10]. Przewiduje się, że do roku 2020 r. Chiny będą miały ok. 15% udział w światowej konsumpcji energii (na początku lat 70. XX wieku udział ten wynosił 5%)[11].

Wzrastające wydobycie i produkcja energii związane jest z szybkim i ciągłym rozwojem kraju. Węgiel jest, więc, ważnym elementem, który napędza chińską gospodarkę – dosłownie i w przenośni. Niewystarczająca podaż w stosunku do popytu węgla powodowała wzrost jego cen. Problemy z węglem na rynku wewnętrznym w Chinach wynikają zarówno z różnej struktury energetycznej, czy z różnych poziomów efektywności energetycznej, jak i ze sprzecznych interesów przemysłu energetycznego i wydobywczego węgla[12]. Wydaje się że sektor energetyczny zyskuje wyższą pozycję, co jest sutkiem polityki władz w zakresie kontroli cen węgla. Państwo aktywnie działa również w zakresie kontroli cen benzyny. Rozwiązywania tych problemów, mimo wprowadzanych reform, nie ułatwia polityka władz zarówno na szczeblu lokalnym, jak i centralnym.

---

[8] *Key World Energy Statistics 2008*, IEA, Paris 2008.

[9] R. Rosicki, *Europejska polityka energetyczna – między solidaryzmem a egoizmem*, w: Z. Czachór (red.), *50 lat i co dalej? Europa i Unia Europejska między integracją a atomizacją...*, UAM, Poznań 2007, s. 289 – 300.

[10] Na początku lat 50. XX wieku wydobycie węgla wynosiło ponad 60 milionów ton; pod koniec lat 70 – tych już 636 milionów ton, a w XXI wieku przekroczyło 2 miliardy ton.

[11] *China Worldwide Quest for Energy Security*, OECD/IEA, Paris 2000, s. 14.

[12] B. Wang, *An imbalanced development of coal and electricity industries in China*, Energy Policy, no 35, 2007, s. 4959 – 4968.

Wzrastające zapotrzebowanie Chin na ropę i gaz może być zagrożeniem dla UE i USA. Powoduje to konieczność poszukiwania nowych form działalności. Widoczne było to w momencie, gdy w 2005 r. jedno z chińskich przedsiębiorstw energetycznych (CNOOC) chciało wykupić amerykańską firmę (Unacal). Politycy w USA podnieśli alarm, że byłoby to zagrożenie dla bezpieczeństwa energetycznego państwa. Wynika z tego, że punkt widzenia zależy od punktu siedzenia, tzn., że jeżeli amerykańskie lub europejskie koncerny dokonują zakupu przedsiębiorstw, np. azjatyckich czy rosyjskich, to jest to wielki sukces albo wielka szansa. Gdy dzieje się to w odwrotną stronę – mówi się o zagrożeniu bezpieczeństwa energetycznego. Jak widać, globalizacja gospodarcza zaczyna przenikać w kolejne sektory, a problemy z tym związane zaczynają dotyczyć wszystkich.

W Chinach import ropy naftowej od 1993 r. wzrósł o ok. 23 %. W 2007 r. wynosił 168 Mt (ok. 4 razy mniej niż USA). Znaczna część tego surowca pochodzi z Bliskiego Wschodu, ale widoczne jest zaangażowanie Chin w poszukiwanie partnerów na innych kontynentach. Import ropy naftowej z Bliskiego Wschodu od 1993 r. rósł o 25% każdego roku[13]. Innymi kierunkami importu tego surowca są Afryka i Rosja. Surowiec ten staje się strategiczny ze względu na konieczność utrzymania rozwoju gospodarczego. Z tego względu, zabezpieczenie dostaw ropy i infrastruktury przesyłowej stanowi dla chińskiego rządu jeden z głównych elementów bezpieczeństwa energetycznego i gospodarczego. Stąd też plany rozbudowy rurociągów biegnących z obszaru Federacji Rosyjskiej i z zachodniej części kraju. Chiny dokonują inwestycji zarówno w system transportowy, jak i we własny przemysł petrochemiczny.

Na uwagę zasługuje fakt znacznego zainteresowania krajów azjatyckich rozwojem cywilnych programów atomowych, w tym rozwojem energetyki jądrowej. Plany Chin przewidują szeroki rozwój tej energetyki (osiągnięcie mocy reaktorów 40 GW do 2020 r., a do 2050 r. nawet 150 GW)[14]. Plan ten zakłada, że w 2050 r. moc chińskich reaktorów przekroczy o ⅓ obecną moc reaktorów amerykańskich. Obecnie USA są potentatem, jeśli chodzi o zaangażowanie się w energetykę atomową (reaktory o ogólnej mocy ok. 99 GW)[15]. Realizacja wspomnianego planu mogłaby ułatwić Chinom zmniejszenie zarówno zanieczyszczeń powietrza, jak i zmianę struktury produkcji energii ze względu na surowce. Tylko w 2007 r. w Chinach podłączono 1 nowy reaktor jądrowy, a rozpoczęto budowę 2 nowych. Rok wcześniej podłączono na świecie dwa nowe reaktory – jeden w Chinach, drugi w Indiach. W 2007 r. Chiny posiadały 11 reaktorów jądrowych. Należy zwrócić uwagę na wzrastającą pozycję energetyki jądrowej w całej Azji, nie tylko w Korei Południowej i Japonii. MAEA zmienia swoje przewidywania, co do trendów rozwoju tego sektora ze względu na ten obszar. Obecnie 19 z 34 budowanych reaktorów jądrowych na świecie pochodzi z tego właśnie kontynentu[16].

---

[13] Energy Asia, Vol. 13, Issue 7, 2006, s. 2.

[14] *China's Worldwide Quest for Energy Security*, OECD/IEA 2000, s. 30; *Coal in the Energy Supply of China (Report of the CIAB Asia Committee)*, OECD/IEA 1999, s. 19 – 26; *World Energy Outlook 1998*, OECD/IEA, s. 289; *Asia Electricity Study*, OECD/IEA 1997, s. 42; K. Rixin, *Nuclear Power: an indispensable power resource in China*, w: (Documents with) *19 th World Energy Congress*, Sydney – Australia 5 – 9 September 2004, s. 3 – 4.

[15] *Ochrona Środowiska 2004,* GUS, Warszawa 2004, s. 496.

[16] *Key World Energy Statistics 2008*, IEA, Paris 2008; *Nuclear Technology Review 2008*, IAEA, Vienna 2008; *Nuclear Technology Review 2007*, IAEA, Vienna 2007; *Nuclear Safety Review for the Year 2007*, IAEA, Vienna 2007.

Indie zajmują trzecie miejsce na świecie w wydobyciu węgla kamiennego (pierwsze miejsce należy do Chin i USA). W porównaniu z Chinami, Indie mają wyższy poziom importu węgla kamiennego – 4 miejsce na świecie[17]. Znaczny poziom wydobycia węgla nie oznacza, że Indie posiadają duże złoża węgla wysokojakościowego, niezbędnego dla elektrowni. Podobnie, jak w przypadku Chin, Indie planują rozbudowę potencjału energetyki jądrowej do 2020 r. (planuje się osiągnięcie mocy reaktorów na poziomie 20 GW). Obecnie Indie posiadają 17 reaktorów jądrowych, więcej niż Chiny, ale ich całościowa moc jest mniejsza o prawie połowę i wynosi 3782 MW[18]. Indie są 5 importerem ropy naftowej, czwartym importerem węgla kamiennego, oraz czwartym producentem energii elektrycznej na świecie. Zarówno Chiny, jak i Indie mają porównywalny udział energetyki wodnej w krajowej produkcji energii (ok. 15%). Z tym, że moc chińskich elektrowni wodnych wynosi 118 GW, a indyjskich 32 GW. Chiny dystansują Indie, jeśli chodzi o udziały w światowej produkcji energii przez elektrownie wodne (Chiny – 14%, Indie – 3,6%)[19]. Państwem w Europie Zachodniej, które ma zbliżony procentowy udział w produkcji energii przez tego typu elektrownie jest Norwegia.

Bezpieczeństwo energetyczne Indii wynika w głównej mierze z położenia oraz kierunków importu surowców energetycznych (Azja Środkowa, Zatoka Perska). Ważną rolę pełnią tutaj bezpieczne dostawy surowców drogą morską, co wynika z dominacji tego rodzaju transportu w Indiach. Należy zwrócić uwagę na wysoki poziom uzależnienia Indii od importu ropy naftowej. Stąd, wszelkie wahania na rynku tego surowca uderzają w określone sektory gospodarcze, szczególnie w transport, choć nie tylko. Indie w wysokim stopniu są również uzależnione od importu węgla kamiennego. Znaczna część importowanego węgla to węgiel wysokojakościowy, którego większe złoża w Indiach nie występują. Ten sam problem dotyczy gazu[20]. Indie wraz z Chinami dołączają do czołówki państw azjatyckich importujących gaz i ropę (Japonia i Korea Pd.). Państwa te odpowiadają również za kilkudziesięcioprocentowy wzrost globalnego zużycia ropy w ostatnich latach.

Struktura energetyczna UE (udział procentowy w zużyciu energii pierwotnej) jest następująca: ropa naftowa (38%), gaz (23%), paliwa stałe (18%), paliwa jądrowe (15%) i odnawialne źródła energii (6%). Plany UE przewidują znaczący wzrost udziału źródeł odnawialnych, które mogą stać się przeciwwagą dla energetyki konwencjonalnej i jądrowej. Obecnie trwa dyskusja, jakimi środkami doprowadzić do zmniejszenia zanieczyszczenia powietrza – energią zieloną, czy także jądrową. Dyskusja ta toczy się zazwyczaj, na poziomie krajowym, bowiem sama UE nie przesądza, które drogi są najlepsze. Wybór każdej ma bowiem ujemne i dodatnie strony, co zresztą podkreślają orędownicy każdej z nich. Należy zwrócić uwagę, że niektóre kraje unijne dawno już wybrały konkretną drogę. Niektóre próbują zmieniać swoją obecną strukturę energetyczną, co nie zawsze jest wynikiem analiz ekonomicznych, ale raczej decyzji politycznych. Jedno jest pewne: do 2030 r. nastąpi wzrost konsumpcji energii o 15 % (w porównaniu z 2000 r.). Dodatkowo przewiduje się, że w okresie od 2000 do 2030 r. produkcja energii

[17] *Key World Energy Statistics 2008*, IEA, Paris 2008, s. 15.
[18] *Nuclear Technology Review 2008*, IAEA, Vienna 2008.
[19] *Key World Energy Statistics 2008*, IEA, Paris 2008.
[20] Z. Shalizi, *Energy and Emissions: Local and Global Effects of the Rise of China and India*, World Bank Policy Research Working Paper 4209, April 2007.

elektrycznej wzrośnie o ok. 50%[21]. Ze względu na wzrost importu gazu i paliw zmniejszy się bezpieczeństwo energetyczne samej UE. Nastąpi więc uzależnienie od dostaw zewnętrznych. Obecnie uzależnienie UE od importu szacuje się na poziomie 50%, do 2020 r. uzależnienie to ma wzrosnąć do 60%. Największy wzrost dotyczyć będzie importu gazu[22]. Przed podobnymi problemami stoją państwa azjatyckie. Ocenia się, że jeżeli wzrost gospodarczy w Chinach będzie się utrzymywał na poziomie 8 – 9%, to uzależnienie od importu samej ropy może osiągnąć do 2030 r. poziom 80%[23].

ABSTRACT

The article will concern the relations between China, India and Europe in respect to their position. The consequence of the economic development especially in China and India is the increase in energy demand. Rich coal resources in China are not enough to satisfy a significant increase in energy demand. For instance, it is thought that the oil import in the next 20-30 years will go up by 50 %. A similar situation can be observed in India. Both countries are searching for solutions to increase their energy security. Surely, such actions do not necessarily correspond with policies of other European countries and UE. On the one hand, there is an impressive economic development of Asian countries, but on the other hand, there is a necessity to meet their demands. Economists claim that Chinese and Asian development exerts a positive influence on world economy but in the context of competition . In case of energy security, as one of the elements of national security, it does not have to have a positive effect. The position of Europe in this respect becomes unstable. It means that Europe and UE countries are one of those entities which queue for natural resources and energy and it does not necessarily mean that they have to be before Asian countries. All this has an influence on, for instance, the development of new energy technologies, searching new sources of natural resources, the increase in energy and resources prices and also on changes in energy structure (e.g. renewable or nuclear energy)

[21] *European Energy and Transport. Trends to 2030 – update 2005*, European Commision 2006, s. 7, 10; *Energy & Transport in Figures 2006 (Part 2: Energy)*, European Commission, Directorate – General for Energy and Transport, 2006.

[22] *Statistics in focus – Environment and energy*, „EUROSTAT" 2006, nr 12.

[23] Energy Asia, Vol. 13, Issue 7, 2006, s. 13.

III.
TECHNIKA, TECHNOLOGIA I BEZPIECZEŃSTWO INFORMATYCZNE

Elżbieta Ciszewska
Natalia Łepczyk

Zabezpieczenia w polskich dokumentach publicznych

Bez dokumentów życie w nowoczesnym świecie nie byłoby możliwe. Każda wizyta w banku, na poczcie czy też w urzędzie administracji publicznej, wymaga okazania dokumentu potwierdzającego naszą tożsamość. Bez tego nie można założyć konta, odebrać paczki ani zapisać się na wizytę do lekarza, nie mówiąc już o podróżowaniu.

Brak umiejętności weryfikacji podstawowych cech zabezpieczających może narazić nas na nieprzyjemności. Nie dotyczy to tylko dokumentów tożsamości, ale również znaków pieniężnych, dokumentów komunikacyjnych i innych druków specjalnych. Często słyszymy o fałszywych banknotach, jednak nikt z nas nie myśli o tym, co się stanie, jeśli taki pieniądz trafi do naszego portfela. Gorszą rzeczą jest zakup samochodu albo domu na kredyt w przypadku, gdy sprzedający posłużył się sfałszowanymi dokumentami potwierdzającymi jego tożsamość jak i dokumentami potwierdzającymi własność ruchomości bądź też nieruchomości.

Podstawowa znajomość elementów zabezpieczających stosowanych w drukach zabezpieczonych powinna być obowiązkiem każdego z nas i może nas uchronić przed stratami finansowymi oraz innymi szkodami moralnymi. Biorąc powyższe pod uwagę chcemy przybliżyć Państwu sposoby zabezpieczania druków specjalnych przed podrobieniem bądź przerobieniem. Zostaną one omówione na przykładzie polskich dokumentów powszechnie znanych i najczęściej używanych: dowodu osobistego i paszportu.

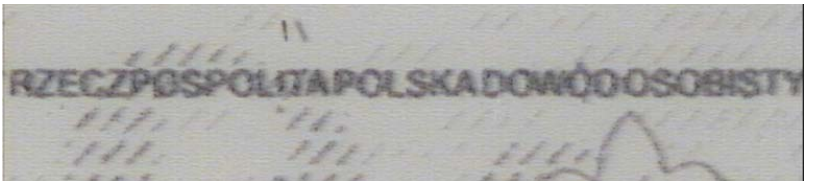
DOWÓD OSOBISTY

Dowód osobisty jest dokumentem stwierdzającym tożsamość osoby oraz poświadczającym obywatelstwo polskie [1]. Dokument ten ma postać wielowarstwowej karty z poliwęglanu w formacie ID-1 o wymiarach 53,98 mm x 85,60 mm [2, 3]. Dokument personalizowany jest za pomocą grawerowania laserowego. W trakcie procesu personalizacji dane posiadacza dokumentu oraz jego wizerunek i podpis, a także numer, data wydania i ważności dokumentu umieszczane są na dokumencie przez wypalanie (zaczernianie) uczulonego na promieniowanie laserowe poliwęglanu [2]. Data urodzenia, jako jedyna z nanoszonych podczas personalizacji danych, grawerowana jest „na wyskok", co sprawia, iż jest wyczuwalna w dotyku. Przykład spersonalizowanego blankietu polskiego dowodu osobistego przedstawiony jest na rysunku 1.

A. B.

Rys. 1. Wzór spersonalizowanego dowodu osobistego: awers (A) i rewers (B).

Awers dokumentu zadrukowany jest na całej powierzchni. Zawiera on następujące elementy graficzne: tło, cienkie linie giloszowe, godło państwowe, stylizowane litery „RP" oraz mikrodruk [3]. Elementy te nanoszone są przy zastosowaniu techniki druku offsetowego, która charakteryzuje się bardzo dobrym odwzorowaniem szczegółów oraz równomiernym rozprowadzaniem środka kryjącego. Dzięki tej technice można uzyskać cienkie, zachowujące ciągłość linie oraz płynne przejścia kolorystyczne zwane drukiem irysowym bądź też tęczowym. W przypadku polskiego dokumentu techniką tą naniesione są gilosze, czyli cienkie, ciągłe linie o płynnym przejściu kolorystycznym niebiesko - czerwono - niebieskim. Element umieszczony w górnej części karty, tuż pod napisem „REPUBLIC OF POLAND/IDENTITY CARD", wyglądający na pierwszy rzut oka jak cienka czarna linia, to mikrodruk (rys. 2), którego odczytanie wymaga odpowiedniego powiększenia.

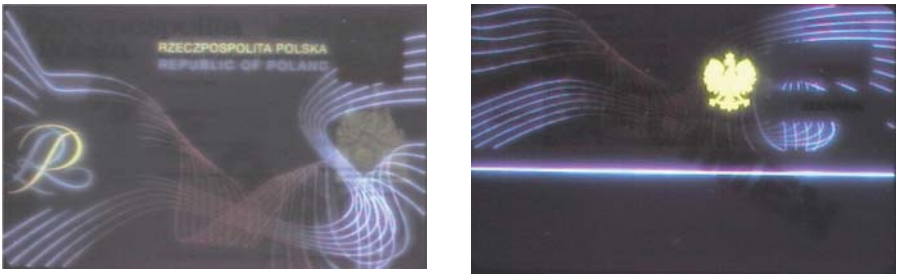


Rys. 2. Mikrodruk występujący na awersie polskiego dowodu osobistego.

Wymienione graficzne elementy protekcyjne wprowadzane są do dokumentów w celu zabezpieczenia przed kopiowaniem oraz próbami przerobienia bądź podrobienia. Przy zastosowaniu prostych metod reprodukcji nie jest możliwe wierne odtworzenie subtelnych szczegółów druku, dlatego dokumenty sfałszowane często zawierają np. nieczytelny mikrodruk.

Farby zastosowane do nadrukowania giloszy mają właściwości fluoryzujące – w promieniowaniu ultrafioletowym (UV) wykazują barwne świecenie. Ponadto, w świetle UV ujawnia się obecność napisów i elementów naniesionych farbami niewidocznymi w świetle dziennym (rys. 3A). Szczególnie ważnym elementem zabezpieczającym są naniesione w polu zdjęcia stylizowane litery „RP" umieszczone tam z powodu dużego narażenia zdjęcia posiadacza na ataki fałszerzy.

A. B.



Rys. 3. Dowód osobisty w promieniowaniu ultrafioletowym: awers (A) i rewers (B).

W dolnym rogu karty występuje kinegram, czyli zabezpieczenie stanowiące rodzaj dyfrakcyjnego elementu optycznie zmiennego [2]. Umieszczony jest on pomiędzy poszczególnymi warstwami dokumentu, dzięki czemu nie jest narażony na uszkodzenia i próby usunięcia a następnie ponownego wykorzystania. W zależności od kąta obserwacji ujawniane zostają naprzemiennie stylizowane litery „RP" oraz kontury mapy Polski wraz z mikrodukiem. Kinegram jest dodatkowo spersonalizowany poprzez wygrawerowanie w jego polu numeru dowodu osobistego oraz terminu jego ważności. Przykład spersonalizowanego kinegramu przedstawiony jest na rysunku 4.

Rys. 4. Kinegram występujacy na awersie polskiego dowodu osobistego

Rewers dokumentu pod względem graficznym zabezpieczony jest analogicznie do awersu. W tle o przejściu barw z czerwonej do szarej znajduje się gilosz w tych samych odcieniach, co na awersie. Linie giloszowe, podobnie jak na awersie, w ultrafiolecie fluoryzują (rys. 3B).

Zadruk farbami widocznymi w świetle dziennym to jedynie nieco ponad połowa powierzchni rewersu. Dolną jego część stanowi białe pole (MRZ, *ang.* ***M****achine* ***R****eadable* ***Z****one*) przeznaczone do odczytu maszynowego [3]. Dzięki jego obecności możliwe jest używanie dowodu osobistego jako dokumentu podróży. W polu tym umieszczone są trzy linie, po 30 znaków każda, w których naniesione są dane indywidualne dla każdego dokumentu. Znaki te zapisywane są specjalną czcionką o kroju OCR-B. W kolejnych liniach zawarte są:

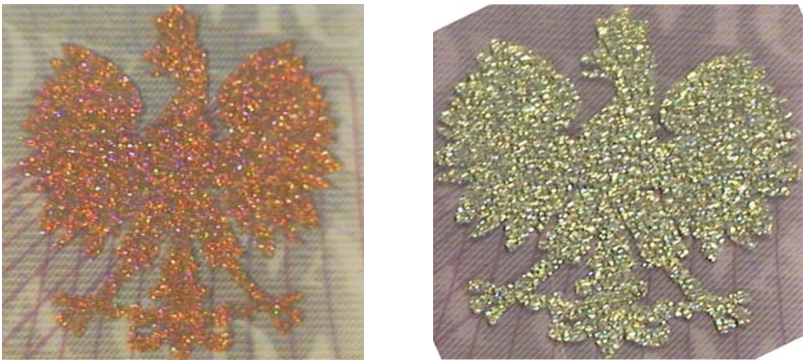
- w pierwszej: kod dokumentu, kod kraju wydającego dokument, seria i numer dokumentu oraz cyfra kontrolna;
- w drugiej: data urodzin posiadacza, oznaczenie płci, termin ważności dokumentu, narodowość oraz cyfry kontrolne;
- w trzeciej: nazwisko i imię posiadacza.

Wspomniane cyfry kontrolne obliczane są za pomocą specjalnego algorytmu, a ich obecność ma na celu potwierdzenie autentyczności danych zapisanych w polu MRZ.

Wszystkie znaki znajdujące się w polu przeznaczonym do odczytu maszynowego wprowadzane są do dokumentu, podobnie jak pozostałe dane posiadacza w trakcie jego personalizacji przy zastosowaniu techniki grawerowania laserowego.

Pole przeznaczone do odczytu maszynowego oddzielone jest od strony z danymi posiadacza białą nitką zabezpieczającą, fluoryzujacą w świetle UV na niebiesko (rys. 3B).

Ciekawym zabezpieczeniem optycznym jest wizerunek orła w koronie wykonany farbą optycznie zmienną naniesioną za pomocą techniki sitodruku. Farba optycznie zmienna (OVI, *ang.* ***O****ptically* ***V****ariable* ***I****nk*) to farba specjalna wykorzystywana do zabezpieczania dokumentów podróży, tożsamości, komunikacyjnych, banknotów i innych druków zabezpieczonych. Farba wykazuje charakterystyczną, płynną zmianę barwy w zależności od kąta obserwacji lub oświetlenia [4]. W polskim dowodzie osobistym jest to przejście kolorystyczne od czerwieni, poprzez złoto, do zieleni (rys. 5.).



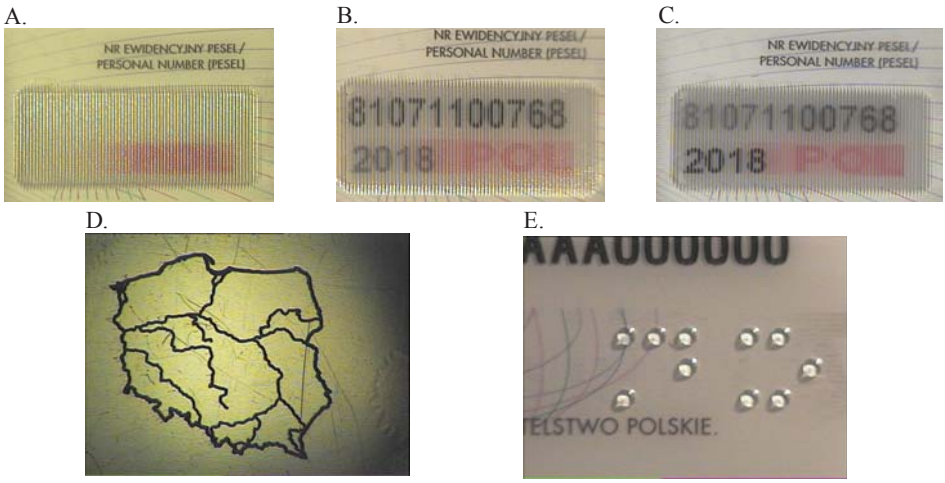
Rys. 5. Wizerunek orła nadrukowany farbą optycznie zmienną w polskim dowodzie osobistym.

Zastosowana w dokumencie farba optycznie zmienna dodatkowo wykazuje fluorescencję w promieniowaniu UV. W przypadku dowodów z początkowej fazy produkcji jest to świecenie niebieskie, natomiast żółte w dowodach pozostałych. Przykłady dwóch kolorów fluorescencji orła wykonanego farbą OVI przedstawione są na rysunku 6.

A. B.

Rys. 6. Wizerunek orła w promieniowaniu ultrafioletowym: dokumenty z początkowej fazy produkcji (A) i pozostałe (B).

Na rewersie dowodu osobistego umieszczone zostały trzy elementy zabezpieczające, wyczuwalne w dotyku. Są to tłoczone kontury mapy Polski wraz z głównymi rzekami, znaki zapisane alfabetem Braille'a oraz najważniejszy z nich – personalizowany CLI (ang. ***C****hangeable* ***L****aser* ***I****mage*). Numery znajdujące się w CLI są grawerowane podczas personalizacji dokumentu. W zależności od kąta obserwacji widać wyraźniej jeden z nich. Przykład niespersonalizowanego CLI wraz z wygrawerowanym numerem PESEL oraz rokiem, w którym upływa termin ważności dokumentu, przedstawiony jest na rysunku 7.



Rys. 7. Elementy wyczuwalne w dotyku na rewersie: niespersonalizowane CLI (A); spersonalizowane CLI (B, C); tłoczona mapa Polski (D); znaki zapisane alfabetem Braille'a (E).

PASZPORT

Drugim ważnym dla obywatela dokumentem jest paszport. Dokument paszportowy uprawnia do przekraczania granicy i pobytu za granicą oraz poświadcza obywatelstwo polskie, a także tożsamość osoby w nim wskazanej w zakresie danych, jakie ten dokument zawiera [5]. Rozróżnia się następujące dokumenty paszportowe: paszport, paszport tymczasowy, paszport dyplomatyczny, paszport służbowy Ministerstwa Spraw Zagranicznych.

Wszystkie paszporty występują w formie książeczek w formacie ID-3 (125 x 88 mm) [2]. Każdy z nich zawiera w zależności od rodzaju dokumentu różną ilość stron wizowych oraz stronę z danymi osobowymi.

Najbardziej popularnym dokumentem jest paszport zwykły dla obywatela, który od 28 sierpnia 2006 roku jest wyposażony w elektroniczny nośnik danych biometrycznych – bezkontaktowy mikroprocesor z anteną. Są tu przechowywane umieszczone na stronie personalizacyjnej dane o posiadaczu dokumentu wraz z kolorowym zdjęciem (I cecha biometryczna) i skanem podpisu, a od dnia 29 czerwca 2009 roku również obraz linii papilarnych dwóch palców (II cecha biometryczna). Poszczególne elementy książeczki paszportowej to:

1. Okładka dokumentu,
2. Wyklejka,
3. Strona personalizacyjna,
4. Strony wizowe,
5. Nić do zszycia dokumentu,
6. Inlet – wkładka zawierająca mikroprocesor.

1. Okładka dokumentu

Okładka paszportowa jest w kolorze bordowym. Centralnie na pierwszej stronie umieszczone są złocenia: napisy, różne w zależności od przeznaczenia dokumentu,

oznaczenie informujące, iż jest to dokument biometryczny oraz wizerunek orła w koronie. Dodatkowym elementem zabezpieczającym okładkę jest bieżący wzór widoczny tylko w promieniowaniu UV. Fragmenty okładki w świetle widzialnym i ultrafioletowym przedstawione są na rysunku 8.

A. B.

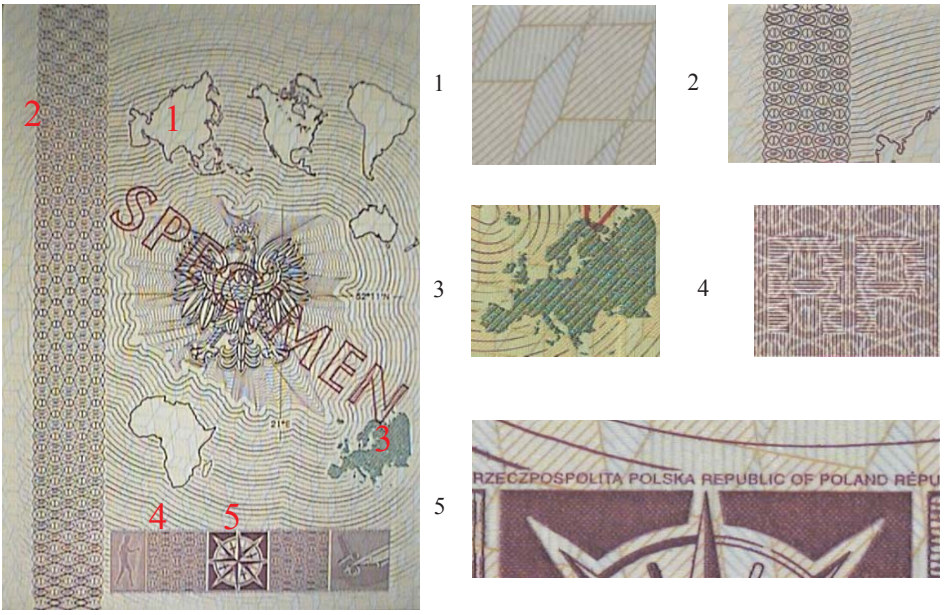
Rys. 8. Zdjęcie fragmentu okładki paszportu: w świetle dziennym (A) i w promieniowaniu ultrafioletowym (B).

2. Wyklejka

Strona wyklejkowa wykonana jest z papieru niewykazującego luminescencji w promieniowaniu UV, niezawierającego znaku wodnego, wykazującego się charakterystyczną reaktywnością w kontakcie z odczynnikami chemicznymi. Papier zabezpieczony jest także włóknami specjalnymi. W świetle dziennym w strukturze papieru widoczne są włókna w kolorze granatowym. W promieniowaniu UV część granatowych włókien wykazuje niebieską luminescencję. Są tu także włókna niewidoczne w świetle dziennym, aktywne w promieniowaniu UV, świecące na czerwono oraz zielono. Przykłady włókien widocznych we fragmencie strony wyklejkowej w promieniowaniu UV przedstawione są na rysunku 9.

Rys. 9. Włókna zabezpieczające widoczne w promieniowaniu ultrafioletowym na stronie wyklejkowej.

Zabezpieczenia graficzne, znajdujące się na pierwszej części strony wyklejkowej wyszczególnione są na rysunku 10. Jest to giloszowe tło nadrukowane techniką offsetową oraz elementy wklęsłodrukowe. Wśród elementów wykonanych techniką stalorytu najciekawszym zabezpieczeniem jest efekt kątowy (rys. 10.3). Jest to wzór złożony z wypukłych linii przecinających się pod kątem prostym, uwidaczniający dany motyw, wykorzystujący efekty światła i cienia [2]. W zależności od kierunku padania światła widoczne są litery „RP" jako jasne na ciemnym tle lub odwrotnie. Na stronie znajduje się ponadto element (mapa Europy) naniesiony techniką stalorytu, wykonany farbą optycznie zmienną, wykazujący przejście kolorystyczne od zieleni do fioletu.



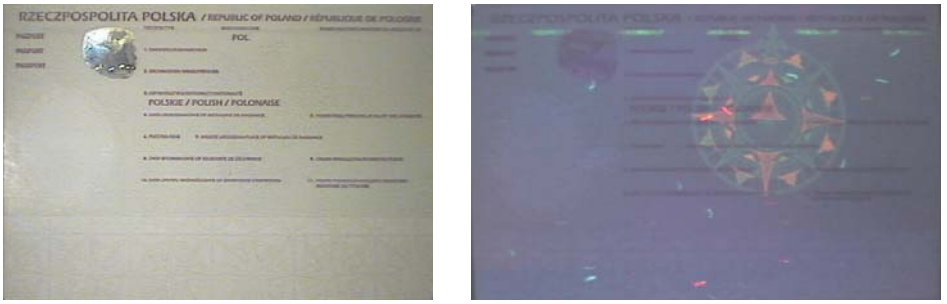
Rys. 10. Fragment strony wyklejkowej oraz wyszczególnione elementy graficzne: tło giloszowe (1), element stalorytniczy (2), efekt kątowy (4) i mikrodruk (5) wykonane techniką stalorytniczą oraz element nadrukowany farbą optycznie zmienną (3).

3. Strona personalizacyjna

Struktura strony personalizacyjnej różni się od pozostałych stron paszportu. Składa się ona z papieru zalaminowanego dwustronnie w folię wykonaną z poliwęglanu przystosowanego do grawerowania laserowego. Papier ten zabezpieczony jest chemicznie przed próbami przerobienia (jest reaktywny na działanie odczynników chemicznych). Wzór niespersonalizowanej strony personalizacyjnej znajduje się na rysunku 11.

Papier stanowiący rdzeń karty zadrukowany jest dwustronnie techniką offsetową z zastosowaniem techniki druku irysowego oraz elementami mikrodruku. Ponadto, napis „Rzeczpospolita Polska" w górnej części karty wykonany został techniką sitodruku przy wykorzystaniu farby OVI. Wykazuje ona w zależności od kąta obserwacji płynne przejście kolorystyczne od fioletu do zieleni. Na stronie znajduje się również niewidoczny w świetle dziennym, a wykazujący w promieniowaniu UV kolorowe świecenie nadruk w postaci Róży Wiatrów.

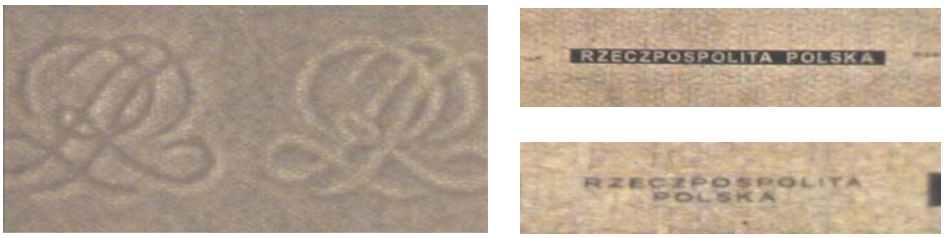
A. B.



Rys. 11. Wzór niespersonalizowanej strony z danymi osobowymi: w świetle dziennym (A); w promieniowaniu ultrafioletowym (B).

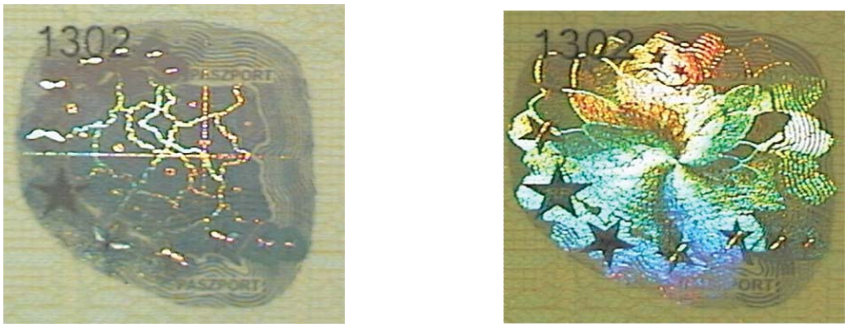
Papier zawiera włókna niewidoczne w świetle dziennym, świecące w ultrafiolecie na zielono i czerwono. Posiada również umiejscowiony, dwutonalny znak wodny oraz częściowo demetalizowaną nitkę zabezpieczającą. W nitce tej znajduje się również pozytywowy i negatywowy mikrodruk („Rzeczpospolita Polska") biegnący w powtarzających się blokach. Napis ten wprowadzony jest prawo- i lewoczytelnie. Elementy te znajdują się na rysunku 12. W promieniowaniu ultrafioletowym nitka wykazuje segmentową luminescencję w kolorach czerwonym i zielonym (rys. 11B).

A. B.



Rys. 12. Elementy zabezpieczające znajdujące się w strukturze papieru użytego do produkcji strony personalizacyjnej: znak wodny (a) i nitka zabezpieczająca (B).

Tuż nad polem zdjęciowym naniesiony jest hologram przedstawiający otoczony gwiazdkami kontur Polski, zawierający w swoim wnętrzu wizerunek orła w koronie (rys. 13)



Rys. 13. Hologram występujący na stronie personalizacyjnej polskiego paszportu.

4. Strony wizowe

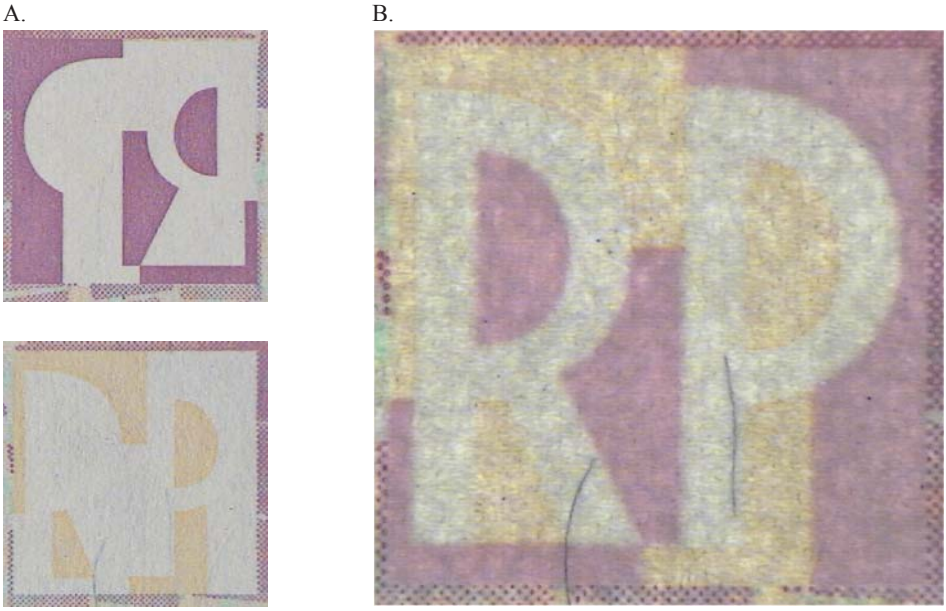
W polskim paszporcie dla obywatela umieszczono 40 stron wizowych. Zostały one wydrukowane na papierze zabezpieczonym włóknami, podobnie jak na stronie wyklejkowej: granatowymi w świetle dziennym, z których część wykazuje niebieską fluorescencję w UV oraz niewidocznymi w świetle dziennym, świecącymi w ultrafiolecie na czerwono i zielono. Papier jest reaktywny na działanie odczynników chemicznych. Każda kartka zawiera wielotonalny, umiejscowiony znak wodny w postaci orła w koronie, na przemian negatywowego i pozytywowego. W strukturze każdej kartki znajduje się podobni jak na stronie personalizacyjnej, częściowo zdemetalizowana nitka zabezpieczająca, z pozytywowo – negatywowym, prawo i lewoczytelnym mikrodrukiem „Rzeczpospolita Polska". Fragment strony wizowej widocznej w świetle przechodzącym, przedstawiono na rysunku 14. W promieniowaniu ultrafioletowym nitka wykazuje segmentową fluorescencję w kolorach czerwonym i zielonym (rys. 15).

Rys. 14. Zdjęcie fragmentu strony wizowej polskiego paszportu wykonane w świetle przechodzącym, ukazujące wielotonalny umiejscowiony znak wodny i nitkę zabezpieczającą.

Pod względem graficznym każda strona jest inna, przy czym linie giloszy wraz z mikrodrukiem stanowią pastelowe tło. W projekt każdej ze stron wizowych wkomponowano jej numer. Ponadto, na wybranych stronach wizowych w promieniowaniu ultrafioletowym ujawniają się elementy graficzne w kolorach pomarańczowym i zielonym. Taką samą fluorescencję wykazuje także numer strony. Przykład jednej z nich jest przedstawiony na rysunku 15.

Dodatkowym zabezpieczeniem graficznym umiejscowionym na stronach wizowych jest recto – verso. Jest to uzupełniający się obraz, złożony z motywów wydrukowanych pozornie bezładnie na przednim i tylnym fragmencie podłoża. W świetle przechodzącym motywy te dokładnie do siebie pasują i tworzą kompletny obraz [2]. Recto – verso umieszczone w polskim paszporcie przedstawione jest na rysunku 16.

Rys. 15. Strona wizowa nr 33: widoczna w świetle dziennym (A) i promieniowaniu ultrafioletowym (B).



Rys. 16. Zabezpieczenie recto – verso obecne w polskim paszporcie: elementy na przednim i tylnym fragmencie podłoża (A); obraz kompletny, widoczny w świetle przechodzącym (B).

Wszystkie elementy graficzne, tj. tło giloszowe z elementami mikrodruku, numery poszczególnych stron, teksty wykonane wiśniową farbą, elementy widoczne tylko w promieniowaniu UV oraz recto – verso nadrukowane są przy zastosowaniu techniki offsetu.

Na pierwszej stronie wizowej umieszczono serię i numer dokumentu składający się z dwóch liter i siedmiu cyfr. W dokumentach zabezpieczonych numery nadrukowuje się stosując technikę druku wypukłego. Jej cechy charakterystyczne to wgłębienia wytłoczone w podłożu. Zastosowany do tego środek kryjący penetruje podłoże na czerwono. W promieniowaniu UV wykazuje zieloną fluorescencję. Przykładowy numer przedstawiono na rysunku 17.

A. B. C.

Rys. 17. Przykładowa numeracja dokumentu: widoczna w świetle dziennym (A); w promieniowaniu UV (B); na odwrocie kartki (C).

Dodatkowym zabezpieczeniem polskiego paszportu jest perforacja laserowa, powtórzona na każdej stronie wizowej łącznie z tylną okładką. Numer ten powstaje poprzez przepalanie podłoża za pomocą lasera. Zabezpieczenie charakteryzuje się śladami zażółcenia widocznymi na brzegach otworów oraz tym, iż perforowane otwory zmniejszają się stożkowo od przodu ku tyłowi książeczki [2]. Na rysunku 18 przedstawiono przykład perforacji laserowej na pierwszej stronie wizowej i tylnej części wyklejki. Wyraźnie widoczna jest różnica w średnicy otworów pomiędzy pierwszą stroną wizową, a tylną wyklejką dokumentu paszportowego.

A. B.

Rys. 18. Numeracja laserowa polskiego paszportu: pierwsza strona wizowa (A); tylna część wyklejki (B).

5. Nić introligatorska

Nić introligatorska w paszporcie służy do zespolenia stron wizowych oraz strony personalizacyjnej z wyklejką. W polskim paszporcie nić jest spleciona z dwóch różnych nitek: białej, wykazującej niebieską fluorescencję w ultrafiolecie oraz czerwonej, świecącej w UV na czerwono. Fragment szycia dokumentu przedstawiony jest na rysunku 19.

A. B.

Rys. 19. Fragment szycia dokumentu: widok w świetle dziennym (A) i w ultrafiolecie (B).

Podsumowanie

Niniejszy artykuł miał na celu zapoznanie czytelników z podstawowymi zabezpieczeniami stosowanymi w najważniejszych dokumentach publicznych – dowodzie osobistym i paszporcie. Omówiona została jedynie część zabezpieczeń, pozwalająca na weryfikację autentyczności dokumentu każdej osobie bez używania specjalistycznych urządzeń. Oprócz zabezpieczeń tu wymienionych, w dokumentach znajdują się także inne elementy, których obecność jest możliwa do stwierdzenia jedynie w wyspecjalizowanych laboratoriach.

Literatura

1. *Ustawa z dn. 10.04.1974 r. o ewidencji ludności i dowodach osobistych* (Dz. U. nr 14, poz. 85).
2. Glosariusz Rady UE, *Dokumenty zabezpieczone, zabezpieczenia i inne powiązane terminy techniczne*.
3. ICAO Doc 9303, *Machine Readable Ravel Documents*, część 3;
4. *Pigmenty specjalne. Postęp technologiczny w służbie fałszerzy*, Prezentacja wygłoszona na XIII Sympozjum Ekspertów Badań Dokumentów, Polańczyk, 06--10.10.2008 r.;
5. *Ustawa z dn. 13.07.2006 r. o dokumentach paszportowych* (Dz. U. nr 143, poz. 1027).

ABSTRACT

This article aims to familiarize its readers with the basic security features used in official documents such as identity card or passport. These documents allow to confirm our identity, citizenship and are required during crossing a border. It might also be necessary to have a personal identity card or passport during certain transactions. Inability to verify security features of the aforementioned documents may be a cause of various problems, including financial losses.

Waldemar Maciejko

Zastosowanie automatycznego rozpoznawania mówców w kryminalistyce

Wprowadzenie

Rozpoznawanie przez człowieka znanych mu osób na podstawie ich głosu jest rzeczą naturalną. Powszechność tego zjawiska powoduje, iż człowiek świadomie nigdy nie analizuje cech głosu, które wpłynęły na proces percepcji. Próba zautomatyzowania tej czynności uświadamia nam, jak skomplikowany jest to proces. Współczesne aplikacje automatycznego rozpoznawania mówców są systemami informatycznymi, wykorzystującymi wiedzę z dziedziny elektroakustyki, akustyki słuchu i mowy, statystki oraz rachunku prawdopodobieństwa.

Podział systemów automatycznych

Rozpoznawanie mówcy jest pojęciem szerokim, które obejmuje m.in. identyfikację oraz weryfikację. W procesie identyfikacji tożsamość nie jest wstępnie deklarowana a mówca, którego głos podlega badaniu, może być już uprzednio zarejestrowany w systemie (tzw. identyfikacja w zbiorze zamkniętym) lub jest kimś zupełnie nie znanym dla systemu (identyfikacja w zbiorze otwartym). Zadanie weryfikacji natomiast polega na rozstrzygnięciu, czy badana wypowiedź należy do mówcy o deklarowanej tożsamości.

Systemy automatycznego rozpoznawania mówców można podzielić również na zależne i niezależne od tekstu. Zależność od tekstu oznacza, że w trakcie próby rozpoznania wymaga się, aby osoba rozpoznawana wypowiedziała słowa, które wystąpiły w sekwencji uczącej (wzorcowej). Jeżeli natomiast w wypowiedzi znajdują się dowolne słowa (stawia się jedynie wymagania co do długości wypowiedzi oraz jakości nagrania), to mówimy o systemach niezależnych od tekstu. Rozpoznanie zależne od tekstu wymaga użycia bardzo złożonych obliczeniowo algorytmów, przy czym skuteczność tych dwóch różnych metod jest zbliżona [Reynolds, D. A., 1995]. W niniejszej pracy skupiono się na systemach niezależnych od tekstu, ponieważ są najbardziej rozpowszechnione oraz - zgodnie z danymi publikowanymi przez NIST[1)] – są najbardziej efektywne pod względem osiąganych rezultatów przy minimalnej złożoności obliczeniowej[2)].

Automatyczne rozpoznawanie osób znajduje zastosowanie w systemach chroniących dostęp do zastrzeżonych usług, realizacji operacji finansowych w banku za pośrednictwem telefonu, kontroli dostępu do systemów zarządzania, systemów dowodzenia i chronionych stref w budynkach itp.

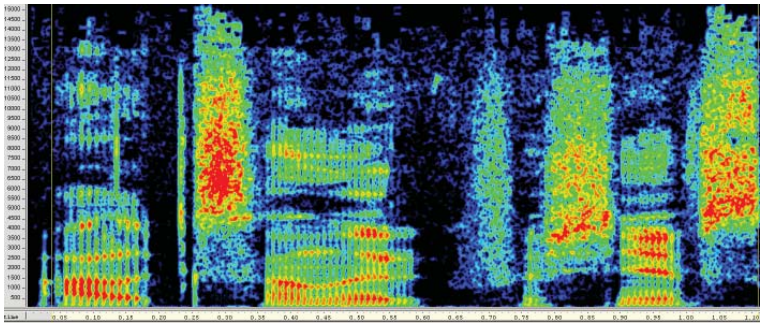
[1)] Narodowy Instytut Standaryzacji i Technologii (ang. *National Institute of Standards and Technology – NIST*) – w ramach NIST prowadzone są coroczne badania międzylaboratoryjne producentów systemów automatycznego rozpoznawania mówców. Celem tych badań jest określenie najlepszej metody identyfikacji poprzez porównanie wyników osiągniętych przez systemy poszczególnych laboratoriów [itl.nist.gov].

[2)] Złożoność obliczeniowa – odpowiada na pytanie; jak czas wykonania algorytmu (przez komputer) będzie rósł wraz ze wzrostem ilości danych wejściowych. Pojęcie to określa szybkość wykonania algorytmu [Szwabiński, J., 2006].

Automatyczne rozpoznawanie mówców zajęło szczególnie ważne miejsce w kryminalistyce i sądownictwie. W przypadku, gdy treści zarejestrowanych wypowiedzi stanowią naruszenie prawa (np. groźby karalne) lub jest mowa o przestępczym działaniu (np. kradzież, zamach terrorystyczny), nagranie takie może stanowić dowód w sprawie, o ile podejrzany o te działania zostanie lub nie zostanie na podstawie głosu zidentyfikowany.

Metody rozpoznawania mówców

Pierwsze próby rozpoznawania głosów w inny sposób, niż za pomocą słuchu, prowadzono w latach sześćdziesiątych. Metody te bazowały na subiektywnym porównaniu obrazów wypowiedzi, tak zwanych spektrogramów (rys.1). Każdy spektrogram zawiera dużą ilość użytecznych informacji w układzie współrzędnych czas – częstotliwość – amplituda [Kersta, L.G., 1962].



Rys. 1. Spektrogram wypowiedzi „Aleksander”

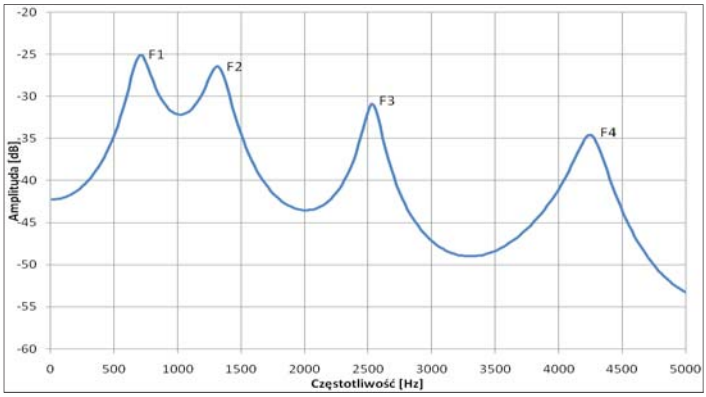
Możliwość zidentyfikowania mówcy jedynie na podstawie spektrogramu szybko jednak podważono. Jednocześnie prowadzono badania nad możliwością zastosowania parametrów takich, jak ton krtaniowy oraz częstotliwości formantowe. Ton krtaniowy jest to częstotliwość drgań wiązadeł głosowych. Natomiast częstotliwości formantowe są to wartości maksymalne w widmie samogłosek, powstałe na skutek formowania dźwięku przez układ artykulacyjny człowieka (rys. 2).

Badaniami podstawowych parametrów w dziedzinie częstotliwości, jakimi są ton krtaniowy oraz częstotliwości formantowe, zajął się między innymi Wiktor Jassem z Polskiej Akademii Nauk. Wyniki opublikował w 1973 r. jednoznacznie stwierdzając, iż częstotliwości formantowe są parametrami, które z bardzo dużym prawdopodobieństwem różnicują mówców [Jassem W., 1973].

Częstotliwości formantowe oraz ton krtaniowy stosowane są szeroko do dnia dzisiejszego. Pojawienie się szybkich komputerów pozwoliło na powszechne wykorzystanie dyskretnych metod analizy sygnału (realizowalnych jedynie przy pomocy maszyn cyfrowych). W roku 1963 amerykańscy naukowcy B.P. Bogert, M.J.R. Healy oraz J.W. Tukey zaproponowali tzw. cepstralną analizę sygnału [Bogert B.P., 1963]. Teoretyczne założenie analizy cepstralnej opiera się na możliwości zamiany operacji mnożenia sygnałów w ich sumowanie i w efekcie rozdzielenie[3)]. Dzięki temu parametry anali-

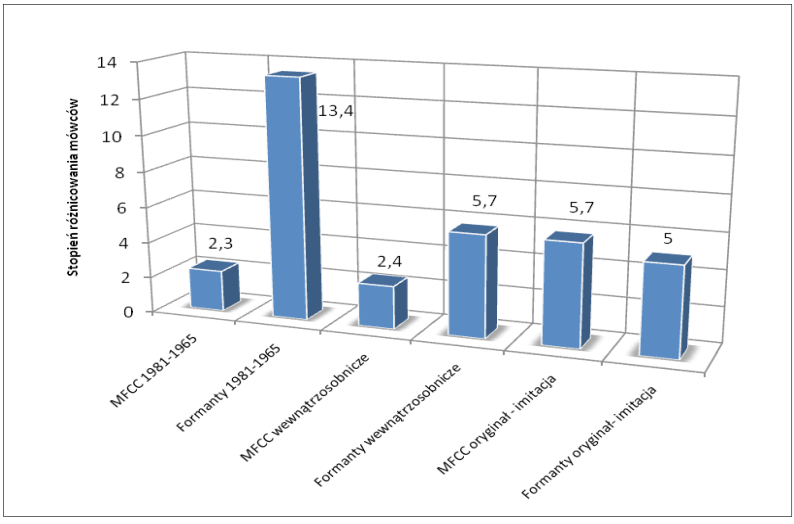
[3)] Chodzi o własność logarytmu: logarytm z iloczynu liczb to suma logarytmów tych liczb.

zy cepstralnej okazały się istotnie odporne na zakłócenia w kanale transmisji. Okazało się również, że są to wartościowe parametry, jeżeli chodzi o rozpoznawanie mówców.



Rys. 2. Widmo głoski /a/ we frazie /aleks/ otrzymane w wyniku zastosowania LPC[4]. Widoczne maksyma to częstotliwości formantowe.

Wykres na rys. 3 przedstawia porównanie możliwości różnicowania osób poprzez parametry cepstralne (MFCC) oraz formanty. Do badań wykorzystano trzy bazy głosów. Pierwsza baza zawierała głosy tych samych mówców zarejestrowane w roku 1965 oraz 1981. Kolejna składała się z głosów tych samych mówców nagrywanych co kilkadziesiąt dni na przestrzeni około 6 miesięcy. Za pomocą tej bazy oceniono średnie wahania wewnątrzosobnicze. Trzecia baza to wypowiedzi mówców oryginalnych oraz ich imitatorów. Porównań dokonano na tych samych wypowiedziach. Jako stopień różnicowania mówców przyjęto odległość Bhattacharyya [Malegaonkar A., 2008].



Rys. 3. Porównanie możliwości różnicowania głosów poprzez częstotliwości formantowe oraz parametry MFCC [Maciejko W., 2005].

[4] LPC – liniowe kodowanie predykcyjne to metoda stosowana m.in. do obliczania widma sygnału (praktycznych zastosowań tej metody jest wiele, np. kompresja dźwięku, kodowanie głosu do celów transmisji GSM itp.)

Pierwsza baza posłużyła do oceny, jak wielkim zmianom ulegną parametry na długiej przestrzeni czasowej (16 lat). Ze względu na to, że porównywano wypowiedzi tych samych osób, spodziewać się należy, iż zaobserwowane różnice pomiędzy głosami będą niewielkie.

W przypadku parametrów cepstralnych wynoszą one średnio 2,3[5], tymczasem dla formantów aż 13,4. Odnosząc to do obserwowanych średnich zmian wewnątrzosobniczych, opierając się na formantach, stwierdzonoby, iż analizie poddano głosy różnych mówców. Zbadano również, na ile wyćwiczony imitator jest w stanie naśladować widmowe cechy głosu. Również w tym przypadku parametry cepstralne okazały się skuteczniejsze.

Dzięki temu, że obliczenia MFCC dokonuje się z całych wypowiedzi (formanty realizowane są w obrębie głosek dźwięcznych), dużo łatwiejsze stało się zautomatyzowanie operacji obliczenia cech osobniczych mówcy. Analiza cepstralna generuje „obraz" mówcy w postaci setek kolumn liczb. Pojawił się zatem kolejny problem: w jaki sposób dokonać porównania dwóch modeli mówców, zakodowanych w ogromnej ilości danych. Tak więc na przestrzeni ostatnich 20 lat rozwijano algorytmy, które na podstawie nagranych głosów nie tylko obliczą cechy osobnicze, ale również będą samodzielnie wnioskować o tożsamości mówców. W te badania zaangażowało się wiele uznanych laboratoriów (takich jak MIT Lincoln Laboratory, Bell Telephone Laboratories). Przetestowano wiele metod modelowania oraz wnioskowania, takich jak sieci neuronowe, niejawne modele Markowa, metody nieparametryczne (kwantyzacja wektorowa, najbliższy sąsiad, najbliższa średnia). Dziś, ze względu na bardzo dużą efektywność, w centrum uwagi badaczy znalazły się tzw. metody modelowania parametrycznego, w których wynikiem rozpoznania jest prawdopodobieństwo, że dana wypowiedź została wyartykułowana przez określoną osobę. Podstawą tych algorytmów jest podejście bayesowskie. Można powiedzieć, że dobrze znany wzór Bayesa stał się podstawą do rozwoju teorii i algorytmów różnych form wnioskowania probabilistycznego [Cichosz P. (2000)].

Jedną z najchętniej stosownych metod modelowania parametrycznego mówców jest tzw. kombinacja modeli normalnych (ang. *gaussian mixture models* - GMM). Systemy rozpoznawania tego typu od kilku lat zapewniają uzyskanie najlepszych wyników spośród wszystkich metod rozpoznawania [Reynolds, 1995][6].

Kolejnym elementem systemu automatycznego podwyższającym skuteczność, niezbędnym w praktyce kryminalistycznej, jest moduł kompensujący cechy osobnicze oraz normalizujący kanał transmisji. W praktyce kryminalistycznej najczęściej porównuje się głosy nagrywane w różny sposób, często nieznany dla eksperta w trakcie prowadzenia badań. W celu zminimalizowania wpływu właściwości kanału transmisji na cechy osobnicze głosu, stosuje się jednocześnie wiele metod. Jedna z nich to specjalny rodzaj filtracji, która realizowana jest w oparciu o parametry cepstralne. Polega ona na odejmowaniu uśrednionej charakterystyki współczynników cepstrum, których wartości zmieniają się wolniej niż cepstrum sygnału mowy[7]. Inne popularne metody służące do normalizacji to stosowanie parametrów liniowego kodowania perceptualnego [Hermansky, H., 1994] oraz statystyczna kompensacja cech osobniczych. Ostatnia

[5] Odległość Bhattacharyya - jest miarą stosowaną w statystyce do oszacowania różnicy między dwoma rozkładami prawdopodobieństwa. W analizowanym przypadku zastosowano wzór na n – wymiarowy rozkład normalny. Odległość należy interpretować w ten sposób, że: im miara odległości jest większa, tym różnica pomiędzy głosami jest większa.

[6] Celem nie jest szczegółowe opisanie wspominanych metod, przekraczałoby to znacznie ramy niniejszej pracy. Zainteresowanych odsyłam do literatury wymienionej na końcu.

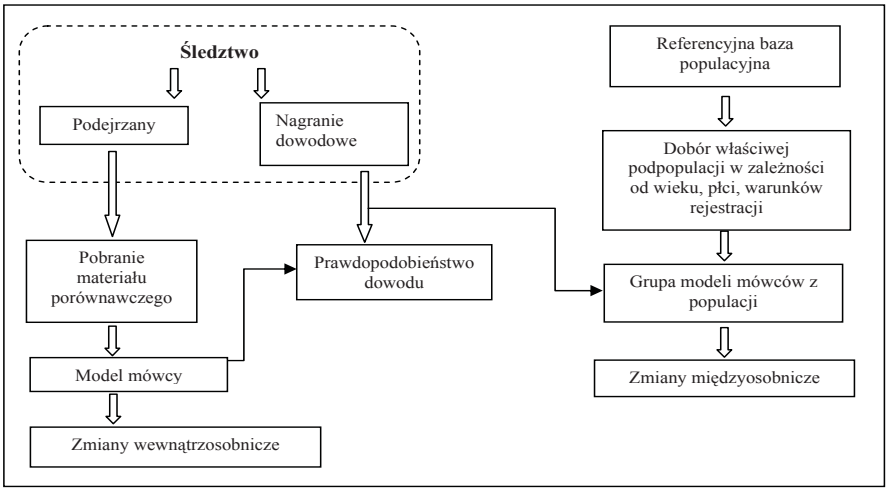
[7] Metoda CMS (ang. *Cepstral Mean Substraction*).

z wymienionych metod polega na empirycznej obserwacji tego, jak zmieniają się parametry osobnicze na grupie mówców referencyjnych (w praktyce około 10 osób) pod wpływem danego rodzaju transmisji, a następnie zmiana cech głosów zniekształconych o zaobserwowane wartości.

Automatyczne rozpoznawanie mówców w kryminalistyce

Metody automatycznego rozpoznawania mówców znalazły zastosowanie przede wszystkim w identyfikacji kryminalistycznej. Dzięki temu, iż badania przy ich pomocy są w pełni obiektywne oraz pozwalają na identyfikację na podstawie krótkich (kilkunastosekundowych) wypowiedzi, uzupełniają powszechnie stosowane metody językowe[8)].

Na rysunku 4 przedstawiono poglądowy schemat automatycznego systemu rozpoznawania mówców. Jednym z elementów tego systemu jest populacyjna baza głosów, która wykorzystywana jest do oceny zmian międzyosobniczych. Taka baza zawiera głosy, które powinny być maksymalnie zbliżone do głosu nagrania dowodowego.



Rys. 4. Podstawowy schemat pracy automatycznego systemu rozpoznawania mówców [Gonzalez - Rodriguez J., 2003].

Na pierwszym etapie procesu porównania tworzone są modele głosów osoby podejrzanej oraz model populacyjny. Na model mówcy (lub model populacyjny), w przypadku wspomnianego wyżej algorytmu GMM, składają się wartości średnie, odchylenie standardowe oraz wagi poszczególnych parametrów. Na drugim etapie obliczane są prawdopodobieństwa wystąpienia cech głosu z nagrania dowodowego w modelu mówcy podejrzanego oraz populacji. Iloraz tych prawdopodobieństw to tzw. iloraz wiarygodności, oznaczany jako LR. Wartość LR mówi, ile razy prawdopodobieństwo tego, że mówca w nagraniu dowodowym i porównawczym to ta sama osoba jest większe od prawdopodobieństwa, że jest to inny mówca.

[8)] Celem analizy językowej jest wyszczególnienie zestawu cech i parametrów indywidualizujących poszczególne osoby.

Zakończenie

W ciągu ostatnich kilku lat można zaobserwować zintensyfikowane działania laboratoriów badawczych na całym świecie zmierzające do udoskonalenia metod identyfikacji osób na podstawie głosu. Przejawia się to m.in. w liczbie publikacji, ciągle rosnącej liczbie laboratoriów biorących udział w testach organizowanych przez NIST oraz, wreszcie, w pojawieniu się na rynku nowego oprogramowania, które wykorzystuje coraz doskonalsze rozwiązania.

Nad wdrożeniem lub doskonaleniem własnych metod automatycznej identyfikacji pracuje również wiele laboratoriów kryminalistycznych. Obserwując postęp w tej dziedzinie, wydaje się, że wkrótce tego typu metody badawcze zajmą ważne miejsce w procesie kryminalistycznej identyfikacji mówców.

Literatura:

1. D.A. Reynolds and R.C. Rose, *Robust text-independent speaker identification using Gaussian mixture speaker models*, IEEE Transactions on Speech and Audio Processing 1995, 3(1):72–83.
2. J. Szwabiński, *Metody numeryczne,* 2006.
3. L.G. Kersta, *Voiceprint Identification,* Nature 1962, vol. 196, pp. 1253–1257.
4. W. Jassem, *Podstawy fonetyki akustycznej,* IPPT PAN 1973.
5. B.P. Bogert, M.J.R. Healy, and J.W. Tukey, *The quefrency alanysis of time series for echoes: Cepstrum, pseudo-autocovariance, cross-cepstrum, and saphe cracking,* w: M. Rosenblatt, Ed., 1963, Time Series Analysis, ch. 15, s. 209–243.
6. W. Maciejko, *Różnice wewnątrzosobnicze i międzyosobnicze w parametrach mówców oryginalnych i ich imitatorów*, Politechnika Wrocławska 2005.
7. A. Malegaonkar, P. Ariyaeeinia, P. Sivakumaran, S. Pillay, *Discrimination effectivness of speech cepstral features,* Biometrics and Identity Management Volume 2008, 5372/2008.
8. H. Hermansky, *RASTA Processing of Speech*, IEEE Trans. on Speech, and Audio Proc, 1994, 2(4):578–589.
9. P. Cichosz, *Systemy uczące się,* WNT 2000
10. http://www.itl.nist.gov/iad/mig//tests/sre/.
11. J. Gonzalez-Rodriguez, J. Fierrez-Aguilar, J. Ortega-Garcia, *Forensic identification reporting using automatic speaker recognition systems,* ICASSP 2003.

ABSTRACT

Automatic Speaker Recognition (ASR) is among most extensively developed biometric techniques. The highly effective recognition methods can be successfully implemented in various fields, such as forensic sciences. This paper describes the fundamentals of automatic speaker recognition, including brief history of speech analysis research, aiming at speaker recognition as well as classification of the ASR systems. Presented are state – of – the – art recognition methods in connection with individual speaker features and with the classification techniques. The principal requirements of forensic speaker recognition were defined in order to characterize the theoretical model of an optimal automatic speaker recognition system.

IV.
PRAWO

Antoni Podolski

Miejsce Rządowego Centrum Bezpieczeństwa w systemie bezpieczeństwa antyterrorystycznego Rzeczypospolitej Polskiej

Zagrożenia o charakterze asymetrycznym, szczególnie związane z działaniami terrorystycznymi, są wyjątkowe z punktu widzenia teorii i praktyki zarządzania kryzysowego. Angażują bowiem, niezależnie od skali zaistniałego zdarzenia, najwyższe szczeble decyzyjne i wykonawcze w państwie, pozornie odmiennie od zasad przyjętych w systemie zarządzania kryzysowego, każące reagować na zagrożenia na możliwie najniższym, kompetentnym szczeblu. Pozornie, gdyż w przypadku terroryzmu tym najniższym kompetentnym szczeblem jest właśnie szczebel najwyższy, a więc co najmniej minister spraw wewnętrznych, a zapewne także premier i cały rząd. Trudno bowiem sobie wyobrazić, by w przypadku zdarzenia o charakterze terrorystycznym zaistniałym np. na szczeblu miasta lub powiatu, szczebel reakcji ograniczył się, podobnie jak w przypadku „zwykłej" sytuacji kryzysowej, do poziomu wójta, burmistrza czy starosty wraz z będącymi w ich dyspozycji zasobami policji, straży miejskiej czy straży pożarnej. Jasne jest, że natychmiast o zaistniałej sytuacji zawiadomieni zostaną wojewoda, minister spraw wewnętrznych, premier, zaś koordynację obiegu informacji i decyzji przejmie Rządowe Centrum Bezpieczeństwa (dalej RCB) wraz z Centrum Antyterrorystycznym (dalej CAT). Zaistnieje zapewne również potrzeba zwołania Rządowego Zespołu Zarządzania Kryzysowego obsługiwanego informacyjnie i organizacyjnie przez RCB.

To właśnie RCB, utworzone na mocy art. 10 ustawy z dnia 26 kwietnia 2007 (Dz. U. z 2007 r. nr 89, poz. 590 z późn. zm.) o zarządzaniu kryzysowym oraz wydanego na jej podstawie rozporządzenia Prezesa Rady Ministrów, zapewnia obsługę Rady Ministrów, Prezesa Rady Ministrów, Rządowego Zespołu Zarządzania Kryzysowego (dalej RZZK) i ministra właściwego do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz pełni funkcję krajowego centrum zarządzania kryzysowego (art. 11).

Te dwa zapisy konstytuują wyjątkową pozycję Centrum (dalej RCB) w systemie zarządzania kryzysowego i szerzej – bezpieczeństwa narodowego. Mimo, że podlega premierowi i ma zapewnić rządowi możliwość sprawowania zarządzania kryzysowego w Polsce, to nie jest urzędem ani organem centralnym (art. 10 ust. 1) i nie jest częścią Kancelarii Premiera. RCB zapewnia obsługę w tym zakresie całej Rady Ministrów, a dopiero później premiera, RZZK i ministra spraw wewnętrznych. Wynika to jasno nie tylko z kolejności przyjętej w przywołanym art. 10, ale i generalnej filozofii ustawy o zarządzaniu kryzysowym stanowiącej, iż to właśnie cała Rada Ministrów, a nie premier, sprawuje zarządzanie kryzysowe na terytorium Rzeczpospolitej Polskiej (art. 7 ust. 1). Warto również zwrócić uwagę na fakt, iż „w przypadkach niecierpiących zwłoki" to nie premier, a minister właściwy do spraw wewnętrznych, sprawuje zarządzanie kryzysowe (art. 7 ust. 2), a jego decyzje rozpatruje Rada Ministrów na najbliższym posiedzeniu (art. 7 ust. 3).

Możemy z kolei przyjąć, iż większość sytuacji kryzysowych, to właśnie „przypadki niecierpiące zwłoki", szczególnie zaś wywołane działaniami terrorystycznymi, obliczonymi przecież w swej logice na wywołanie efektu zaskoczenia i zamieszania.

Dlatego RCB, w większości przypadków reagowania na sytuacje kryzysowe, pracuje w pierwszej kolejności i fazie na potrzeby ministra właściwego do spraw wewnętrznych. Można wręcz zaryzykować tezę, iż o ile rząd jako całość zaangażowany jest w dwie pierwsze i ostatnią fazę zarządzania kryzysowego (zapobieganie, przygotowanie, odbudowa), o tyle minister spraw wewnętrznych i administracji jest niemal niekwestionowanym suwerenem w zakresie fazy reagowania. Stąd logiczna decyzja ustawodawcy, by RCB pełniło również codzienną obsługę tegoż ministra w kwestiach zarządzania kryzysowego (art. 11 ust. 1) i aby tenże minister nie musiał tworzyć odrębnego centrum zarządzania kryzysowego[1)].

RCB obsługuje natomiast premiera jako Przewodniczącego Rządowego Zespołu Zarządzania Kryzysowego, gdyż dyrektor RCB pełni funkcję sekretarza tegoż Zespołu (art. 10 ust. 2a). Możliwe jest jednak, by również w tym przypadku premier delegował do kierowania RZZK swego zastępcę – wiceprezesa Rady Ministrów (art. 8. ust. 7 pkt 1). W przypadku, gdy minister właściwy do spraw wewnętrznych pełni również funkcje wicepremiera upraszcza to funkcjonowanie systemu i zdejmuje część bieżących zadań w tym zakresie z premiera.

Należy podkreślić, iż w myśl ustawy o zarządzaniu kryzysowym ani RCB, ani jego Dyrektor nie są w żadnym wypadku superdowództwem na wypadek sytuacji kryzysowych. Nie są również organem administracji państwowej, mają jedynie zapewnić stały przepływ informacji na potrzeby zarządzania kryzysowego, przygotowanie i aktualizacje planów i procedur, umożliwić koordynację działań i zarządzanie kryzysowe przez odpowiednie organy - Radę Ministrów i ministra właściwego do spraw wewnętrznych.

RCB jako zespół apolitycznych urzędników i funkcjonariuszy średniego szczebla służbowego ma być, w miarę, odporną na zawirowania i zmiany polityczne, instytucją sztabowo-planistyczną wypełniającą lukę niekompetencji lub braku przygotowania merytorycznego czynników politycznych.

Omawiając zadania RCB z punktu widzenia zagrożeń terrorystycznych, należy przede wszystkim zauważyć, iż są one dwojakiego rodzaju: część to zadania RCB jako całości, pozostała część – zadania Dyrektora RCB, który realizuje je przy pomocy kierowanej przez siebie jednostki organizacyjnej. W niniejszym opracowaniu aspekt ten jest potraktowany wtórnie w stosunku do zakresu przedmiotowego tych zadań.

Podstawowymi zadaniami RCB jako jednostki jest pełnienie funkcji krajowego centrum zarządzania kryzysowego i zapewnienie obsługi Rady Ministrów, Prezesa Rady Ministrów, Rządowego Zespołu Zarządzania Kryzysowego i ministra właściwe-

[1)] Nie można jednak mówić, iż RCB podlega organizacyjnie i kadrowo szefowi resortu spraw wewnętrznych i administracji, gdyż stan taki byłby niezgodny z ustawą. Warto również wspomnieć, iż w myśl ustawy wyznaczanie dyrektora RCB i jego zastępców jest wyłączną kompetencją premiera (art. 10., ust 2 i 3) i ustawa nie przewiduje udziału w tym procesie jakiegokolwiek ministra, w tym również właściwego do spraw wewnętrznych. Jedyną formą podległości ministrowi właściwemu do spraw wewnętrznych jest fakt, iż koszty funkcjonowania RCB pokrywane są z części budżetu państwa, której dysponentem jest minister właściwy do spraw wewnętrznych (art. 11 ust. 2a). Było to rozwiązanie podyktowane faktem, iż zarządzanie kryzysowe znajduje się właśnie w kompetencji budżetowej ministra właściwego do spraw wewnętrznych, zaś RCB jako jednostka budżetowa podległa Prezesowi Rady Ministrów nie jest częścią jego Kancelarii, nie może więc być finansowana z tej części budżetu. Jest to rozwiązanie logiczne, wiążące finansowanie RCB z finansowaniem pozostałych elementów zarządzania kryzysowego w kraju, szczególnie w wymiarze terytorialnym.

go do spraw wewnętrznych w sprawach zarządzania kryzysowego oraz zapewnienie obiegu informacji między krajowymi i zagranicznymi organami i strukturami zarządzania kryzysowego. Jedną zaś z podstawowych funkcji każdego centrum zarządzania kryzysowego jest stały monitoring potencjalnych zagrożeń. Monitorowanie zagrożeń to podstawowa, „pozakryzysowa" działalność RCB. Oznacza również, iż zadanie to realizuje całe RCB, a nie jedna tylko z jego części składowych, np. służba dyżurna, która jest wyłącznie jednym z narzędzi, jakimi dysponuje RCB. Elementem tych działań jest analiza i ocena możliwości wystąpienia zagrożeń lub ich rozwoju, gromadzenie informacji o zagrożeniach i analiza zebranych materiałów oraz wypracowywanie wniosków i propozycji dotyczących zapobiegania i przeciwdziałania zagrożeniom. W tym celu RCB musi współdziałać z centrami zarządzania kryzysowego organów administracji publicznej i pozyskiwać od komórek właściwych w sprawach zarządzania kryzysowego w urzędach wojewódzkich niezbędne informacje odnośnie aktualnego stanu bezpieczeństwa na obszarze danego województwa.

Należy zwrócić uwagę iż w obecnym stanie prawnym pozyskiwanie przez RCB informacji dotyczących aktualnego stanu bezpieczeństwa na obszarze danego województwa jest jedynie zadaniem domyślnym, pośrednio wyinterpretowanym z właściwego zadania ustawowego, jakie ciąży na komórkach organizacyjnych właściwych w sprawach zarządzania kryzysowego w urzędzie wojewódzkim[2)]. Zadanie to polega na przekazywaniu do RCB informacji na temat aktualnego stanu bezpieczeństwa na właściwym terytorialnie obszarze. Skoro takie zadanie ciąży na 16 urzędach wojewódzkich i wszystkie one mają przekazywać tego typu informacje m.in. do RCB, to jasne jest, iż tym samym do zadań Centrum powinno należeć pozyskiwanie i przetwarzanie tego typu informacji. Jest to więc zadanie pośrednio związane z monitoringiem potencjalnych zagrożeń, ale mające szerszy charakter, gdyż zakłada monitorowanie całego stanu bezpieczeństwa kraju. Widać tu pewną niekonsekwencję ustawodawcy, gdyż z jednej strony jako zadania RCB wymienia się monitoring potencjalnych zagrożeń, ale już monitoring aktualnego stanu bezpieczeństwa ujęto pośrednio jako zadanie bierne. Jako zadanie aktywne zapisane jest w artykule dotyczącym zadań urzędów wojewódzkich. W przyszłości wskazane byłoby dopisanie do obowiązków RCB prowadzenie monitoringu aktualnego stanu bezpieczeństwa kraju (państwa). Warto podkreślić, iż Dyrektor RCB na mocy art. 20a ma prawo – na równi z organami właściwymi w sprawach zarządzania kryzysowego – *do żądania udzielenia informacji oraz gromadzenia i przetwarzania danych niezbędnych do realizacji zadań określonych w ustawie* (o zarządzaniu kryzysowym).

W momencie wystąpienia sytuacji kryzysowej niezwykle istotne jest reagowanie na nią w myśl wcześniej przygotowanych procedur związanych z zarządzaniem kryzysowym, w tym przygotowywanie projektów opinii i stanowisk RZZK. Jak wspomniano na wstępie, sytuacje kryzysowe spowodowane czynnikami o charakterze terrorystycznym wymagają zaangażowania w ich zwalczanie najwyższych czynników decyzyjnych,

[2)] Art. 14 ust. 6: *Do zadań komórki organizacyjnej właściwej w sprawach zarządzania kryzysowego w urzędzie wojewódzkim należy w szczególności: (...) dostarczanie niezbędnych informacji dotyczących aktualnego stanu bezpieczeństwa dla wojewódzkiego zespołu zarządzania kryzysowego, zespołu zarządzania kryzysowego działającego w urzędzie obsługującym ministra właściwego do spraw wewnętrznych oraz Centrum.*

w tym również RZZK, zadaniem RCB jest przygotowywanie i obsługa techniczno-organizacyjna prac RZZK, informowanie, zgodnie z art. 8 ust. 2 i 3, członków RZZK o potencjalnych zagrożeniach oraz działaniach podjętych przez właściwe organy. Powyższe zadania związane są z pełnieniem przez Dyrektora RCB funkcji Sekretarza RZZK. Aby tę funkcję pełnić efektywnie, Dyrektor-Sekretarz musi mieć możliwość zarówno zapewnienia właściwej obsługi prac RZZK, w razie potrzeby także z uwzględnieniem wymogów ustawy o ochronie informacji niejawnych, oraz być w stanie przedstawić członkom Zespołu niezbędne dla właściwego prowadzenia jego prac analizy i opinie, także prawne, oraz projekty pisemnych decyzji.

Z kolei, podstawowym zadaniem ustawowym Dyrektora RCB jest kierowanie Rządowym Centrum Bezpieczeństwa i pełnienie wspomnianej funkcji sekretarza RZZK (art. 10 ust 2a) czego logiczną konsekwencją jest pełnienie przez RCB roli sekretariatu tegoż Zespołu (lub wybraną przez Dyrektora jego komórkę organizacyjną). Dyrektor RCB jest więc obok premiera i ministrów właściwych do spraw wewnętrznych, obrony i zagranicznych, jedynym stałym z mocy ustawy uczestnikiem prac Zespołu. Nie jest jednak jego członkiem, gdyż nie jest wymieniony w składzie zespołu, ale w odrębnym ustępie[3)]. Rozwijając ten wątek warto również zaznaczyć, iż funkcja Sekretarza RZZK jest funkcją czysto techniczno-logistyczną i nie może być interpretowana jako np. odpowiadająca za terminowe i zgodne z zasadami zwoływanie i wykorzystywanie Zespołu, co jest wyłączną kompetencją jego przewodniczącego, tj. Prezesa Rady Ministrów lub upoważnionego przez niego zastępcę w randze wicepremiera (art. 8 ust.7).

Ponieważ zagrożenia terrorystyczne i sposoby ich zwalczania są elementem szerszego katalogu zagrożeń dla bezpieczeństwa narodowego i metodyki ich zwalczania, należy wspomnieć w tym miejscu również o zadaniach związanych ze sporządzaniem i koordynacją sporządzania planów zarządzania kryzysowego przez kolejne szczeble administracji publicznej. Bezpośrednim zadaniem Dyrektora RCB jest uzgadnianie z ministrami – kierownikami urzędów centralnych sporządzanych przez nich planów zarządzania kryzysowego, które to stanowią załącznik funkcjonalny do Krajowego Planu Zarządzania Kryzysowego (na podstawie art. 12 ust. 2), jak również opiniowanie zarządzenia ministra właściwego do spraw wewnętrznych zawierającego wytyczne do wojewódzkich planów zarządzania kryzysowego dla wojewodów i opiniowanie wojewódzkich planów zarządzania kryzysowego przed zatwierdzeniem ich przez ministra właściwego do spraw wewnętrznych.

W zapisanych w ustawie zadaniach z zakresu planowania cywilnego kryje się jedno z najważniejszych zadań RCB jako bezpośredniego zaplecza doradczego Rady Ministrów i ministra właściwego do spraw wewnętrznych. Zadanie to – to opracowywanie propozycji rozwiązań sytuacji kryzysowych, a w praktycznym wymiarze przedkładanie ministrowi właściwemu do spraw wewnętrznych, przewodniczącemu RZZK lub Radzie Ministrów projektów decyzji i konkretnych działań. Takimi propozycjami mogą być np.: wzmocnienie sił i środków pozostających w dyspozycji danego wojewody odwodami centralnymi, wsparcie konkretnego resortu przez inne organy lub służby, czy

[3)] Art. 10 ust. 2a . W pierwotnej wersji ustawy ustęp ten znajdował się w artykule omawiającym skład i zadania RZZK (art. 8), ale obecne jego usytuowanie w artykule poświęconym zadaniom RCB jest jak najbardziej logiczne i służy rozwianiu wątpliwości co do właściwej roli Dyrektora RCB w RZZK.

wystąpienie o pomoc zagraniczną. W ramach planowania cywilnego RCB przedstawia szczegółowe sposoby i środki reagowania na zagrożenia oraz ograniczania ich skutków, w ramach opracowywanego i aktualizowanego (we współpracy z właściwymi komórkami organizacyjnymi urzędów obsługujących ministrów oraz kierowników urzędów centralnych) Krajowego Planu Zarządzania Kryzysowego. Zadaniem RCB jest także uzgadnianie planów zarządzania kryzysowego sporządzanych przez ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych. Zadanie to związane jest z obowiązkiem uzgadniania przez Dyrektora RCB z ministrami i kierownikami urzędów centralnych sporządzanych przez nich planów zarządzania kryzysowego, które stanowią załącznik funkcjonalny do Krajowego Planu Zarządzania Kryzysowego na podstawie art. 12 ust. 2.

Z planowaniem związana jest realizacja zadań planistycznych i programowych z zakresu ochrony infrastruktury krytycznej, w tym opracowywanie i aktualizacja załącznika funkcjonalnego do Krajowego Planu Zarządzania Kryzysowego dotyczącego ochrony infrastruktury krytycznej, a także współpraca, jako krajowy punkt kontaktowy, z instytucjami Unii Europejskiej i Organizacji Traktatu Północnoatlantyckiego oraz ich krajami członkowskimi w zakresie ochrony infrastruktury krytycznej. W celu optymalnej realizacji przez Polskę współdziałania sojuszniczego w tym zakresie, na RCB ciąży zadanie przygotowania projektu zarządzenia Prezesa Rady Ministrów (o którym mowa w art. 7 ust. 4), które, z zachowaniem przepisów o ochronie informacji niejawnych, określi wykaz przedsięwzięć i procedur systemu zarządzania kryzysowego, z uwzględnieniem zobowiązań wynikających z członkostwa w Organizacji Traktatu Północnoatlantyckiego oraz organy odpowiedzialne za ich uruchamianie. Wspomniany wykaz przedsięwzięć i procedur uwzględniający zobowiązania członkowskie NATO ma regulować zobowiązania Polski do realizacji m.in. przedsięwzięć wynikających z *NATO Crisis Response System* (NCRS), określanego w polskich przepisach niezbyt ściśle jako Narodowy System Pogotowia Kryzysowego NATO. Przypomnijmy, iż w pierwotnej wersji ustawy o zarządzaniu kryzysowym z 2007 roku mówiono wprost o wykazie zadań i procedur NSPK i wykazie przedsięwzięć NSPK[4)]. Obecne brzmienie jest zapisem znacznie szerszym i nie likwidującym w żaden sposób współpracy z NATO w ramach NCRS, a wręcz go poszerzającym na inne agendy i uniezależniającym od ewentualnych zmian terminologii procedur kryzysowych NATO. Podobnym zadaniem jest współdziałanie z podmiotami, komórkami i jednostkami organizacyjnymi Organizacji Traktatu Północnoatlantyckiego i Unii Europejskiej oraz innych organizacji międzynarodowych, odpowiedzialnymi za zarządzanie kryzysowe i ochronę infrastruktury krytycznej oraz informowanie Komisji Europejskiej i państw członkowskich Unii Europejskiej o środkach zastosowanych w sytuacji kryzysowej w celu zabezpieczenia prawidłowego działania publicznej sieci telekomunikacyjnej oraz stacji nadawczych i odbiorczych używanych do zapewnienia bezpieczeństwa, w zakresie dotyczącym systemu łączności i sieci teleinformatycznych na podstawie art. 11a ustawy o zarządzaniu kryzysowym.

[4)] Wersja pierwotna brzmiała: *Prezes Rady Ministrów w drodze zarządzenia niepodlegającego ogłoszeniu, określa wykaz zadań i procedur NSPK, w tym sposoby i tryb ich uruchamiania zwany dalej wykazem przedsięwzięć NSP.* Artykuł ten zmieniono ustawą z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym (Dz. U. z 2009 r nr 131, poz. 1076).

W ramach wykonywania zadań związanych z przeciwdziałaniem i zapobieganiem zagrożeniom Dyrektor RCB przygotowuje - we współpracy z ministrami i kierownikami urzędów centralnych odpowiedzialnych za systemy infrastruktury krytycznej oraz właściwymi w sprawach bezpieczeństwa narodowego - Narodowy Programu Ochrony Infrastruktury Krytycznej[5]. Zadanie to jest istotne w kontekście omawianego zagadnienia, gdyż zagrożenia terrorystyczne skierowane są zazwyczaj przeciwko obiektom i instalacjom czy systemom infrastruktury krytycznej państwa. W związku z tym, Dyrektor RCB odpowiada również za sporządzanie jednolitego wykazu obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej z podziałem na systemy. Wykaz ten Dyrektor RCB sporządza na podstawie kryteriów zawartych w wyżej wymienionym Programie, we współpracy z ministrami odpowiedzialnymi za systemy infrastruktury krytycznej. Ponieważ jedynym narzędziem organizacyjnym, jakim dysponuje Dyrektor, jest właśnie RCB jasne jest, że zarówno Program, jak i wykaz, będą sporządzane siłami Centrum. Konsekwencją tego procesu jest kolejne zadanie, czyli opracowanie wyciągów z wykazu infrastruktury krytycznej, o którym mowa w art. 5b ust. 7 pkt 1, znajdującej się w danym systemie oraz przekazywanie ich ministrom i kierownikom urzędów centralnych odpowiedzialnym za dany system. Dyrektor RCB odpowiada również za opracowanie wyciągów z wykazu infrastruktury krytycznej, o którym mowa w art. 5b ust 7 pkt.1, znajdującej się na terenie województw oraz przekazywanie ich właściwym wojewodom. Do jego obowiązków należy także informowanie właścicieli, posiadaczy samoistnych i zależnych, obiektów, instalacji lub urządzeń o ujęciu ich w wykazie, o którym mowa w art. 5b ust 7 pkt. 1.

W kontekście bezpośrednio związanym z zagrożeniami terrorystycznymi niezwykle istotne jest kolejne zadanie ustawowe Dyrektora RCB, czyli pozyskiwanie od Szefa Agencji Bezpieczeństwa Wewnętrznego informacji o podjętych przez niego działaniach na mocy art. 12a , ust. 4 omawianej ustawy. Przypomnijmy, iż zgodnie z tym zapisem *Szef Agencji Bezpieczeństwa Wewnętrznego, w przypadku podjęcia informacji o możliwości wystąpienia sytuacji kryzysowej będącej skutkiem zdarzenia o charakterze terrorystycznym, zagrażającego infrastrukturze krytycznej, życiu lub zdrowiu ludzi, mieniu w znacznych rozmiarach, dziedzictwu narodowemu lub środowisku, może udzielać zaleceń organom i podmiotom zagrożonym tymi działaniami oraz przekazywać im niezbędne informacje służące przeciwdziałaniu zagrożeniom* (art. 12a ust. 3). Intencją i celem tego zapisu jest zapewnienie dodatkowej kontroli administracji cywilnej nad działaniami służb specjalnych, szczególnie w tak wrażliwym wymiarze ich relacji z obywatelami, podmiotami gospodarczymi lub samorządami. Fakt, iż po każdorazowym udzieleniu zaleceń Szef ABW musi o podjętym działaniu poinformować Dyrektora RCB jasno wskazuje, iż wspomniane zalecenia nie mogą być traktowane jako element działania operacyjnego Agencji, ale jako podstawowa działalność administracyjna Szefa ABW – centralnego organu administracji rządowej.

---

[5] Narodowy Program Ochrony Infrastruktury Krytycznej zawiera, zgodnie z artykułem art. 5 b *Ustawy o zarządzaniu kryzysowym* narodowe priorytety, cele, wymagania oraz standardy, służące zapewnieniu sprawnego funkcjonowania infrastruktury; wykaz ministrów kierujących działami administracji rządowej i kierowników urzędów centralnych odpowiedzialnych za systemy o których mowa w ustawie o zarządzaniu kryzysowym; szczegółowe kryteria pozwalające wyodrębnić obiekty, instalacje, urządzenia i usługi wchodzące w skład systemów infrastruktury krytycznej.

W ustawie, w ramach zadań RCB, zapisane są wprost dwa zadania związane z zagrożeniami terrorystycznymi. Jest to, po pierwsze, realizacja zadań z zakresu zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym, i po drugie, współdziałanie z Szefem Agencji Bezpieczeństwa Wewnętrznego w zakresie zapobiegania, przeciwdziałania i usuwania skutków zdarzeń o charakterze terrorystycznym.

Dwa wyżej wymienione zadania związane z zagrożeniami o charakterze terrorystycznym wymagają dokładniejszego wyjaśnienia. Należy przede wszystkim podkreślić, iż RCB w żadnym przypadku nie odpowiada za zapobieganie i przeciwdziałanie terroryzmowi, jak to bywało czasami błędnie interpretowane przez media i ekspertów. Jest to zadanie służb dysponujących uprawnieniami i możliwościami prowadzenia pracy operacyjnej, w tym przede wszystkim ABW. Natomiast powyższy zapis powinien być rozumiany w ten sposób, iż RCB odpowiada za realizację zadań z zakresu zapobiegania skutkom zdarzeń o charakterze terrorystycznym, przeciwdziałania skutkom takich zdarzeń i usuwania ich skutków. Są to zadania głównie z zakresu profilaktyki i przygotowania systemu bezpieczeństwa, infrastruktury i procedur reagowania pod kątem minimalizacji lub wręcz eliminacji ewentualnych skutków zdarzeń terrorystycznych. Przykładowo, chodzi o takie przygotowanie dróg ewakuacyjnych w obiektach użyteczności publicznej, by ewentualny zamach terrorystyczny miał jak najmniejsze skutki pośrednie w postaci ewentualnych ofiar paniki czy braku powietrza.

Dyrektor RCB ma również zapewnić koordynację przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego (art. 5a ust 2). W ramach tego zadania Dyrektor RCB przy pomocy podległej jednostki musi zapewnić warunki do osiągnięcia pełnej spójności merytorycznej i logicznej dokumentu, zgodnie z wymogami właściwego Rozporządzenia Rady Ministrów[6)]. Pod pojęciem zapewnienia koordynacji rozumiemy nie tylko zapewnienie uzgodnienia i zharmonizowania treści i trybu prac nad dokumentem, ale również - szczególnie w trakcie prac nad pierwszą edycją Raportu - wytworzenie swoistej kultury pracy zespołowej nad tym nowatorskim w polskiej administracji rządowej dokumentem oraz wypracowanie i przedstawienie pewnych wzorców przygotowania jego części składowych. Jest to wreszcie kwestia pilnowania i egzekwowania terminów wykonania Raportu przez jego podwykonawców. Warto również poświęcić uwagę budzącemu spore kontrowersje i nieporozumienia zarówno w trakcie prac parlamentarnych, jak i w mediach, zapisowi dotyczącemu roli Szefa ABW w koordynacji prac nad Raportem[7)]. Z zapisu wskazującego, iż Szef ABW zapewnia koordynację prac nad częścią Raportu dotyczącą zagrożeń o charakterze terrorystycznym wynika jasno nie tylko, że jest to zadanie podwykonawcze w stosunku do nadrzędnego zadania zapewnienia koordynacji przygotowania całości Raportu, ciążącego na Dyrektorze RCB, ale i że – w tym wymiarze – Dyrektor RCB znajduje się w roli nadrzędnej w stosunku do Szefa ABW i w ramach posiadanego wyższego zadania ustawowego powinien

[6)] Art. 5a ust. 6: *Rada Ministrów określi, w drodze rozporządzenia, sposób, tryb i terminy opracowywania Raportu, biorąc pod uwagę konieczność zapewnienia odpowiedniego poziomu bezpieczeństwa narodowego.*

[7)] Art. 5a ust.2: *Koordynację przygotowania Raportu zapewnia dyrektor Rządowego Centrum Bezpieczeństwa, a w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej, Szef Agencji Bezpieczeństwa Wewnętrznego.*

egzekwować swe uprawnienia wynikające z zapisów omawianego artykułu również w stosunku do tej części prac nad Raportem.

W kontekście zwalczania zagrożeń terrorystycznych, mogących wymagać współdziałania z siłami zbrojnymi i udziału ministra obrony narodowej w systemie zarządzania kryzysowego, istotne jest właściwe zaplanowanie wykorzystania Sił Zbrojnych Rzeczypospolitej Polskiej do wykonywania zadań, o których mowa w art. 25 ust. 3 oraz planowanie wsparcia przez organy administracji publicznej realizacji ich zadań. W tym kontekście należy również wspomnieć o utrzymywaniu przez RCB stałego dyżuru w ramach gotowości obronnej państwa.

Jednym z podstawowych celów ataków terrorystycznych jest wywołanie możliwie największego efektu psychologicznego i społecznego, paniki, podważenie zaufania społecznego do rządu, nacisku na zmianę prowadzonej w danym momencie, a niezgodnej z celami terrorystów, polityki. Dlatego, w zwalczaniu tego typu zjawisk niezwykle istotne jest zapewnienie koordynacji polityki informacyjnej organów administracji publicznej w czasie sytuacji kryzysowej. Jest to nowe zadanie RCB, wprowadzone w efekcie nowelizacji ustawy o zarządzaniu kryzysowym w 2009 roku. Kwestia właściwej komunikacji ze społeczeństwem i polityki medialnej jest jednym z kluczowych zagadnień nowoczesnego zarządzania i reagowania kryzysowego. W dobie globalnej komunikacji multimedialnej, nieskrępowanego dostępu do nośników obrazu i dźwięku władze i służby państwowe utraciły monopol informacyjny i pierwszeństwo w informowaniu społeczeństwa i mediów o sytuacjach kryzysowych i zagrożeniach bezpieczeństwa. Coraz częściej to przekaz pochodzący od świadków lub uczestników wydarzeń trafia via media do reszty społeczeństwa, stając się nie tylko podstawowym źródłem informacji dla obywateli, ale czasem również dla władz administracyjnych. Szybkość, z jaką informacja o zdarzeniach dociera do odbiorców, wymusza także szybszą i jawną reakcję administracji, rodzi presję medialną przede wszystkim na szybkość reakcji, czasem kosztem jej efektywności. Zdarza się również, iż właściwe reagowanie kryzysowe ustępuje miejsca reagowaniu na przekaz medialny, na obraz zdarzenia w mediach i świadomości społecznej, a nie wydarzenie samo w sobie. Niewłaściwa polityka informacyjna, chaotyczna, niespójna czy nieadekwatna, a w najgorszym przypadku fałszywa informacja, mogą wywołać wrażenie nieradzenia sobie przez władze z danym kryzysem, poderwać zaufanie obywateli do organów państwa, a w ekstremalnym przypadku prowadzić do wybuchu paniki i histerycznych, niekontrolowanych zachowań społecznych.

Na koniec warto wspomnieć o niezwykle istotnym i wymagającym dużego nakładu pracy, właściwym szkoleniu kadr i struktur odpowiedzialnych za polski system zarządzania kryzysowego i zwalczania zagrożeń, w tym oczywiście także tych o charakterze terrorystycznym. Zadaniem RCB jest organizowanie, prowadzenie i koordynacja szkoleń i ćwiczeń z zakresu zarządzania kryzysowego oraz udział w ćwiczeniach krajowych i międzynarodowych. Ponadto, na mocy art. 11 ust. 3 Rada Ministrów lub Prezes Rady Ministrów mogą zlecić Centrum dodatkowe zadania związane z zarządzaniem kryzysowym.

ABSTRACT

This article presents activities of Government Security Centre in the Polish antiterrorist protection system, as well as its place in the Polish legislative system. It indicates the basic Government Security Centre tasks in the area of terrorist threats and cooperation with other institutions in case of a crisis situation occurring.

Jacek Grzemski
Andrzej Krześ

Analiza pojęcia „przestępstwa godzące w podstawy ekonomiczne państwa" w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu

Do zakresu działań Agencji Bezpieczeństwa Wewnętrznego wymienionych w ustawie z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (tj. Dz.U. z 2010 r. nr 29, poz. 154), na podstawie art. 5 ust. 1 pkt 2 lit. b, należy rozpoznawanie, zapobieganie i wykrywanie przestępstw oraz ściganie sprawców przestępstw godzących w „podstawy ekonomiczne państwa".

Autorzy niniejszego artykułu podjęli próbę zdefiniowania zapisu zawartego w art. 5 ust. 1 pkt 2 lit. b cyt. ustawy, który mówi o rozpoznawaniu, zapobieganiu i wykrywaniu przez funkcjonariuszy ABW przestępstw „godzących w podstawy ekonomiczne państwa" oraz ściganiu ich sprawców. W tym miejscu należy zaznaczyć, że podobne uregulowanie zawarte było w art. 1 ust. 2 pkt 3 ustawy z dnia 6 kwietnia 1990 r. o Urzędzie Ochrony Państwa (t.j. Dz.U. z 1999 r. nr 51, poz. 526). Rozważając zapis zawarty w art. 5 ust. 1 pkt 2 lit. b cyt. ustawy nie sposób nie zauważyć, że ani ustawa o UOP, ani ustawa o ABW oraz AW nie zawiera słownika, w którym zdefiniowane byłoby pojęcie „podstawy ekonomiczne państwa". Tym samym, przy zdefiniowaniu przedmiotowego określenia należy posłużyć się w pierwszej kolejności wykładnią językową, a w dalszej systemową i funkcjonalną, mając na uwadze przede wszystkim przepisy: ustawy z 6 czerwca 1997 r. Kodeks postępowania karnego (Dz.U. z 1997 r. nr 89, poz. 555), ustawy z dnia 6 czerwca 1997 r. Kodeks Karny (Dz.U. z 1997 r nr 88, poz. 553) oraz ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (tj. Dz.U. z 2005 r. nr 196, poz.1631 z późn. zm.).

Autorzy, poświęcając uwagę pojęciu „podstawy ekonomiczne państwa", zawartemu w ustawie o ABW oraz AW, chcą zwrócić uwagę na fakt, że jego prawidłowa interpretacja i stosowanie decyduje o tym, czy rozpatrywanie konkretnego czynu należy do właściwości kompetencyjnej ABW. Niniejszy artykuł ma stanowić próbę udzielenia odpowiedzi na poniższe pytania:

- czy wśród obowiązujących przepisów prawa mamy definicję pojęcia „podstawy ekonomiczne państwa"?,
- jeśli nie ma takiej definicji, to co należy rozumieć pod pojęciem „podstawy ekonomiczne państwa?",
- czy każda szkoda wyrządzona Skarbowi Państwa należy do kategorii czynów naruszających podstawy ekonomiczne państwa?,
- czy o tym, że mamy do czynienia z przestępstwem godzącym w podstawy ekonomiczne państwa decyduje wysokość szkody, czy też rodzaj popełnionego przestępstwa?,
- czy mówiąc o naruszeniu podstaw ekonomicznych państwa zawsze mamy na myśli wyrządzenie szkody majątkowej? (czy w przypadku osiągnięcia korzyści osobistej należy mówić o przestępstwie łapówkarstwa czynnego, czy biernego), a co za tym idzie, czy określenie „podstawy ekonomiczne państwa" występujące w ustawie o ABW oraz AW dotyczy tylko i wyłącznie przestępstw materialnych?,

Zdaniem autorów, wprowadzenie przez ustawodawcę do ustawy o ABW oraz AW zapisu „podstawy ekonomiczne państwa" miało na celu rozróżnienie przestępstw gospodarczych, które leżą w kompetencji ABW i tych, których ściganie leży w kompetencji innych służb, w szczególności Policji. Należy zwrócić uwagę, że zakresy kompetencyjne Policji i ABW krzyżują się, w związku z czym niejednokrotnie na etapie operacyjnym funkcjonariusze obu służb mogą gromadzić materiał dotyczący tego samego zakresu przedmiotowego (przestępstwa gospodarcze). Zdaniem autorów, wprowadzenie przez ustawodawcę do ustawy o ABW oraz AW zapisu kompetencyjnego dla ABW poprzez sformułowanie „podstawy ekonomiczne państwa" miało skierować działania funkcjonariuszy Agencji na przestępstwa, w wyniku których dochodzi do narażenia interesu Skarbu Państwa na olbrzymie straty.

Ponadto, należy tutaj wymienić przestępstwa, które mogą mieć wpływ na zachwianie finansów publicznych i spowodować utratę zaufania obywateli do państwa i podmiotów gospodarczych typu: banki, instytucje ubezpieczeniowe, fundusze inwestycyjne, giełdy papierów wartościowych oraz Zakład Ubezpieczeń Społecznych, czy Narodowy Fundusz Zdrowia.

Pojęcie „podstawy ekonomiczne państwa", zdaniem autorów, odnosi się do najważniejszych dziedzin gospodarki, które mają wpływ na prawidłowe funkcjonowanie instytucji państwa. I tak, wśród podstaw ekonomicznych państwa należy wymienić między innymi te, które mają wpływ na prawidłowe funkcjonowanie gospodarki energetycznej kraju, transportu krajowego i międzynarodowego, przetargów publicznych, czy też na prawidłowe funkcjonowanie finansów państwa. Do kategorii przestępstw godzących w podstawy ekonomiczne państwa należy zaliczyć te, które swoimi rozmiarami (wysokość szkody), czy też rodzajem mogą spowodować zachwianie systemu gospodarczego państwa. Dotyczyć to może w szczególności: szkód wywołanych złym zarządzeniem majątkiem Skarbu Państwa (w spółkach z udziałem Skarbu Państwa czy w przedsiębiorstwach państwowych), sprzedaży majątku Skarbu Państwa po cenach znacznie odbiegających od wartości rynkowych (prywatyzacja spółek państwowych, sprzedaż mienia państwa przez agendy rządowe np. Agencję Nieruchomości Rolnych czy Agencję Mienia Wojskowego po niekorzystnych dla Skarbu Państwa cenach oraz na niekorzystnych zasadach, pozorowana upadłość spółek państwowych w celu ich przejęcia). Ponadto do takich przestępstw należy zaliczyć te, w trakcie dokonywania których instytucje państwowe dokonują zakupu dóbr w drodze przetargu z narażeniem Skarbu Państwa na straty wywołane podpisaniem niekorzystnych gospodarczo kontraktów. Ponadto należy wymienić tutaj zapewnienie przez powołane do tego organy skarbowe prawidłowego wpływu należności publicznoprawnych (podatek od towarów i usług, podatek akcyzowy), które stanowią najważniejsze przychody budżetu państwa.

Reasumując należy powiedzieć, że o podstawach ekonomicznych państwa mówimy w odniesieniu do najważniejszych dziedzin gospodarki państwa, które mają wpływ na jego funkcjonowanie.

Autorzy pomimo podjętych prób, nie zdołali znaleźć definicji pojęcia „podstawy ekonomiczne państwa". Słowniczka definiującego niniejsze pojęcie nie zawiera ani ustawa o UOP, ani ustawa o ABW oraz AW.

Wydaje się zatem, że nie każdy czyn karalny powodujący szkodę w mieniu Skarbu Państwa będzie klasyfikowany jako czyn godzący w podstawy ekonomiczne państwa. W tym miejscu należy zadać pytanie, czy i jak duża musi być szkoda, żeby można było mówić o naruszeniu podstaw ekonomicznych państwa? Zdaniem autorów, trudno jest jednoznacznie odpowiedzieć na to pytanie, mając na uwadze fakt, iż niejednokrot-

nie szkody o znikomej wartości mogą spowodować nieodwracalne w skutkach straty dla Skarbu Państwa (np. sprzedaż majątku Skarbu Państwa z naruszeniem przepisów ustawy o zamówieniach publicznych bez wyceny lub na preferencyjnych warunkach; brak uwzględnienia danej transakcji w ofercie przetargowej lub strategii sprzedaży).

Zapewnienie bezpieczeństwa podstawowych interesów ekonomicznych państwa związane jest z jego prawidłowym funkcjonowaniem. Tym samym wiąże się z polityką społeczno-gospodarczą przyjętą przez państwo. Podstawy te decydują nie tylko o prawidłowym funkcjonowaniu państwa jako całości, ale w szczególności, instytucji powołanych przez państwo do zapewnienia prawidłowego jego funkcjonowania i zapewnienia redystrybucji dóbr dla obywateli. Nadmienić należy, iż aktualny katalog funkcji państwa jest bardzo rozbudowany. Obok funkcji wewnętrznych, tradycyjnych, takich jak: prawodawcza, porządkowa i administracyjna, państwo wypełnia nowe funkcje, takie jak gospodarczo-organizacyjna, socjalna czy kulturalno-oświatowa, nie wspominając już o zewnętrznych – zapewnienie obrony granic i integralności państwa oraz bieżącego i wzmożonego kontaktu z innymi państwami.

Mając powyższe na uwadze, autorom wydaje się, że zwrot „podstawy ekonomiczne państwa" związany jest między innymi z zapewnieniem prawidłowego funkcjonowania systemu podatkowego w państwie (wyeliminowaniem „szarej strefy" i zapewnienie wpływu środków finansowych do budżetu). Przykładem przestępstwa godzącego w podstawy ekonomiczne państwa może być wprowadzanie do obrotu oleju opałowego jako oleju napędowego, co w konsekwencji prowadzi do uszczuplenia należności publicznoprawnych, w tym podatku akcyzowego, podatku od towarów i usług oraz podatku dochodowego od osób prawnych.

Wśród przestępstw godzących w podstawy ekonomiczne państwa należy wskazać te ujęte w kodeksie karnym w rozdziale XXXVI, tj.: art. 296 kk (nadużycie zaufania), art. 297 kk (oszustwo kapitałowe), art. 298 kk (oszustwo ubezpieczeniowe), art. 299 kk (pranie brudnych pieniędzy), art. 300 kk (utrudnianie dochodzenia roszczeń), art. 301 kk (pozorne bankructwo), 302 kk (dowolne zaspokajanie wierzycieli), art. 305 kk (utrudnianie przetargu publicznego), oraz te które zostały ujęte w innych ustawach, w szczególności w kodeksie karnym skarbowym (art. 54 kks – nieujawnienie (niezgłoszenie) właściwemu organowi przedmiotu opodatkowania albo podstawy opodatkowania) i art. 56 kks (podanie nieprawdy, zatajenie prawdy w deklaracji/zgłoszeniu).

Oszustwo, o którym mowa w art. 56 § 1-3 kks, popełnia się w deklaracji podatkowej lub w oświadczeniu podatkowym, składanym organowi podatkowemu lub innemu uprawnionemu organowi (np. celnemu, przy wykazywaniu podatku VAT od importu - art. 33 u.p.t.u.) albo płatnikowi podatku (pojęcie deklaracji podatkowej i oświadczenia podatkowego - zob. uw. 8 i 9 do art.53 § 30; pojęcie płatnika, uw. 6 do art. 53 § 30). Oszustwo podatkowe ujęte w art. 56 § 1-3 kks popełnia się przez: a) **podanie nieprawdy**, a więc podanie danych niezgodnych z rzeczywistością, np. dokonanie odliczeń podatkowych, mimo że fakty niezbędne do ich zaistnienia nie miały miejsca, czy złożenie płatnikowi nieprawdziwego oświadczenia, o którym mowa w art. 37 ustawy o podatku dochodowym od osób fizycznych z 1991 r., rzekomy brak innych źródeł dochodu do rozliczenia rocznego podatku **lub podanie** zaistniałych wprawdzie zdarzeń, które jednak nie są uwzględniane przez przepisy ustaw podatkowych i dokonanie mimo to, w oparciu o nie, obliczeń istotnych dla podstawy i wymiaru podatku (zob. uw. 4); b) **zatajenie prawdy**, czyli podanie nie wszystkich danych istotnych do ustalenia prawidłowej wysokości zobowiązania podatkowego, np. ukrycie niektórych dochodów

podlegających sumowaniu (nie stanowi zatajenia brak wykazania w rocznym zeznaniu podatkowym tych dochodów, od których odprowadzono podatek w formie ryczałtu i których - zgodnie z art. 30 ustawy o podatku dochodowym od osób fizycznych - nie łączy się z innymi dochodami); **c) niedopełnienie obowiązku zawiadomienia** o zmianie danych objętych deklaracją lub oświadczeniem, np. o rozwodzie w trakcie roku podatkowego, mimo uprzedniego złożenia oświadczenia o wspólnym opodatkowaniu dochodów, w celu obniżenia zaliczek na podatek dochodowy od osób fizycznych (zob. art. 32 ust. 1a i 1b ustawy o podatku dochodowym od osób fizycznych)[1].

Dodatkowo, w przypadku stwierdzenia przestępstw skarbowych na wielką skalę, należy rozważyć zastosowanie definicji legalnej z art. 53 § 11 kks. Stanowi ona, że przestępstwo skarbowe skierowane przeciwko istotnym interesom finansowym państwa polskiego, o którym mowa w art. 3 § 3, to takie przestępstwo skarbowe, które zagraża Skarbowi Państwa powstaniem uszczerbku finansowego w wysokości co najmniej dziesięciokrotności wielkiej wartości.

W ramach realizacji zadania dotyczącego rozpoznawania, zapobiegania i wykrywania przestępstw godzących w podstawy ekonomiczne państwa, Agencja Bezpieczeństwa Wewnętrznego prowadzi działania w następujących obszarach:
- oszustwa podatkowe,
- pranie brudnych pieniędzy,
- przestępstwa giełdowe,
- nieprawidłowości w gospodarowaniu środkami uzyskanymi z UE.

I. Oszustwa podatkowe

W ramach wyżej przedstawionych grup przestępstw, największe szkody finansowe dla budżetu państwa wyrządzane są przez przemyt do Polski towarów bez naliczania należnego podatku akcyzowego oraz wyłudzanie zwrotów podatku od towarów i usług (VAT). Ponieważ podatek akcyzowy i VAT stanowią główne źródło przychodów budżetu państwa, zagrożenia związane z ich naruszeniem godzą w podstawowe interesy ekonomiczne państwa. Z tego powodu ściganie tego typu przestępstw należy do kompetencji ABW.

Przemyt towarów akcyzowych

Rozumiany jest jako przemieszczanie towarów pomiędzy państwami, z pominięciem opłat celnych, akcyzy, podatku VAT i innych należności wobec państwa, na którego terytorium wwieziono towar lub też wwiezienie towaru, którym obrót jest w danym kraju zakazany.

W Polsce z powodu wysokiego podatku akcyzowego opłacalny stał się przemyt papierosów, alkoholu i paliw płynnych. Zajmują się nim zarówno pojedyncze osoby, tzw. „mrówki", jak i większe, zorganizowane grupy.

W zwalczaniu tego typu przestępczych związków ABW współpracuje z komórkami operacyjnymi Izb Celnych oraz regionalnych oddziałów Straży Granicznej, które

[1] T. Grzegorczyk, *Komentarz ABC 2006*, Komentarz do art. 56 kodeksu karnego skarbowego (Dz.U.99.83.930), w: T. Grzegorczyk, *Kodeks karny skarbowy. Komentarz*, Dom Wydawniczy ABC, 2006, wyd. III.

w swoich kompetencjach posiadają zwalczanie przemytu towarów i korupcji funkcjonariuszy.

Akcesja Polski do Unii Europejskiej obliguje nasze państwo do ochrony interesów fiskalnych nie tylko Polski, ale i całej Wspólnoty. Częstym rodzajem oszustwa celnego, podczas dokonywania którego dochodzi do przekroczenia przepisów Wspólnotowego Kodeksu Celnego, jest usuwanie towarów spod procedury tranzytowej.

Ważnym aspektem skutecznego zwalczania tego typu przestępstw, skierowanych przeciwko systemowi podatkowemu Wspólnoty jest współdziałanie z partnerskimi służbami specjalnymi w ramach wymiany informacji i koordynacji wspólnie podejmowanych działań.[2)]

Wyłudzenia zwrotu podatku VAT

Podatek VAT jest podatkiem od wartości dodanej (ang. *Value Added Tax*), czyli od całkowitych, ostatecznych wydatków konsumpcyjnych, dotyczących nabycia towarów i usług, ostatecznie obciążającym ich indywidualną konsumpcję.

W przepisach dotyczących VAT wykorzystuje się system kredytów podatkowych do przeniesienia ostatecznych i rzeczywistych obciążeń podatkowych na konsumenta oraz w celu uwolnienia „pośredników" od jakichkolwiek ostatecznych kosztów podatku.

Wyłudzenia zwrotów podatku VAT mają miejsce głównie w dwóch przypadkach:

- przy wprowadzaniu do obrotu gospodarczego faktur zawierających podatek VAT naliczony, które dokumentują zaistnienie fikcyjnych zdarzeń gospodarczych lub zawierają znacząco zawyżoną cenę towaru lub usługi,
- w przypadku fikcyjnego eksportu towarów. Poświadczenie nieprawdy w dokumentach celnych, w zakresie dokonania wywozu towaru za granicę, przy pomocy skorumpowanych celników, uprawnia firmę - eksportera do zastosowania stawki 0% podatku VAT do eksportowanego towaru.

Po akcesji naszego kraju do Unii Europejskiej i wprowadzeniu przepisów Wspólnotowego Kodeksu Celnego, także w Polsce pojawił się problem wyłudzeń zwrotów podatku VAT od wspólnotowych dostaw towarów oraz wspólnotowego nabycia towarów. Wyłudzeniom tym towarzyszy wykorzystanie Administracyjnych Dokumentów Towarzyszących (ADT).

Wyłudzenia VAT wewnątrz UE mają miejsce najczęściej w ramach tzw. „karuzeli podatkowej", która polega na wielokrotnym eksporcie i ponownym imporcie tych samych towarów za pośrednictwem złożonego łańcucha dostaw. Charakter przestępstw „karuzelowych", wymaga ścisłej współpracy i wymiany informacji w tym zakresie ze służbami państw Unii Europejskiej.

W celu skutecznego eliminowania przestępstw polegających na wyłudzaniu zwrotów podatku VAT, ABW współpracuje z organami kontroli skarbowej, które są najlepiej przygotowane do wykrywania i dokumentowania działalności firm nie uiszczających należnych podatków.[3)]

[2)] Zob. oficjalna strona internetowa Agencji Bezpieczeństwa Wewnętrznego, www.abw.gov.pl.
[3)] Zob. oficjalna strona internetowa Agencji Bezpieczeństwa Wewnętrznego, www.abw.gov.pl.

II. Pranie brudnych pieniędzy

Pranie brudnych pieniędzy to proceder obejmujący wszelkiego rodzaju operacje mające na celu wprowadzenie do legalnego obrotu wartości majątkowych, które pochodzą z nielegalnych lub nieujawnionych źródeł.

Zjawisko to inicjowane jest przez zorganizowane grupy przestępcze, nierzadko o charakterze międzynarodowym. Efektem przestępczej działalności tych grup jest uzyskiwanie tzw. „brudnych pieniędzy", czyli dochodów pochodzących z nielegalnej działalności, związanej najczęściej z przemytem towarów akcyzowych, narkotyków, handlem bronią i materiałami wybuchowymi, działalnością terrorystyczną, oszustwami finansowymi (podatkowymi), paserstwem, łapówkarstwem itp. Dochody te, aby mogły swobodnie uczestniczyć w obrocie gospodarczym, nie mogą budzić żadnych wątpliwości co do swej legalności. Dlatego też wykorzystywane są coraz bardziej wyrafinowane techniki prania brudnych pieniędzy w celu ukrycia prawdziwego źródła ich pochodzenia i nadania im cech legalności.

W ramach posiadanych kompetencji ustawowych ABW aktywnie zwalcza proceder prania brudnych pieniędzy, ścigając sprawców przestępstw, które są źródłem uzyskiwania nielegalnych dochodów.

W przedmiotowym zakresie ABW współpracuje również (na podstawie zawartego porozumienia) z wyspecjalizowaną instytucją ulokowaną w strukturze Ministerstwa Finansów, tj. z Generalnym Inspektorem Informacji Finansowej.[4)]

III. Przestępstwa giełdowe

Rynek kapitałowy jest miejscem, gdzie pojawia się pokusa szybkiego zdobycia pieniędzy w sposób nielegalny. Przestępstwa giełdowe są szczególnie szkodliwe, gdyż poza realnymi stratami dla firm i zwykłych graczy giełdowych, podważają one zaufanie do stabilności i przewidywalności rynku, co ma odzwierciedlenie w gospodarce państwa.

Istnieje wiele rodzajów przestępstw giełdowych, ale w polskich warunkach najczęściej spotykane są przestępstwa związane z nielegalnym wykorzystywaniem informacji. Jak wiadomo, osoby mające szybki dostęp do informacji uzyskują przewagę nad innymi inwestorami. Nic złego się nie dzieje, gdy dostęp do informacji jest równy i duży bank inwestycyjny uzyska je w tym samym momencie, co mały inwestor - amator. Jednak nie zawsze tak jest. Przestępstwa związane z nielegalnym wykorzystaniem informacji to przykładowo: zatajenie, wykorzystanie lub podanie nieprawdziwych informacji, na przykład przez pracownika biura maklerskiego lub spółki notowanej na giełdzie, który wiedząc wcześniej, że spółka ta poniosła straty, sprzedaje jej akcje, zanim dowiedzą się o tym inwestorzy i kurs tych akcji zacznie spadać.

Instytucją państwową sprawującą nadzór nad rynkiem finansowym w Polsce jest Komisja Nadzoru Finansowego, która przejęła część kompetencji Komisji Papierów Wartościowych i Giełd. W zwalczaniu przestępczości giełdowej ABW współpracuje także z tymi instytucjami.[5)]

[4)] Zob. oficjalna strona internetowa Agencji Bezpieczeństwa Wewnętrznego, www.abw.gov.pl.

[5)] Zob. oficjalna strona internetowa Agencji Bezpieczeństwa Wewnętrznego, www.abw.gov.pl.

IV. Nieprawidłowości w gospodarowaniu środkami uzyskanymi z UE

Przystąpienie Polski do Unii Europejskiej otworzyło możliwości korzystania ze środków finansowych, rozdysponowywanych w ramach struktur UE zarówno przez osoby fizyczne, prawne, jak i jednostki samorządu terytorialnego. Pojawia się jednak problem prawidłowej absorpcji tych środków oraz wystąpienia nieprawidłowości na etapie ich dystrybucji.

Działania ABW w przedmiotowym zakresie koncentrują się na zapobieganiu oraz ujawnianiu nadużyć mających miejsce przy rozdziale, wydatkowaniu i rozliczaniu środków pochodzących z UE. Rozpoznane zagrożenia można podzielić na:

1. Popełnianie przestępstw związanych z dystrybucją funduszy unijnych, polegających na wyłudzaniu środków, co często związane jest z korupcją urzędników instytucji zarządzających funduszami.
2. Wykonywanie przez urzędników biorących udział przy dystrybucji środków unijnych nie rejestrowanej pracy zarobkowej w zakresie wykonawstwa dokumentacji projektowej, studium wykonalności oraz wniosków o dotacje. Osoby te biorą następnie udział w kontroli i weryfikacji powyższych wniosków, co powoduje, że nie jest możliwa obiektywna ocena projektów.
3. Pozaprawny lobbing - polegający na składaniu przez podmioty doradcze propozycji „załatwienia" pozytywnej oceny ich wniosku, przy jednoczesnym powoływaniu się na posiadane wpływy w instytucjach zatwierdzających projekty.
4. Brak skutecznej koordynacji między instytucjami odpowiedzialnymi za wybór i wdrażanie projektów.
5. Niepełne przygotowanie instytucji państwowych i samorządowych do roli dysponentów funduszy unijnych.

W rozpoznawaniu i zwalczaniu nieprawidłowości w absorpcji środków unijnych ABW współpracuje z Pełnomocnikiem Rządu do Spraw Zwalczania Nieprawidłowości Finansowych na Szkodę Rzeczpospolitej Polskiej lub Unii Europejskiej. ABW jest również aktywnym uczestnikiem Międzyresortowego Zespołu do spraw Zwalczania Nieprawidłowości Finansowych na Szkodę Rzeczpospolitej Polskiej lub Unii Europejskiej.[6)]

Wydaje się, że do przedstawionego powyżej katalogu kompetencji ABW powinno być dodane przeciwdziałanie przestępstwom związanym z prywatyzacją mienia Skarbu Państwa. „Prywatyzacja" znaczy tyle samo co przekazywanie majątku państwowego podmiotom prywatnym, przekształcanie gospodarki państwowej w gospodarkę prywatną, ograniczanie roli państwa w gospodarce. Jest to proces prowadzący do zmiany kontroli nad gospodarką i zmiany własności społecznej w prywatną. Co do rodzajów przestępstw związanych z prywatyzacją spółek Skarbu Państwa, wymienić należy art. 296 kk.

Podsumowując należy stwierdzić, iż przestępstwa „godzące w podstawy ekonomiczne państwa" to takie, które mogą spowodować zakłócenie sprawności funkcjonowania państwa w realizacji przez nie funkcji wynikających m.in. z ustawy zasadniczej, tj. Konstytucji. Ma to znaczenie o tyle istotne, że przedsiębrane przez państwo dzia-

[6)] Zob. oficjalna strona internetowa Agencji Bezpieczeństwa Wewnętrznego, www.abw.gov.pl.

łania powinny prowadzić do identyfikowania się z nimi obywateli. Z tego też powodu można powiedzieć, że efektywne zwalczanie przez ABW przestępstw godzących w podstawy ekonomiczne państwa to jedna z najważniejszych kompetencji tej instytucji.

ABSTRACT

In the present article the authors took attempts to define a scope of the crime‘s name aimed at country‘s economic basic. This notion was not defined at binding legal regulations, and particularly in the legacy of the act of ABW and AW. This legacy was not also defined at any other act. Taking into consideration the mentioned matter, the authors realized that the most precise answer the questions presented in this article allows for the proper use of legacy enclosed in the article 5 part 1 point 2 letter b act of ABW and AW. Considerations undertaken in the publication led the authors to the conclusion that the most proper way is the define the legacy enclosed in the act “crimes aimed at country‘s economic basis” in a descriptive way.

V.
RECENZJE

Piotr Chlebowicz

Metody sztucznej inteligencji

E. Nawarecki, G. Dobrowolski, M. Kisiel – Dorohnicki (red.) *Metody sztucznej inteligencji w działaniach na rzecz bezpieczeństwa publicznego****, Kraków 2009, Wydawnictwa AGH, s. 291.***

Recenzowana monografia prezentuje wyniki projektów badawczo-rozwojowych realizowanych w Katedrze Informatyki AGH w Krakowie w związku z udziałem Katedry w pracach Polskiej Platformy Bezpieczeństwa Wewnętrznego. Zasługuje ona na uwagę gdyż w interesujący sposób przedstawia potencjały nowych narzędzi informatycznych w zakresie zwalczania zaawansowanych form zjawiskowych przestępczości, w tym przestępczości zorganizowanej i ekonomiczno - finansowej, jak również terroryzmu i aktywności obcych wywiadów. Warto zwłaszcza zwrócić uwagę, iż omawiana publikacja AGH łączy w sobie zarówno wymiar „technologiczny", jak i prawny. W związku z powyższym, adresowana jest nie tylko do przedstawicieli nauk technicznych, ale także do prawników karnistów, kryminologów i kryminalistyków. Ze względu na obszerność i złożoność materii zawartej w 13 rozdziałach, należy skoncentrować się na wybranych kwestiach, najbardziej istotnych z punktu widzenia bezpieczeństwa wewnętrznego.

Znaczna część rozważań dotyczy propozycji usprawnień narzędzi informatycznych wykorzystywanych w ramach wywiadu kryminalnego. Zagadnienie analizy kryminalnej będącej centralnym elementem wywiadu jest oczywiście znane zarówno praktyce policyjnej, jak i środowiskom akademickim, lecz Autorzy proponują oryginalne rozwiązanie polegające na uzupełnieniu katalogu technik analitycznych o metody badań sieci społecznych (*Social Network Analysis*). Otwiera to nowe możliwości w zakresie analizy kryminalnej w szczególności przy ustalaniu powiązań osobowych. Na marginesie trzeba zauważyć, iż znaczenie SNA wzrasta, gdyż opiera się na trafnych socjologicznych koncepcjach sieci społecznych, które wiernie odzwierciedlają stosunki społeczne ery informacyjnej. Pierwotnie wymieniona metoda była wykorzystywana w obrocie cywilnym. Wymienia się tutaj na przykład badania struktur organizacji, analizę relacji pomiędzy firmami i instytucjami, a nawet przy badaniach współautorstwa i cytowań w literaturze naukowej. Obecnie jednak SNA jest również wykorzystywana, zwłaszcza w USA, przez instytucje odpowiedzialne za bezpieczeństwo (systemy *CrimeNet Explorer*, COPLINK, NETEST). Polska koncepcja metody identyfikacji struktury związków i grup przestępczych zawarta jest w narzędziu informatycznym KASS (Kryminalna Analiza Sieci Społecznych).

KASS wykorzystuje w swym działaniu możliwość odtworzenia sieci społecznej na podstawie bilingów telefonicznych. Szczegółowe omawianie parametrów tej aplikacji nie mieści się w ramach recenzji. Warto jednak w tym miejscu wskazać, iż jeden z elementów KASS odnosi się do typologii ról, które mogą pełnić przestępcy (terroryści) w sieci społecznej opracowanym przez J. Arquillę i D. Ronfeldt'a analityków znanego *think tanku* RAND. W związku z powyższym wydaje się, iż powstaje dylemat posłużenia się metodami sieci badań społecznych w aspekcie kryminalistycznym i dowodowym. Chodzi o to, czy terminologia zaproponowana przez Autorów KASS,

w szczególności zaś rozbudowana typologia ról w organizacji przestępczej (11 ról) będzie „kompatybilna" ze schematami pojęciowymi i nomenklaturą używaną przez prawników i funkcjonariuszy organów ścigania. Kwestia ta będzie istotna choćby z tego względu, iż argumentowanie w sporach prawnych (w tym konkretnym przypadku udowodnienie udziału określonej osoby - podejrzanego lub oskarżonego w zorganizowanej grupie) opiera się na prawniczej interpretacji rzeczywistości. Wydaje się zatem, iż typologia ról funkcjonująca w ramach KASS nie będzie mogła mieć bezpośredniego zastosowania w postępowaniu przygotowawczym i sądowym. Użytkownicy KASS będą zatem mogli w swych analizach opierać się na dotychczasowych typologiach (ale tylko wyłącznie w ramach czynności operacyjno-rozpoznawczych, lub analityczno-informacyjnych), lecz w przypadku gdyby analiza miała stanowić fragment materiału dowodowego, używanie sformułowań „izolator", „komunikator", „strażnik" nie byłoby z punktu widzenia taktyki śledztwa i ewentualnego procesu karnego właściwym zabiegiem. Jest tak również dlatego – pomijając podane wyżej argumenty – iż prawniczy sposób myślenia nie obejmuje sformułowań, które nie mają żadnego związku z obowiązujacym stanem prawnym i tradycyjną kryminalistyką. Z drugiej jednak strony, rewolucja informatyczna i realia stechnicyzowanego świata muszą wpływać na taktykę i technikę kryminalistyczną XXI wieku. Można natomiast zaproponować, aby typologia ta mogła być przekształcona w argumentację o charakterze prawniczym. Przykładowo można wskazać, iż rola X jest kierownicza, istotna, drugorzędna, peryferyjna i poprzez opis zachowań X uzasadnić wymienione stwierdzenia.

Powyższe rozważania na kanwie fragmentu opracowania AGH stanowią jedynie przyczynek do szerszego zagadnienia wskazania miejsca analizy kryminalnej w praktyce śledczej. Obecnie, bowiem, analiza kryminalna i rozwijane instrumentarium informatyczne znajduje swe zastosowanie przede wszystkim w płaszczyźnie wykrywczej a nie dowodowej. Z tym faktem należy się liczyć, gdyż pomimo zwiększających się możliwości technologicznych i technicznych narzędzi informatycznych (w tym również narzędzi wspierających analizę kryminalną) w zakresie uzyskiwania i łączenia danych w logiczną całość, wyniki procesów przetwarzania informacji nie zawsze będą możliwe do wykorzystania procesowego.

Trzeba również dodać, iż KASS stanowi zaledwie jeden z komponentów narzędzi informatycznych określanych mianem Zintegrowanego Środowiska Analizy Kryminalnej. Narzędzia tworzące Zintegrowane Środowisko umożliwiają analizę danych pochodzących z różnych źródeł (bazy danych, bilingi) i wizualizację uzyskanych wyników. Istota tego instrumentu sprowadza się do ekstrakcji informacji ze źródeł elektronicznych, w szczególności Internetu. Tym samym, wymieniony produkt informatyczny w połączeniu z systemem IBIS stanowi idealne narzędzie do prowadzenia białego wywiadu. Dużym atutem omawianych aplikacji jest wysoki stopień automatyzacji wyszukiwania i selekcji danych, co korzystnie wpływa na ekonomikę prac analitycznych. Wydajność tego systemu jest duża, gdyż podstawowe moduły IBIS zapewniają możliwość przeanalizowania zbioru obiektów liczącego kilkadziesiąt milionów stron.

Niewątpliwie interesującym aspektem monografii jest rozdział dotyczący analizy przepływów finansowych, w którym przedstawiony został *modus operandi* prania brudnych pieniędzy. Techniki stosowane przez „praczy" stanowią punkt odniesienia dla konstrukcji prototypu systemu wspomagającego analityka w zakresie spraw z art. 299 kk. Jako ostatni, ale nie najmniej ważny można wskazać opis funkcjonowania systemu „Wizjer", który monitoruje aktywność użytkowników komputerów oraz techniki zarządzania dokumentami tekstowymi w postaci elektronicznej.

Reasumując należy stwierdzić, iż recenzowana publikacja prezentuje oryginalny dorobek zespołu badawczego Katedry Informatyki AGH. *Novum* tego opracowania polega na tym, iż technologie informatyczne i oparte na tych technologiach narzędzia zostały zaprojektowane w celu podniesienia efektywności działań organów i instytucji odpowiedzialnych za bezpieczeństwo narodowe kraju. Ważnym zagadnieniem jest także wykorzystanie najnowszych osiągnięć techniki kryminalistycznej nie tylko w celach wykrywczych lub analityczno – informacyjnych, lecz również procesowych. W literaturze przedmiotu dostrzega się bowiem, iż rozwój nauki powoduje konieczność uwzględniania w procesach tzw. dowodów naukowych. Wydaje się, iż niniejsza publikacja może stanowić punkt wyjścia do dalszych poszukiwań nowych możliwości zarówno w sferze wykrywczej, jak i dowodowej.

Jan Larecki

Roger Faligot, *Tajne służby chińskie* (*Od Mao do igrzysk olimpijskich*), Katowice 2009

R. Faligot, francuski dziennikarz i badacz historii służb specjalnych różnych państw, znany jest już polskiemu czytelnikowi, przede wszystkim jako współautor (z Rémi Kaufferem) znakomitej pracy *Służby specjalne. Historia wywiadu i kontrwywiadu na świecie* (Warszawa 1998). Omawiana pozycja, tym razem napisana samodzielnie, jest chronologiczną kontynuacją innej ich wspólnej publikacji – *Tajne służby Chin 1927-1987* (Warszawa 1994).

Z lektury książki wynika jednoznacznie, że w przeciwieństwie do wielu państw, służby bezpieczeństwa i wywiadu różnej proweniencji tworzą w Chińskiej Republice Ludowej trzeci – obok partii i wojska – mocny filar władzy. Służby te ze względów konspiracji notorycznie zmieniają swe nazwy. Do 1985 r. właściwie nie znano ich struktur, a obecnie wciąż należą do najmniej rozpoznanych na świecie. Jak rodzynki z ciasta trzeba wydłubywać z tekstu dane dotyczące organizacji czy obsady kadrowej służb partyjnych, cywilnych (rządowych) czy wojskowych, żmudnie gromadzone przez autora. Od lat 30. XX wieku bowiem nalezy do tradycji chińskiej fakt, że prawie każdy liczący się polityk chciał mieć swoje służby specjalne i grać nimi na giełdzie stanowisk i wpływów. I trudno się temu dziwić. Przecież to Chiny są ojczyzną Su Tzu, dowódcy i stratega sztuki wojennej, pierwszego człowieka na świecie, który opracował kodeks zasad prowadzenia działań szpiegowskich.

Cechą charakterystyczną działań służb chińskich jest korzystanie (podobnie jak w przypadku Mossadu z diaspory żydowskiej) z licznej, rozsianej po całym świecie, kolonii osób narodowości chińskiej. Co więcej, nie są to tylko imigranci polityczni, którym udało się uciec spod jarzma komunistycznego reżimu, lecz w dużej mierze osoby świadomie i celowo wysyłane za granicę na studia, w poszukiwaniu pracy itp. Tworzą one w ten sposób zaplecze w postaci ogromnej bazy operacyjnej. Wśród tego typu osób jest liczna grupa (nikt nie potrafi określić, jak liczna) uplasowana w interesujących, bądź mogących się stać ważnymi, w sferach nielegalnych pracowników operacyjnych zwanych eufemistycznie „rybami wielkich głębin". Jak wiadomo z licznych afer szpiegowskich, ujawnianych głównie w Stanach Zjednoczonych (ale nie tylko), wielu Chińczyków często zajmuje niezbyt wysokie stanowiska w instytucjach strategicznych, dające im dostęp do newralgicznych danych. Nie bez kozery, więc, (vide - omawiany raport DNI *The National Intelligence Strategy of the United States of America,* August 2009) funkcjonariusze wywiadu USA wśród priorytetów zainteresowania wywiadowczego plasują Chiny wyżej niż Rosję. Bowiem zakres prowadzonego przez Chiny szpiegostwa gospodarczego, technologii wojskowych i przygotowań do wojny informatycznej (liczne oddziały wysokiej klasy hakerów wojskowych) sprawiają, że kraj ten urasta do rangi groźnego przeciwnika.

W tym miejscu warto przytoczyć celną ocenę autora: *Chińskie służby specjalne stały się na początku XXI w. największymi na świecie. Przynajmniej pod względem liczby funkcjonariuszy, oficerów prowadzących i agentów, nawet jeżeli nie osiągnęły jeszcze poziomu technologicznego Amerykanów. Ale doganiają ich*. Silna, scentralizowana władza aparatu partyjno-rządowego w połączeniu z dynamicznym rozwojem gospodarki rynko-

wej, narodową cierpliwością i pracowitością, o populacji już nie wspominając, sprawiają, że w niedalekiej przyszłości kraj ten może stać się pod wieloma względami mocarstwem nr 1.

W świetle postępującej globalizacji działań chińskich tajnych służb należy postawić pytanie retoryczne, czy Polska, członek NATO i Unii Europejskiej, już znajduje się bądź wkrótce znajdzie się w sferze ich wywiadowczej penetracji. Otwartą kwestią pozostaje również to, w jakim zakresie nasz kraj będzie obiektem ich operacyjnego zainteresowania oraz czy nasze służby przygotowane są na taką konfrontację.

VI.
WYDARZENIA

Marta Bykas-Strękowska
Sławomir Szczepańczyk
Dariusz Laskowski

Sprawozdanie z pokazu technicznego zabezpieczenia śladów kryminalistycznych w miejscu symulowanego wybuchu

W dniu 19 września 2009 r. weszła w życie ustawa z dnia 17 lipca 2009 r. o zmianie ustawy o zarządzaniu kryzysowym, ogłoszona w Dzienniku Ustaw nr 131, poz. 1076 z dnia 19 sierpnia 2009 r.

Zgodnie z częścią zapisów wyżej wymienionej nowelizacji, zadania z zakresu przeciwdziałania, zapobiegania i usuwania skutków zdarzeń o charakterze terrorystycznym mają być realizowane we współpracy z organami administracji rządowej właściwymi w tych sprawach, w szczególności z Szefem Agencji Bezpieczeństwa Wewnętrznego. Szefowi ABW nadano prawo do udzielania zaleceń organom i podmiotom zagrożonym działaniami o charakterze terrorystycznym oraz przekazywania im niezbędnych informacji służących przeciwdziałaniu tym zagrożeniom, a także nałożono obowiązek informowania dyrektora Rządowego Centrum Bezpieczeństwa o podjętych działaniach.

Zgodnie z tą nowelizacją, Szef ABW jest również zobowiązany do koordynacji przygotowania Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń o charakterze terrorystycznym, mogących doprowadzić do sytuacji kryzysowej.

Rozwiązania te mają służyć skuteczniejszej realizacji ustawowych zadań Agencji Bezpieczeństwa Wewnętrznego, o których mowa w art. 5 ust. 1 pkt. 2 lit. a ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, to jest rozpoznawaniu, zapobieganiu i wykrywaniu przestępstw terroryzmu. Przy obecnie obowiązującym stanie prawnym właśnie najszersze kompetencje (zadania) w zakresie działań antyterrorystycznych zostały przyznane ABW.

Biorąc powyższe pod uwagę, niezbędne jest podejmowanie działań mających na celu utrzymywanie na stałym, wysokim poziomie umiejętności związanych m.in. z ujawnianiem i zabezpieczaniem śladów z miejsca zdarzenia po zamachu terrorystycznym, a także przeprowadzanie wspólnych szkoleń z innymi służbami zajmującymi się zwalczaniem terroryzmu, zmierzających zarówno do wypracowania wspólnych rozwiązań w tym zakresie, jak i zapoznania się z możliwościami skutecznego wykorzystania tych służb w przypadku zaistnienia zdarzenia o charakterze terrorystycznym.

W dniu 27 listopada 2009 r. Biuro Badań Kryminalistycznych ABW przygotowało i przeprowadziło szkolenie (w formie pokazu) z zakresu zabezpieczenia miejsca zdarzenia po zamachu terrorystycznym, z wykorzystaniem materiałów wybuchowych i substancji promieniotwórczych. Pokaz obserwował Szef ABW, płk Krzysztof Bondaryk, wraz z zastępcą – płk. Zdzisławem Skorżą. Pokaz ten miał na celu zapoznanie zaproszonych przedstawicieli jednostek organizacyjnych ABW (Centrum Antyterrorystyczne, Departament Przeciwdziałania Terroryzmowi, Departament Postępowań Karnych, Departament Ochrony Ekonomicznych Interesów Państwa i Zwalczania Przestępczości Zorganizowanej) ze skutkami zamachu bombowego, wyglądem miejsca po wybuchu oraz problemami występującymi podczas działań różnych służb na miej-

scu takiego zdarzenia. W pokazie brali czynny udział eksperci Biura Badań Kryminalistycznych ABW, symulując współpracę z poszczególnymi służbami oraz biorąc udział w praktycznych czynnościach procesowych, ujawnianiu i zabezpieczaniu śladów kryminalistycznych.

Do udziału w pokazie zaproszono następujące służby i osoby:

1. Sekcję minersko-pirotechniczną Komendy Stołecznej Policji,
2. Jednostkę ratowniczo-gaśniczą nr 6 Komendy Państwowej Straży Pożarnej m.st. Warszawy,
3. Sekcję techników kryminalistycznych Komendy Stołecznej Policji,
4. Laboratorium Kryminalistyki Komendy Stołecznej Policji (eksperci),
5. Pana dr. Wojciecha Pawłowskiego – biegłego sądowego, pracownika LK KSP Policji,
6. Inspektora ochrony radiologicznej – kierownika Działu Bezpieczeństwa Ośrodka Radioizotopów Instytutu Energii Atomowej POLATOM,
7. Ekspertów Biura Badań Kryminalistycznych ABW.

Nad bezpieczeństwem gości i uczestników czuwał zespół ratownictwa medycznego.

Scenariusz pokazu uwzględniał:

- wybuch samochodu pułapki,
- przeprowadzenie rozpoznania pirotechnicznego w celu ujawnienia ewentualnych innych ładunków wybuchowych,
- rozbrojenie ujawnionych ładunków wybuchowych,
- przeprowadzenie akcji ratowniczo-gaśniczej z elementami dodatkowego rozpoznania chemicznego,
- przeprowadzenia rozpoznania obecności substancji promieniotwórczych i ich zabezpieczenie,
- zabezpieczenie miejsca wybuchu,
- przeprowadzenie czynności procesowych,
- ujawnienie i zabezpieczenie śladów kryminalistycznych oraz śladów powybuchowych.

Fot. 1. Urządzenie wybuchowe i sposób jego podłożenia.

Przebieg pokazu

Samochód osobowy został zaminowany przy pomocy urządzenia wybuchowego zawierającego ok. 800 gramów heksogenu – jednego z najsilniejszych kruszących materiałów wybuchowych, często wykorzystywanego w armiach całego świata (fot. 1).

Urządzenie wybuchowe ulokowano poza samochodem, na betonowej płycie, pod tylnym siedzeniem z prawej strony. Wewnątrz samochodu pozostawiono liczne ślady daktyloskopijne i biologiczne naniesione na niedopałki papierosów i plastikowe butelki po napojach. Na zewnętrznej powierzchni drzwi i maski również naniesiono ślady daktyloskopijne. Wnętrze samochodu oblano benzyną. Dodatkowy ładunek wybuchowy skonstruowany z ok. 200 gramów heksogenu (fot. 2) i zawierający element symulujący obecność materiałów promieniotwórczych ulokowano w odległości 50 metrów od samochodu.

Fot. 2. Wykonanie dodatkowego urządzenia wybuchowego.

Detonacja (z tzw. „efektem generalskim" – niewielkie problemy techniczne) spowodowała znaczne uszkodzenie samochodu i jego zapalenie. W związku z tym pierwsza na miejsce zdarzenia wkroczyła Państwowa Straż Pożarna. Jest to szczególnie krytyczna część akcji, gdyż z powodu pożaru nie można przeprowadzić rozpoznania pirotechnicznego i ratownicy narażeni są na możliwość wybuchu innych, specjalnie w tym celu pozostawionych urządzeń wybuchowych (fot. 3 i 4).

Przeprowadzono akcję gaśniczą i dokonano wstępnego rozpoznania chemicznego oraz obecności substancji promieniotwórczych (fot. 5)

Po przeprowadzeniu tych czynności funkcjonariusze sekcji minersko-pirotechnicznej KSP rozpoczęli poszukiwanie dodatkowych ładunków wybuchowych. Zlokalizowana została podejrzana torba, której prześwietlenie za pomocą przenośnego zestawu RTG ujawniło obecność urządzenia wybuchowego (fot. 6).

Fot. 3. Po wybuchu – jednostka Państwowej Straży Pożarnej wkracza do akcji.

Fot 4. Akcja gaśnicza.

Fot. 5. Funkcjonariusz PSP dokonuje rozpoznania chemicznego i pomiaru poziomu promieniowania jonizującego.

Fot. 6. Pirotechnik w tzw. stroju podchodzeniowym z elementami zestawu RTG.

Fot. 7. „Działko wodne" ustawione przy torbie zawierającej urządzenie wybuchowe.

Fot. 8. Po użyciu „działka wodnego".

W torbie wykryto również obecność materiału promieniotwórczego. Ponieważ po neutralizacji elementy urządzenia wybuchowego rozpadły się na przestrzeni do 10 metrów, inspektor ochrony radiologicznej, przy pomocy własnego zestawu czujników, ponownie zlokalizował materiał promieniotwórczy i zabezpieczył go w odpowiednim ołowianym pojemniku (fot. 9).

Resztki substancji podobnej do materiału wybuchowego poddane zostały analizie przy pomocy ręcznego detektora działającego w oparciu o metodę IMS (ang. *Ion Mobility Spectroscopy* – spektroskopia mobilnych jonów). Ręczny analizator prawidłowo zidentyfikował NN substancję jako heksogen – kruszący materiał wybuchowy. W trakcie opisanych powyżej czynności Straż Pożarna rozwinęła przenośne stanowisko do de-

Fot. 9. Element promieniotwórczy.

kontaminacji[1)] substancji chemicznych i promieniotwórczych, a Policja zaprezentowała działanie robota pirotechnicznego.

Na tym etapie zakończono najbardziej widowiskowe czynności gaśnicze i pirotechniczne, a zwolnione miejsce zdarzenia zajęli eksperci kryminalistyki z BBK ABW, LK KS Policji oraz technicy KS Policji wraz z funkcjonariuszami dochodzeniowo-śledczymi. Miejsce zdarzenia zostało podzielone na sektory ułatwiające i przyspieszające dokonanie oględzin. W każdym sektorze przeprowadzano czynności dochodzeniowo-śledcze oraz niezależnie od siebie ujawniano, dokumentowano i zabezpieczano ślady kryminalistyczne. Najważniejszymi czynnościami było ustalenie miejsca wybuchu i ujawnienie jak największej ilości fragmentów urządzenia wybuchowego (fot. 10 i 11).

Z ustalonego miejsca wybuchu (w którym zdetonował ładunek wybuchowy) pobrano do analiz laboratoryjnych ziemię. Analizy wskażą na rodzaj materiału wybuchowego użytego do zamachu.

Podczas oględzin ujawnione zostały liczne fragmenty urządzenia wybuchowego. Ich późniejsza analiza w laboratorium pozwoli odtworzyć budowę, użyte materiały i sposób działania tego urządzenia. Wykryte, udokumentowane i zabezpieczone ślady składowano w specjalnie wyznaczonym miejscu, pod nadzorem odpowiedzialnego funkcjonariusza. Po dokonaniu oględzin pokaz zakończono.

Wnioski

Można zadać pytanie o celowość tego typu ćwiczeń. Jednakże poznanie sposobu działania innych służb w trakcie wspólnych ćwiczeń służy wzajemnemu zrozumieniu wykonywanych obowiązków, a wytworzenie pozytywnych relacji pomiędzy służbami zapewnia skuteczne współdziałanie w trakcie rzeczywistych wydarzeń. Miejsce zama-

[1)] Dekontaminacja – dezaktywacja, odkażanie, usuwanie skażeń promieniotwórczych, etc. Źródło: http://encyklopedia.pwn.pl.

chu terrorystycznego, oprócz zniszczonych konstrukcji, będzie wypełnione ofiarami, które muszą być ratowane bez zwracania uwagi na pożary, materiały promieniotwórcze, dodatkowe bomby czy ewentualne ślady kryminalistyczne. Umiejętność współpracy kilku służb (Policja, Państwowa Straż Pożarna, ABW) może okazać się kluczowa dla skutecznej likwidacji skutków zamachu, zminimalizuje negatywny wpływ przeprowadzonej akcji na wartość dowodową śladów kryminalistycznych. Organizując pokaz mieliśmy przede wszystkim na względzie przećwiczenie umiejętności takiej współpracy.

Fot. 10. Samochód po eksplozji. W głębi widoczna wyznaczona do oględzin strefa, w której ujawniono element promieniotwórczy.

Fot. 11. Jeden z ujawnionych śladów kryminalistycznych. Butelka po napoju z wnętrza samochodu.

20 LAT

URZĄD OCHRONY PAŃSTWA URZĄD OCHRONY PAŃSTWA URZĄD OCHRONY PAŃSTWA

EŃSTWA WEWNĘTRZNEGO AGENCJA BEZPIECZEŃSTWA WEWNĘTRZNEGO AGENCJA BEZPIECZEŃSTWA

Sztandar Agencji Bezpieczeństwa Wewnętrznego.

Obchody 20-tej rocznicy utworzenia cywilnych służb specjalnych w demokratycznej Polsce

6 kwietnia 2010 roku przypadła 20. rocznica uchwalenia przez Sejm Rzeczypospolitej Polskiej ustawy o Urzędzie Ochrony Państwa (UOP). Powołanie nowej cywilnej służby specjalnej, w miejsce peerelowskiej Służby Bezpieczeństwa, zostało uczczone zorganizowaniem uroczystości upamiętniających to wydarzenie. Organizatorem obchodów święta była Agencja Bezpieczeństwa Wewnętrznego (ABW), służba utworzona w 2002 r. po rozwiązaniu UOP. Z tej okazji m.in. została wydany znaczek Poczty Polskiej i okazjonalna koperta. Jest to kolejna edycja w 20 – letniej historii służb specjalnych po 1989 r.

Obchody 20-lecia cywilnych służb specjalnych w demokratycznej Polsce zainaugurowali zapaleniem znicza i złożeniem kwiatów w Kaplicy Katyńskiej w Katedrze Polowej Wojska Polskiego w Warszawie Szef ABW, płk Krzysztof Bondaryk i Sekretarz Kolegium ds. Służb Specjalnych, minister Jacek Cichocki.

Następnie w Katedrze została odprawiona msza święta, którą koncelebrowali m.in. biskup polowy WP gen. dyw. prof. dr hab. Tadeusz Płoski i rektor Uniwersytetu Kardynała Stefana Wyszyńskiego ks. prof. dr hab. Ryszard Rumianek. W eucharystii uczestniczyli przedstawiciele władz państwowych, reprezentanci i poczty sztandarowe służb mundurowych, dotychczasowi szefowie UOP i ABW, przedstawiciele środowisk kombatanckich oraz funkcjonariusze i obecne kierownictwo Agencji. Nabożeństwo poprzedził kapelan ABW ks. prałat komandor dr Leon Szot, cytując słowa papieża Jana Pawła II: […] *proszę was byście z zaangażowaniem czynili słowo „służyć" mottem waszego życia* […].

Fot. 1. Szef ABW, płk Krzysztof Bondaryk i Sekretarz Kolegium ds. Służb Specjalnych, minister Jacek Cichocki w Kaplicy Katyńskiej w Katedrze Polowej Wojska Polskiego.

Msza w 20. rocznicę utworzenia cywilnych służb specjalnych była również okazją do nadania Agencji Bezpieczeństwa Wewnętrznego nowego symbolu tożsamości – sztandaru z wyhaftowanym godłem Polski i emblematem ABW, oraz słowami: Bóg, Honor, Ojczyzna.

Bp. T. Płoski poświecił sztandar, a jego symbolicznego wręczenia dokonał prezes Światowego Związku Żołnierzy Armii Krajowej, ppłk Czesław Cywiński. W imieniu Agencji sztandar odebrał Szef ABW, który po zaprezentowaniu wszystkim uczestnikom uroczystości został przekazany pocztowi sztandarowemu.

Płk Krzysztof Bondaryk przekazał na ręce bp. T. Płoskiego godło ABW jako wotum dziękczynne. Kończąc tę część uroczystości Szef Agencji oświadczył: *Dwadzieścia lat temu, 6 kwietnia 1990 r. Sejm przyjął ustawę o Urzędzie Ochrony Państwa. To również 20 lat temu , 6 kwietnia 1990r. Sejm przyjął ustawę przywracającą Święto Konstytucji 3 maja. W tym dniu więc z jednej strony powołano do życia nową służbę demokratycznego , niepodległego państwa , z drugiej przywrócono historyczny symbol jego suwerenności. Jesteśmy dumni z faktu, że przyszło nam żyć i pracować dla niepodległego kraju, strzec jego bezpieczeństwa wewnętrznego i ładu konstytucyjnego. Od dziś naszej służbie będzie towarzyszył sztandar, symbol naszej tożsamości, szacunku dla tradycji i wierności zasadom. Sztandar przejęliśmy z godnych rąk, z rąk żołnierzy Armii Krajowej. Mogę zapewnić Was, że trafił on w godne ręce, ręce funkcjonariuszy Agencji Bezpieczeństwa Wewnętrznego, którzy są kolejną zmianą w długiej sztafecie pokoleń, dla których Polska jest dobrem najwyższym.*

Zgromadzeni w Katedrze wysłuchali homilii bp. T. Płoskiego, podczas której powiedział m.in. […] *Łączymy się dziś w radości z funkcjonariuszami i pracownikami ABW, dla których data 6 kwietnia 2010 roku zostanie zapisana jako wielkie wydarzenie w dziejach Agencji, gdyż poświęcenie i wręczenie sztandaru ma dla każdej formacji olbrzymie znaczenie* […] *Po grecku „sztandar" znaczy „hegemonia". Chodzi tu*

o konieczne władztwo czterech zasad, które będą określać tych wszystkich, którzy będą gromadzić się pod tym sztandarem. Te cztery zasady to: Bóg, Honor, Ojczyzna i Agencja Bezpieczeństwa Wewnętrznego. Zwracając się wprost do funkcjonariuszy ABW zauważył, że w zmaterializowanym świecie bez idei to działalność ABW […] *chroni Polskę i jej ducha.* […] *To Wy funkcjonariusze i pracownicy ABW stoicie na straży uczciwości, to Wy współbudujecie z poświęceniem kraj ojczysty. W szczególnych sytuacjach Ojczyzna domaga się nawet ofiary z życia. Ale w normalnych warunkach domaga się od nas przede wszystkim uczciwości, rzetelności, sprawiedliwości…*

Fot. 2. Szef ABW, płk Krzysztof Bondaryk podczas przekazania wotum bp. Tadeuszowi Płoskiemu

Fot. 3. Poczet sztandarowy ABW w Katedrze Polowej Wojska Polskiego.

Fot. 4. Biskup Polowy WP gen. dyw. prof. dr hab. Tadeusz Płoski podczas homilii.

Spośród zaproszonych gości, w cztery dni po wypowiedzeniu tych słów, w katastrofie pod Smoleńskiem zginęli: biskup polowy WP gen. dyw. prof. dr hab. Tadeusz Płoski, przedstawiciel Ordynariatu Polowego WP ks. Jan Osiński, rektor Uniwersytetu Kardynała Stefana Wyszyńskiego ks. prof. dr hab. Ryszard Rumianek, dowódca Garnizonu Warszawa gen. dyw. Kazimierz Gilarski oraz prezes Światowego Związku Żołnierzy Armii Krajowej ppłk Czesław Cywiński.

Podczas uroczystych obchodów 20-lecia służb specjalnych w siedzibie ABW w Warszawie wręczono wieloletnim funkcjonariuszom UOP i ABW pamiątkowe medale wybite specjalnie na to święto.

Fot. 5. Pamiątkowy medal wybity z okazji 20-lecia służb specjalnych.

Nawiązując do wartości umieszczonych na sztandarze Szef ABW zwrócił się do zebranych słowami odnoszącymi się do codziennej służby: *Funkcjonariusze powinni cenić honor i Ojczyznę i mieć Boga w sercu*.

Obecny na uroczystościach pierwszy szef Urzędu Ochrony Państwa, senator Krzysztof Kozłowski, przypomniał szczególną rolę tych, którzy współtworzyli z nim pierwszą niekomunistyczną służbę specjalną: *Z ogromną wdzięcznością myślę o tych, którzy w roku 1990 przyszli do służby, którym starczyło odwagi i wyobraźni, którzy byli wyjątkiem a nie regułą, którzy nie ulękli się pobrudzenia rąk. Ogromna część społeczeństwa była niechętna temu gmachowi i przemianom, które się tu dokonały.* Podkreślił jednak, że w ciągu tych dwudziestu lat słyszał także słowa, że wszystko było robione *nie tak, że trzeba było rozliczać, zabezpieczać archiwa*.

Jest jednak przekonany, że przemiany, które dokonały się w latach dziewięćdziesiątych w Polsce i w służbach, były niezbędne. *Mieliśmy po swojej stronie premiera, który ufał oraz zespół ludzi, którzy także sobie wzajemnie ufali. Możemy być dumni… Możecie być dumni, że przyłożyliście rękę do czegoś niebywałego. Bowiem rzadko zdarza się w historii, że można brać udział w transformacji państwa. Dziękuję Wam za to, że byliście i że jesteście* – dodał Kozłowski. Ponadto stwierdził, że gdyby ktoś zapytał go, czy warto było, bez wahania odpowiedziałby: Tak trzeba było.

Podczas uroczystości goście podkreślali znaczenie Agencji Bezpieczeństwa Wewnętrznego w systemie bezpieczeństwa państwa. Prezes Światowego Związku Żołnierzy Armii Krajowej płk Czesław Cywiński podkreślił, że mimo, iż Polska jest w Unii Europejskiej i NATO, to nie oznacza, że jest wolna od wszelkich zagrożeń. Dziękując tym wszystkim, którzy włożyli ogromną pracę w tworzenie służb i tym, którzy służą w nich nadal, zaapelował: *Pamiętajcie! Polska na Was liczy.*

Pracę funkcjonariuszy docenił również Marszałek Sejmu Bronisław Komorowski, który mimo nieobecności na uroczystości przysłał list, w którym podkreślił jak ważni są ci, którzy chronili i chronią Polskę. *Waga i znaczenie Państwa pracy jest doceniana szczególnie teraz w dobie globalizacji i zagrożeń teleinformatycznych.*

Na obchody 20-lecia służb specjalnych został zaproszony również Andrzej Milczanowski, który z powodów osobistych nie mógł w nich wziąć udziału. W przysłanym na ręce Szefa Agencji liście złożył życzenia funkcjonariuszom ABW oraz tym, z którymi miał „honor pełnić służbę".

W swoim wystąpieniu w trakcie rocznicowego spotkania pierwszy niekomunistyczny premier RP Tadeusz Mazowiecki zaakcentował, jak ważne jest umacnianie w społeczeństwie świadomości roli państwa i roli ABW. Życzył funkcjonariuszom, by ich działaniom towarzyszyło większe zrozumienie ich pracy. *Takie rocznice są ważne, gdyż pozwalają przywrócić satysfakcję z własnych dokonań* – dodał.

Fot. 6. Szef ABW płk Krzysztof Bondaryk przemawiający podczas uroczystości w siedzibie ABW w Warszawie (w tle były doradca Sejmowej Komisji ds. Służb Specjalnych Michał Stręk, była minister w kancelarii Prezydenta RP Małgorzata Bochenek oraz gen. Zbigniew Nowek).

Fot. 7. Senator Krzysztof Kozłowski przemawiający podczas uroczystości w siedzibie ABW w Warszawie.

Fot. 8. Prezes Światowego Związku Żołnierzy Armii Krajowej płk Czesław Cywiński przemawiający podczas uroczystości w siedzibie ABW w Warszawie.

Fot. 9. Szef ABW płk Krzysztof Bondaryk w rozmowie z Tadeuszem Mazowieckim.

Fot. 10. Pamiątkowe zdjęcie byłego i obecnego kierownictwa UOP i ABW.

ABW i NASK laureatami konkursu „Teraz Polska”

Agencja Bezpieczeństwa Wewnętrznego oraz Naukowa i Akademicka Sieć Komputerowa (NASK) zostały tegorocznymi laureatami konkursu „Teraz Polska” w kategorii Przedsięwzięcia Innowacyjne za system detekcji i wczesnego ostrzegania o zagrożeniach bezpieczeństwa teleinformatycznego sieci administracji Państwa – ARAKIS-GOV.

KAPITUŁA POLSKIEGO GODŁA PROMOCYJNEGO

PRZYZNAJE

POLSKIE GODŁO PROMOCYJNE

TERAZ POLSKA

DLA

NAUKOWEJ I AKADEMICKIEJ SIECI KOMPUTEROWEJ
ORAZ AGENCJI BEZPIECZEŃSTWA WEWNĘTRZNEGO

ZA

system detekcji i wczesnego ostrzegania
o zagrożeniach bezpieczeństwa teleinformatycznego
sieci administracji Państwa arakis.gov

NAGRODZONY
W III EDYCJI KONKURSU
DLA PRZEDSIĘWZIĘĆ INNOWACYJNYCH

PRZEWODNICZĄCY
KAPITUŁY POLSKIEGO
GODŁA PROMOCYJNEGO
prof. Michał Kleiber

PREZES ZARZĄDU
FUNDACJI POLSKIEGO
GODŁA PROMOCYJNEGO
Krzysztof Wrzesiński

WARSZAWA, 24 MAJA 2010 ROKU

Fot. 1. Dyplom Polskie Godło Promocyjne „Teraz Polska”.

System jest wspólnym przedsięwzięciem ABW oraz NASK, a jego głównym zadaniem jest ochrona zasobów teleinformatycznych administracji państwowej. Powstał na potrzeby Rządowego Zespołu Reagowania na Incydenty Komputerowe CERT.GOV.PL, w wyniku rozszerzenia o zaawansowane funkcjonalności systemu ARAKIS opracowanego przez CERT Polska.

ARAKIS-GOV nie jest typowym systemem zabezpieczającym i w żadnym wypadku nie zastępuje funkcjonalności standardowych systemów ochrony sieci, takich jak firewall, antywirus czy IDS/IPS. Unikalność systemu polega na tym, że nie monitoruje

on w żaden sposób treści informacji wymienianych przez chronioną instytucję z siecią Internet. Sondy systemu instalowane są bowiem poza chronioną siecią wewnętrzną instytucji, po stronie sieci Internet.

W chwili obecnej sensory systemu zainstalowane są w ponad 60 urzędach szczebla centralnego. Udział w projekcie ARAKIS-GOV jest bezpłatny.

Fot. 2. Polskie Godło Promocyjne „Teraz Polska”.

VII.
DOKUMENTY

RAPORT Z DZIAŁALNOŚCI ABW ZA 2009 ROK[1)]

I. ROLA ABW W SYSTEMIE BEZPIECZEŃSTWA RP

1. Wprowadzenie

Zapewnienie bezpieczeństwa stanowi jedno z głównych wyzwań, z jakimi musi zmierzyć się współczesny świat, w tym Polska.

Obecnie na całym świecie coraz większego znaczenia nabierają pozamilitarne aspekty zapewnienia bezpieczeństwa. Ewolucji tej towarzyszy zmiana podejścia do walki z pojawiającymi się – nieznanymi do tej pory – zagrożeniami. O skuteczności tej walki decydować będzie innowacyjność, elastyczność oraz profesjonalizm działań. Na znaczeniu zyskuje również profilaktyka zwłaszcza takich zagrożeń o charakterze globalnym, jak: terroryzm, cyberterroryzm, proliferacja broni masowego rażenia oraz międzynarodowa przestępczość zorganizowana.

Tym nowym wyzwaniom są w stanie sprostać przede wszystkim służby specjalne. Unikatowe metody pracy, wyspecjalizowane kadry oraz dostęp do najnowszych osiągnięć technicznych to najważniejsze z czynników, dzięki którym zajmują one obecnie główne miejsce wśród instytucji odpowiedzialnych za ochronę bezpieczeństwa wewnętrznego państwa.

Agencja Bezpieczeństwa Wewnętrznego, rozumiejąc zmiany zachodzące w otaczającej rzeczywistości, stara się wyjść im naprzeciw poprzez dostosowanie swojej działalności do istniejących realiów. Efekty modernizacji struktury i metod pracy ABW to m.in. powołanie do życia Rządowego Zespołu Reagowania na Incydenty Komputerowe *(CERT.GOV.PL)*, nowo powstałe, coraz sprawniej funkcjonujące Centrum Antyterrorystyczne, działania prewencyjne realizowane w ramach Tarczy Antykorupcyjnej oraz program profilaktyki kontrwywiadowczej. Te nowatorskie inicjatywy mają przyczynić się do zwiększenia skuteczności wykonywanych zadań i skupienia się w większym stopniu na zapobieganiu zagrożeniom.

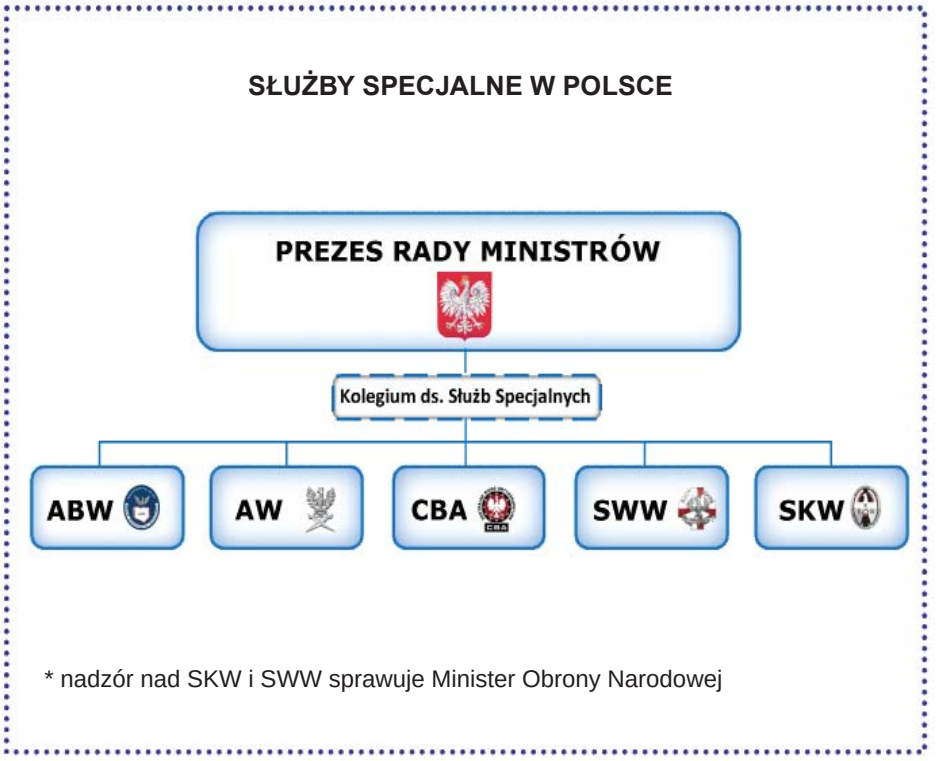
Innym przejawem dostosowywania się Agencji Bezpieczeństwa Wewnętrznego do zmieniających się we współczesnym państwie warunków jest dążenie do przybliżenia Polakom roli i zadań Agencji. W związku z tym w 2009 r. rozpoczęto wydawanie *Przeglądu Bezpieczeństwa Wewnętrznego*, którego celem jest umożliwienie zapoznania się z wybranymi metodami pracy ABW szerszemu gronu odbiorców. Jednocześnie publikacja ma stanowić forum wymiany doświadczeń i poglądów funkcjonariuszy oraz ekspertów i zewnętrznych naukowców.

Agencja Bezpieczeństwa Wewnętrznego chce także popularyzować tematykę dotyczącą służb specjalnych i ogólnie pojętego bezpieczeństwa. Służą temu organizowane konferencje oraz wielotematyczne szkolenia, przeznaczone dla wybranego kręgu odbiorców, głównie przedstawicieli administracji państwowej.

[1)] Raport ukazał się w 2010 roku jako osobne opracowanie.

2. ABW wśród innych służb specjalnych

Agencja Bezpieczeństwa Wewnętrznego została powołana do życia na mocy *Ustawy z dnia 24 maja 2002 r. o ABW oraz AW*, stając się wraz z Agencją Wywiadu spadkobierczynią istniejącego od 1990 r. Urzędu Ochrony Państwa. Jest ona obecnie największą polską służbą specjalną zajmującą kluczową pozycję w systemie bezpieczeństwa wewnętrznego państwa.



Szef ABW koordynuje podejmowane przez służby specjalne czynności operacyjno-rozpoznawcze mogące mieć wpływ na bezpieczeństwo państwa. W tym celu prowadzi centralną ewidencję zainteresowań operacyjnych służb specjalnych.

Szersze informacje na temat struktury ABW, kierownictwa służby oraz aktów prawnych dotyczących działalności Agencji są dostępne na stronie internetowej *www.abw.gov.pl.*

3. Zadania

Ustawodawca nałożył na ABW obowiązek ochrony bezpieczeństwa wewnętrznego oraz porządku konstytucyjnego Rzeczypospolitej Polskiej. Obowiązek ten został sformułowany w art. 5 ust. 1 pkt 1 ustawy o ABW oraz AW, gdzie za podstawo-

wy cel działań Agencji stawia się *rozpoznawanie, zapobieganie i zwalczanie zagrożeń godzących w bezpieczeństwo wewnętrzne państwa oraz jego porządek konstytucyjny, a w szczególności w suwerenność i międzynarodową pozycję, niepodległość i nienaruszalność jego terytorium, a także obronność państwa.*

Agencja Bezpieczeństwa Wewnętrznego realizuje wyżej wymienione zadania w obszarach przedstawionych na poniższym schemacie:

4. Funkcje

Agencja Bezpieczeństwa Wewnętrznego realizuje funkcje: analityczno-informacyjną, operacyjno-rozpoznawczą, dochodzeniowo-śledczą oraz służby ochrony państwa.

Funkcja analityczno-informacyjna jest obecnie najważniejszą funkcją realizowaną nie tylko przez ABW, lecz także przez służby specjalne innych państw. Jest to związane z tym, że w dzisiejszym świecie pierwszoplanową rolę odgrywa informacja.

Warunkiem optymalnego funkcjonowania systemu bezpieczeństwa wewnętrznego państwa jest zapewnienie mu dopływu informacji oraz profesjonalnych analiz wykorzystywanych również przez wymienione w art. 18 Ustawy o ABW oraz AW organy państwa: Prezydenta RP, Prezesa Rady Ministrów, poszczególnych ministrów.

Czynności operacyjno-rozpoznawcze są podstawowym narzędziem realizacji zadań ABW. Są to niejawne oraz przewidziane prawem działania prowadzone przez Agencję w celu pozyskania, sprawdzenia i wykorzystywania informacji o pozostających w jej prawnie uzasadnionym zainteresowaniu osobach, miejscach bądź zdarzeniach.

W trakcie realizacji działań operacyjno-rozpoznawczych oficerowie mogą współpracować z osobami, które nie są funkcjonariuszami Agencji. ABW ma prawo również zwracać się o udzielenie pomocy do innych podmiotów i instytucji.

Czynności operacyjno-rozpoznawcze mogą być prowadzone poprzez zastosowanie kontroli operacyjnej. Polega ona na kontrolowaniu zawartości korespondencji i przesyłek, a także stosowaniu podsłuchów. Zarządzenie kontroli operacyjnej każdorazowo poprzedzane jest zgodą Sądu Okręgowego na podstawie wniosku Szefa ABW, jeśli wcześniej uzyskał on pisemną akceptację Prokuratora Generalnego.

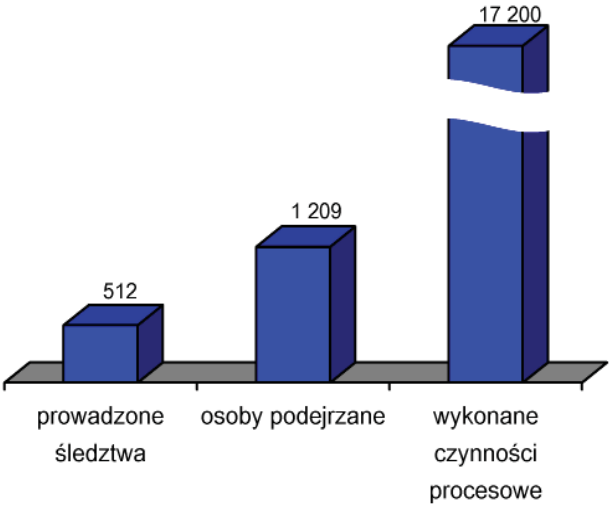
W zależności od rodzaju prowadzonych operacji funkcjonariusze ABW mogą również sprawować niejawny nadzór nad wytwarzaniem, przemieszczaniem i obrotem przedmiotami przestępstwa, jak również stosować elementy prowokacji polegające na ich nabywaniu lub przejmowaniu. Operacje te realizowane są na podstawie zarządzenia Szefa ABW, po uzyskaniu pisemnej zgody Prokuratora Generalnego.

W ramach realizacji ustawowych zadań Agencji funkcjonariusze ABW wykrywają przestępstwa i ścigają ich sprawców. Śledztwa są nadzorowane przez prokuratury różnego szczebla w całym kraju.

Uprawnienia funkcjonariuszy o charakterze procesowym i administracyjno-porządkowym określa art. 23 ustawy o ABW oraz AW.

Zalicza się do nich m.in.:

- zatrzymywanie osób;
- przeszukiwanie osób i pomieszczeń;
- legitymowanie osób;
- stosowanie środków przymusu bezpośredniego;
- kontrolę osobistą.



Rys. 1. Działania pionu postępowań karnych ABW w 2009 roku.

ABW prowadzi również wiele spraw operacyjnych, których liczba, ze względu na ograniczenia wynikające z przepisów ustawy, nie może być ujawniona.

Jednym z aspektów działalności pionu dochodzeniowo-śledczego jest praca Biura Badań Kryminalistycznych ABW.

W 2009 r. Biuro zostało członkiem Europejskiej Sieci Laboratoriów Kryminalistycznych (ENFSI), dołączając tym samym do dwóch innych polskich instytucji wchodzących w jej skład: Centralnego Laboratorium Kryminalistycznego oraz Instytutu Ekspertyz Sądowych.

ENFSI jest renomowaną organizacją międzynarodową, której głównym celem jest rozwój badań kryminalistycznych oraz popularyzowanie nauk sądowych na terenie Europy. ENFSI posiada status monopolisty Unii Europejskiej w dziedzinie kryminalistyki. Oznacza to, że jest jedynym podmiotem opiniotwórczym i doradczym, bezpośrednio konsultującym się z Komisją Europejską, który realizuje zlecenia w postaci opracowywania raportów oraz wydawania rekomendacji z zakresu szeroko pojętej kryminalistyki oraz zagrożeń międzynarodowych.

Biuro Badań Kryminalistycznych jest pierwszym laboratorium służb specjalnych, które zostało włączone w strukturę ENFSI. Członkostwo w tym gremium umożliwi doskonalenie metod pracy funkcjonariuszy ABW w zakresie kryminalistyki, co w przyszłości przełoży się na bardziej efektywną realizację funkcji dochodzeniowo-śledczej przez Agencję.

Od 2009 r. Biuro Badań Kryminalistycznych prowadzi również Centralną Ewidencję Ekspertów Opiniujących. W jej zasobach zarejestrowane są osoby posiadające rozległą wiedzę w obszarach związanych z wykonywanymi przez ABW zadaniami. Wymogiem uzyskania wpisu do ewidencji jest odbycie przez kandydata kilkuletniego szkolenia zakończonego egzaminem.

Realizacja tej funkcji wiąże się z przeciwdziałaniem ujawnianiu tajemnicy państwowej i służbowej oraz sprawdzaniem stanu zabezpieczenia informacji niejawnych. Jest to zadanie szczególnie ważne w kontekście członkostwa Rzeczypospolitej Polskiej w Unii Europejskiej i Pakcie Północnoatlantyckim. ABW realizuje je w trzech obszarach:

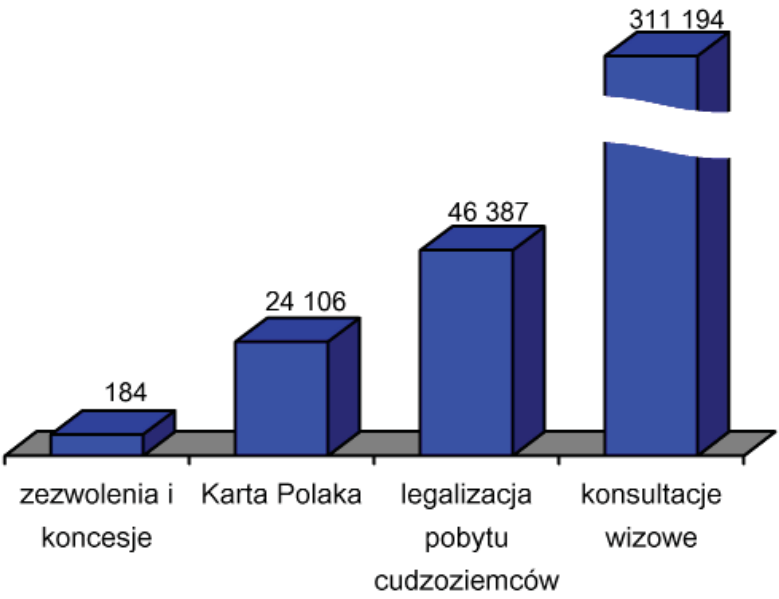
- bezpieczeństwa osobowego – prowadzenie postępowań sprawdzających, których celem jest ustalenie, czy osoba ubiegająca się o zatrudnienie bądź zatrudniona na stanowisku związanym z dostępem do informacji stanowiących tajemnicę państwową lub służbową daje rękojmię jej zachowania;
- bezpieczeństwa przemysłowego – prowadzenie postępowań sprawdzających wobec przedsiębiorców, jednostek naukowych i badawczo-rozwojowych;
- kontroli ochrony informacji niejawnych – ABW jako służba ochrony państwa ma prawo kontrolować przestrzeganie przepisów w zakresie ochrony informacji niejawnych we wszystkich organach władzy publicznej, bankach państwowych i innych państwowych jednostkach organizacyjnych.

W związku z zadaniami dotyczącymi ochrony informacji niejawnych, eksperci Agencji w 2009 r. uczestniczyli w pracach nad nowelizacją ustawy o ochronie informacji niejawnych. Jednym z głównych celów tych zmian jest uproszczenie przepisów i usprawnienie wymiany informacji niejawnych przed objęciem przez Polskę prezydencji w Unii Europejskiej. Przykładowo, nowy wzór ankiety bezpieczeństwa osobowego będzie zgodny ze standardami UE. Zniknie z niej część pytań dotyczących rodziny osób podlegających sprawdzeniom, natomiast uszczegółowiony zostanie blok pytań dotyczących sytuacji finansowej. Docelowo ankieta ma być przystosowana do wypełniania i przekazywania drogą elektroniczną.

W relacjach międzynarodowych instytucja właściwa w sprawach ochrony informacji niejawnych nazywana jest Krajową Władzą Bezpieczeństwa. W sferze cywilnej RP funkcję tę pełni Szef Agencji Bezpieczeństwa Wewnętrznego. ABW jako Krajowa Władza Bezpieczeństwa współpracuje ze strukturami bezpieczeństwa Paktu Północnoatlantyckiego oraz Unii Europejskiej**,** a także z Krajowymi Władzami Bezpieczeństwa państw członkowskich NATO i UE.

5. Działalność opiniodawcza

Agencja Bezpieczeństwa Wewnętrznego uczestniczy w procedurach opiniodawczych dotyczących m.in.: wniosków o przyznanie Karty Polaka, zezwolenia na osiedlenie się obcokrajowców na terytorium Polski czy koncesji na wytwarzanie oraz obrót bronią i amunicją, a także zezwoleń na międzynarodowy handel sprzętem wojskowym i uzbrojeniem.



Rys. 2. Liczba wniosków zaopiniowanych w 2009 roku.

6. Współpraca międzynarodowa

Agencja Bezpieczeństwa Wewnętrznego współpracuje ze służbami specjalnymi i właściwymi organami innych państw. Kontakty międzynarodowe są niezwykle ważne zwłaszcza w kontekście walki z takimi globalnymi zagrożeniami, jak: terroryzm, międzynarodowa przestępczość zorganizowana czy proliferacji broni masowego rażenia.

W 2009 r. ABW prowadziła współpracę z 78. służbami specjalnymi i instytucjami z 49 państw. W zależności od stopnia zaawansowania oraz potrzeb współpraca ta

przybierała formę wymiany informacji, wspólnych spotkań eksperckich, konferencji, a także konsultacji i szkoleń specjalistycznych. W niektórych przypadkach oznaczała również wspólne działania o charakterze operacyjno-rozpoznawczym.

Agencja Bezpieczeństwa Wewnętrznego uczestniczy także aktywnie w pracach:

- Klubu Berneńskiego – forum wymiany doświadczeń służb wewnętrznych państw członkowskich UE oraz Szwajcariii Norwegii;
- Konferencji Europy Środkowej (MEC) – założonej z inicjatywy holenderskiej w celu wspierania procesów demokratyzacji państw byłego bloku wschodniego;
- Grupy ds. Zwalczania Terroryzmu (CTG) – jednej z największych organizacji międzynarodowych zajmujących się zagadnieniem terroryzmu muzułmańskiego i ekstremizmu.

Ponadto, ABW bierze udział w posiedzeniach Komitetu Specjalnego NATO (AC/46), który pełni rolę organu konsultatywnego dla służb bezpieczeństwa państw członkowskich Sojuszu Północnoatlantyckiego.

W 2009 roku funkcjonariusze ABW uczestniczyli również w posiedzeniach Komitetu Bezpieczeństwa NATO oraz w obradach powołanej przez ten komitet specjalnej Grupy Roboczej ds. Zaleceń Dotyczących Wdrażania Polityki Bezpieczeństwa NATO.

Polska wywiera także realny wpływ na tworzenie polityki bezpieczeństwa w zakresie ochrony informacji niejawnych Unii Europejskiej. Funkcjonariusze ABW jako przedstawiciele Krajowej Władzy Bezpieczeństwa brali aktywny udział w posiedzeniach Komitetu Bezpieczeństwa Rady Unii Europejskiej, w trakcie których dyskutowano i opracowano nowe przepisy bezpieczeństwa Rady UE. Agencja reprezentowana jest również na spotkaniach innych organów Komisji Europejskiej, np. Grupy Doradczej Komisji Europejskiej do spraw Polityki Bezpieczeństwa.

ABW odpowiada także za negocjacje oraz zawieranie dwustronnych umów o wzajemnej ochronie informacji niejawnych, regulujących zasady postępowania z informacjami niejawnymi w relacjach RP z innymi państwami. W chwili obecnej Rzeczpospolita Polska związana jest ogólną umową o ochronie informacji niejawnych z 21 państwami.

W 2009 roku weszły w życie umowy o ochronie informacji niejawnych z Francją, Portugalią oraz Litwą. Podpisane zostały również umowy z Macedonią i Słowenią oraz prowadzone były negocjacje umów z Izraelem, Belgią, Cyprem, Słowacją, Luksemburgiem, Afganistanem, Czarnogórą, Kazachstanem, Szwajcarią i Austrią.

Obecnie oficerowie łącznikowi ABW pełnią służbę przy przedstawicielstwach dyplomatycznych RP w Berlinie, Brukseli, Kijowie, Londynie, Moskwie i Pradze.

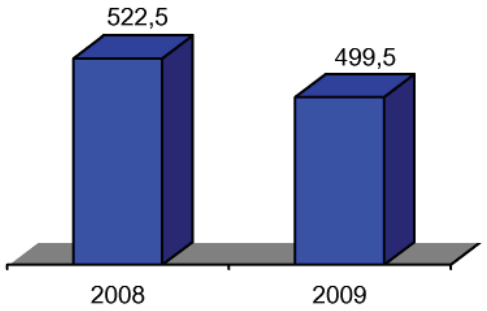
Szef Agencji Bezpieczeństwa Wewnętrznego Krzysztof Bondaryk i Szef Służby Bezpieczeństwa Ukrainy Walenty Naliwajczenko podpisali we wrześniu 2009 r. *Wspólną deklarację Szefów ABW i SBU o realizacji przygotowań do zabezpieczenia EURO 2012*. Obydwie służby uznały za konieczne zapewnienie właściwego poziomu bezpieczeństwa podczas mistrzostw Europy w piłce nożnej na obiektach sportowych i poza nimi. Praktycznym przejawem zawartych uzgodnień były ćwiczenia antyterrorystyczne przeprowadzone na terytorium Ukrainy w październiku 2009 r. z udziałem funkcjonariuszy ABW.

Szczególnym wydarzeniem w 2009 r. było przekazanie przez ABW do zbiorów Muzeum II Wojny Światowej w Gdańsku kompletu mikrofilmowanych materiałów na temat polskich elit politycznych II RP i ich internowania w Rumunii w latach 1939--1945. Materiały te Agencja otrzymała od Rumuńskiej Służby Informacyjnej (SRI).

7. Budżet

Środki finansowe przyznawane są Agencji w ramach ustawy budżetowej. Wydatki ABW w 2009 r. zamknęły się łączną kwotą 499,5 mln zł.

Zarówno planowanie, jak i wykonanie budżetu ABW, podlegają corocznej kontroli ze strony właściwych komisji parlamentarnych oraz Najwyższej Izby Kontroli. Kontrola NIK przeprowadzona w 2009 r. potwierdziła prawidłową realizację budżetu Agencji Bezpieczeństwa Wewnętrznego i przestrzeganie zasad gospodarności, oszczędności i celowości wydatków.

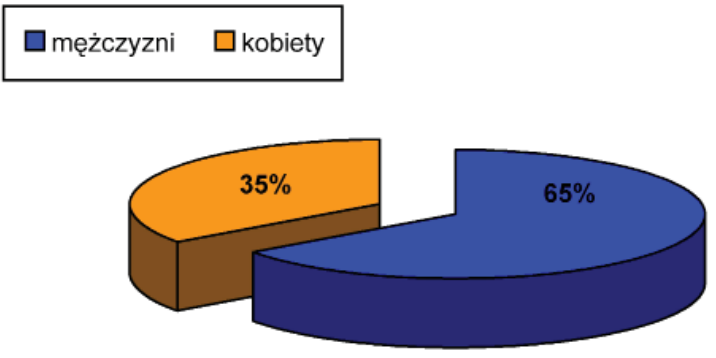


Rys. 3. Budżety ABW w kolejnych latach (w mln zł).

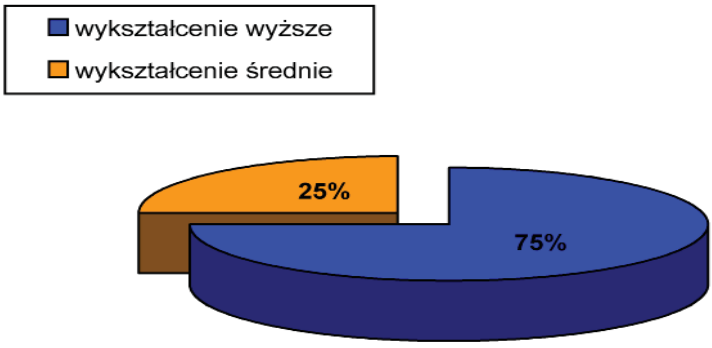
8. Zatrudnienie

Szczególny charakter zadań stawianych ABW przez ustawodawcę implikuje bardzo staranny i rygorystyczny dobór kadr. Służbę w Agencji może pełnić wyłącznie obywatel polski, korzystający z pełni praw publicznych. Osoba taka musi cechować się nieskazitelną postawą moralną, etyczną i patriotyczną.

Liczba etatów, którymi dysponuje ABW corocznie podawana jest w ustawie budżetowej.



Rys. 4. Struktura zatrudnienia funkcjonariuszy ABW wg płci.



Rys. 5. Struktura wykształcenia funkcjonariuszy ABW.

9. Nadzór i kontrola nad ABW

Działalność Agencji Bezpieczeństwa Wewnętrznego kontrolowana jest przez instytucje państwowe posiadające stosowne uprawnienia. Zakres kontroli ograniczony jest przepisami o ochronie informacji niejawnych. Nie oznacza to jednak, że istnieją sfery aktywności ABW wyłączone spod nadzoru tych instytucji. Organami państwowymi uprawnionymi do sprawowania kontroli nad ABW są: Prezydent RP, Prezes Rady Ministrów, sądy, Prokurator Generalny, Sejmowa Komisja ds. Służb Specjalnych oraz Kolegium ds. Służb Specjalnych.

Prezydent RP uprawniony jest do otrzymywania od Szefa ABW informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji naszego kraju. Prezydent wyraża również opinie o zgłoszonym przez premiera kandydacie na stanowisko szefa służby. Szef ABW zobowiązany jest powiadamiać Prezydenta RP o wystąpieniu do Prezesa Rady Ministrów z wnioskiem o udzielenie zgody na prowadzenie czynności operacyjno-rozpoznawczych w sytuacji, gdy sprawa, w zakresie której prowadzone są czynności, należy do kompetencji innych służb lub instytucji.

Prezes Rady Ministrów sprawuje nadzór nad ABW w sposób bezpośredni lub za pośrednictwem powołanego w tym celu ministra koordynującego działalność służb specjalnych. Premier jest również informowany przez Szefa ABW o sprawach mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji Rzeczypospolitej Polskiej.

Kolegium ds. Służb Specjalnych, działające przy Radzie Ministrów, jest organem opiniodawczo-doradczym w sprawach programowania, nadzorowania i koordynowania działalności ABW oraz innych służb. Do zadań Kolegium należy formułowanie ocen lub wyrażanie opinii dotyczących powoływania i odwoływania m.in. Szefa ABW. Ponadto spośród uprawnień kontrolnych Kolegium należy wymienić prawo do opiniowania kierunków i planów działań służb specjalnych, szczegółowych projektów budżetów służb specjalnych, wykonywania powierzonych im zadań oraz rocznych sprawozdań z ich działalności. Kolegium posiada uprawnienia do koordynacji działalności ABW, AW, Służby Kontrwywiadu Wojskowego, Służby Wywiadu Wojskowego i Centralnego Biura Antykorupcyjnego, a także współpracy tych służb z Policją, Strażą Graniczną, Żandarmerią Wojskową, Biurem Ochrony Rządu, Służbą Celną, urzędami skarbowymi, izbami skarbowymi, organami kontroli skarbowej, organami informacji

finansowej i służbami rozpoznania Sił Zbrojnych oraz ich współdziałania w dziedzinie ochrony bezpieczeństwa państwa.

Nadzór i kontrola nad działalnością ABW ze strony sądów i Prokuratora Generalnego jest ściśle związana z działaniami operacyjno-rozpoznawczymi prowadzonymi przez Agencję. Kontrolę operacyjną może zarządzić tylko Sąd Okręgowy w Warszawie, na pisemny wniosek Szefa ABW, jeśli ten ostatni uzyskał wcześniej pisemną zgodę Prokuratora Generalnego na podjęcie tej czynności. Prokurator Generalny musi wydać pisemną zgodę również w przypadku niejawnego nabycia przedmiotu przestępstwa oraz kontrolowanego wręczenia lub przyjęcia korzyści majątkowej. Jest także na bieżąco informowany przez Szefa ABW o przebiegu tego typu operacji. Prokurator Generalny musi być też niezwłocznie powiadomiony przez Szefa ABW o zarządzeniu, przebiegu oraz wynikach czynności podjętych przez funkcjonariuszy Agencji w ramach tzw. przesyłki kontrolowanej. Może również nakazać ich zaprzestanie.

Sejmowa Komisja ds. Służb Specjalnych opiniuje projekty regulacji prawnych dotyczących wszystkich działających w Polsce służb specjalnych, w tym ABW. Komisja wyraża opinię na temat kierunków pracy służb specjalnych, opierając się na informacjach przedstawianych przez ich szefów. Opiniuje również wnioski w sprawie powoływania poszczególnych osób na stanowiska szefów i zastępców szefów. Do zaopiniowania przedstawiane są jej także projekty budżetu państwa w zakresie dotyczącym służb specjalnych oraz sprawozdania z jego wykonania. Ponadto, komisja posiada prawo wydawania ocen na temat współdziałania służb specjalnych z organami administracji państwowej i organami ścigania oraz badania skarg dotyczących ich działalności.

W 2009 r. odbyło się 17 posiedzeń Sejmowej Komisji ds. Służb Specjalnych z udziałem przedstawicieli ABW (z czego dwa w siedzibie Agencji). Dotyczyły one różnych aspektów funkcjonowania Agencji, w tym m.in. zadań związanych z organizacją EURO 2012, efektywności działania Departamentu Postępowań Karnych ABW w zakresie ścigania sprawców przestępstw, kontrwywiadowczej osłony strategicznych gałęzi gospodarki, obrotu towarami o znaczeniu strategicznym oraz procesów prywatyzacyjnych.

II. GŁÓWNE OBSZARY DZIAŁALNOŚCI ABW

1. Zwalczanie terroryzmu

Rok 2009 był pierwszym, pełnym rokiem funkcjonowania w strukturze ABW Centrum Antyterrorystycznego (CAT). To nowatorskie rozwiązanie przyczyniło się przede wszystkim do wzrostu tempa wymiany informacji na temat zagrożeń terrorystycznych i uporządkowania danych dotyczących incydentów potencjalnie związanych z terroryzmem. Oprócz funkcjonariuszy ABW, służbę w CAT pełnią oddelegowani funkcjonariusze, żołnierze i pracownicy cywilni m.in. Policji, Straży Granicznej, Biura Ochrony Rządu, Agencji Wywiadu, Służby Wywiadu Wojskowego, Służby Kontrwywiadu Wojskowego oraz Służby Celnej. Realizują oni zadania w zakresie kompetencji instytucji, którą reprezentują. Ponadto, z Centrum Antyterrorystycznym aktywnie współpracują inne podmioty uczestniczące w systemie ochrony antyterrorystycznej RP, m.in. Rządowe Centrum Bezpieczeństwa, Ministerstwo Spraw Zagranicznych, Państwowa Straż Pożarna, Generalny Inspektor Informacji Finansowej, Sztab Generalny Wojska Polskiego i Żandarmeria Wojskowa.

Centrum Antyterrorystyczne zajmuje się koordynacją działań operacyjno-rozpoznawczych zmierzających do weryfikacji informacji o potencjalnych zagrożeniach. Bierze również udział we wspomaganiu procesów decyzyjnych w przypadkach realnego zagrożenia atakiem terrorystycznym, poprzez przekazywanie wszelkich danych pozwalających na przygotowanie i zabezpieczenie sił i środków niezbędnych do prawidłowego reagowania w sytuacji kryzysowej. W ramach pracy analityczno - informacyjnej CAT sporządza dla kierownictwa państwa, Rządowego Centrum Bezpieczeństwa oraz Międzyresortowego Zespołu ds. Zagrożeń Terrorystycznych informacje na temat aktualnego poziomu zagrożenia terrorystycznego kraju i działań podejmowanych przez służby i instytucje państwowe w celu likwidacji niebezpieczeństw. Prowadzony przez CAT monitoring mediów obcojęzycznych i Internetu ma na celu pozyskanie informacji, które mogą wskazywać na istnienie zagrożenia dla obywateli lub interesów RP. Od kilku lat ABW odnotowuje wyraźny wzrost wykorzystywania Internetu przez terrorystów muzułmańskich do rekrutacji i prowadzenia szkoleń potencjalnych zamachowców.

CAT pracuje na podstawie katalogu incydentów i algorytmów postępowania w sytuacjach związanych z:

- zagrożeniami dla bezpieczeństwa RP;
- zagrożeniami dla przedstawicielstw naszego kraju i Polaków przebywających za granicą;
- zagrożeniami występującymi w rejonach napięć, konfliktów i kryzysów międzynarodowych, które potencjalnie mogą wywierać wpływ na bezpieczeństwo Polski;
- działalnością środowisk ekstremistycznych;
- wprowadzaniem do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł w celu finansowania terroryzmu;
- pobytem cudzoziemców na terytorium RP;
- aktywnością terrorystyczną w mediach i Internecie.

Ze zgromadzonych przez ABW informacji wynika, że w 2009 r. w Polsce nie wystąpiło bezpośrednie zagrożenie terrorystyczne. ABW na bieżąco weryfikuje wszelkie sygnały dotyczące możliwości przeprowadzenia ataku na obszarze naszego kraju i na polskie cele za granicą .

Jednym z ważniejszych zadań kontynuowanych przez CAT w 2009 r. było wspieranie polskich władz w procesie przygotowania i zabezpieczenia antyterrorystycznego mistrzostw Europy w piłce nożnej UEFA EURO 2012. W kolejnych latach CAT będzie nadal prowadził definiowanie potencjalnych zagrożeń związanych z organizacją tej imprezy.

Ponadto, wiedza zgromadzona w CAT posłużyła jako wsparcie informacyjne m.in. w sprawach prowadzonych przez prokuraturę dotyczących porwań obywateli polskich za granicą, jak chociażby uprowadzenia członków załogi chemikaliowca „Bow Asir" i masowca MV „Patriot" (w tym Polaków). ABW współpracuje również z prokuraturą w sprawie monitorowanego przez CAT incydentu dotyczącego oślepiania pilotów samolotów cywilnych wskaźnikami laserowymi.

Funkcjonariusze ABW wzięli udział w odbywających się w dniach 21 – 23 października 2009 r. na terenie Ukrainy ćwiczeniach antyterrorystycznych. Był to jeden z elementów przygotowania zabezpieczenia mistrzostw Europy w piłce nożnej Euro 2012. Na czas trwania ćwiczeń uruchomiono stałe łącze audio-wideo z ukraińskim centrum antyterrorystycznym. Przeprowadzono wideokonferencję pomiędzy Centrum Antyterrorystycznym ABW i ukraińskim Anti-Terrorist Center (ATC), w której uczestniczyli: Prezydent Ukrainy Wiktor Juszczenko i Szef SBU Walenty Naliwajczenko oraz – po

stronie polskiej – Minister Spraw Wewnętrznych i Administracji Jerzy Miller, Podsekretarz Stanu w MSWiA Adam Rapacki i Zastępca Szefa ABW Paweł Białek. Podczas ćwiczeń potwierdzono skuteczność działania systemu łączności w sytuacji kryzysowej, wymagającej podejmowania decyzji na wysokim szczeblu w różnych krajach.

Scenariusz ćwiczeń zakładał m.in. przeprowadzenie akcji uwolnienia pasażerów porwanego samolotu. Uczestniczyli w niej także funkcjonariusze grupy antyterrorystycznej ABW. Przeprowadzone testy pozwoliły na sprawdzenie skuteczności przeciwdziałania zagrożeniu terrorystycznemu zarówno bezpośrednio na miejscu zdarzenia, jak również na poziomie współpracy międzynarodowej. Wypróbowano w praktyce nowoczesne środki wymiany informacji oraz procedury współdziałania krajowych koordynatorów ochrony antyterrorystycznej CAT i ATC.

W listopadzie 2009 roku na terenie Centralnego Ośrodka Szkolenia ABW odbyły się ćwiczenia praktyczne, których celem było przetestowanie i udoskonalenie współpracy pomiędzy ABW, Policją, Państwową Strażą Pożarną oraz Ośrodkiem Radioizotopów Instytutu Energii Atomowej POLATOM. Symulacja obejmowała przeprowadzanie śledztwa powybuchowego po ataku terrorystycznym, w którym została wykorzystana tzw. brudna bomba, czyli klasyczny materiał wybuchowy, połączony z materiałami radioaktywnymi. W ramach ćwiczeń doskonalono procedury współdziałania wyżej wymienionych służb oraz umiejętności gaśnicze neutralizujące ładunek wybuchowy rozpraszający substancje radioaktywne, zabezpieczanie miejsca zdarzenia, procedury kryminalistyczne w zakresie zbierania śladów oraz niektóre inne działania śledcze.

W 2009 r. CAT odwiedzili: Prezydent RP Lech Kaczyński, Prezes Rady Ministrów Donald Tusk, Marszałek Senatu RP Bogdan Borusewicz oraz goście zagraniczni, w tym przedstawiciele misji UE w ramach II rundy wzajemnych misji ewaluacyjnych w zakresie krajowych systemów zwalczania terroryzmu. Do CAT przybyli również z wizytami eksperckimi szefowie zagranicznych służb partnerskich oraz przedstawiciele parlamentów i struktur zajmujących się walką z terroryzmem. Poza tym w Centrum Antyterrorystycznym odbyły się posiedzenia Sejmowych Komisji: Służb Specjalnych, Administracji i Spraw Wewnętrznych oraz Obrony Narodowej.

2. Ochrona cyberprzestrzeni

Dotychczas nie odnotowano żadnych poważnych incydentów naruszenia bezpieczeństwa teleinformatycznego w internetowych sieciach komputerowych administracji państwowej oraz innych systemach komputerowych wchodzących w skład krytycznej infrastruktury teleinformatycznej kraju. Niemniej jednak, w ocenie Agencji Bezpieczeństwa Wewnętrznego, zagrożenie cyberterroryzmem w Polsce utrzymuje się na dość wysokim poziomie.

Zwalczaniem zagrożeń cyberprzestrzeni zajmuje się Rządowy Zespół Reagowania na Incydenty Komputerowe – CERT.GOV.PL. Zespół ten stanowi platformę koordynacji działań w zakresie reagowania na incydenty zagrażające bezpieczeństwu systemów lub sieci teleinformatycznych wykorzystywanych przez organy państwa, których uszkodzenie lub zniszczenie mogłoby doprowadzić do poważnych zakłóceń funkcjonowania kraju.

Zespół CERT.GOV.PL przekazuje instytucjom i podmiotom rządowym wiedzę, dzięki której mogą skutecznie przeciwdziałać atakom na ich systemy teleinformatyczne. Zespół ten, pełniąc rolę centrum kompetencyjnego, wspiera państwowe i samorządowe jednostki organizacyjne w zakresie udostępniania informacji o nowych typach

zagrożeń występujących w sieciach komputerowych, w tym pochodzących z Internetu, oraz o środkach przeciwdziałania im. Prowadzi również szkolenia z zakresu reagowania na incydenty naruszające bezpieczeństwo teleinformatyczne.

Jednym z zadań Zespołu jest wdrażanie i nadzór nad systemem wczesnego ostrzegania o zagrożeniach występujących w Internecie – ARAKIS-GOV. To rozwiązanie jest efektem współpracy ABW oraz działającego w ramach NASK zespołu CERT Polska. ARAKIS-GOV powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych administracji państwowej w wyniku rozszerzenia stworzonego przez CERT Polska systemu ARAKIS o dodatkową funkcjonalność. Obecnie sensory systemu zainstalowane są w ponad 60 urzędach szczebla centralnego i administracji terenowej.

ARAKIS-GOV nie jest typowym systemem zabezpieczającym i w żadnym wypadku nie zastępuje funkcjonalności standardowych systemów ochrony sieci, takich jak firewall, antywirus czy IDS/IPS. Jednak ze względu na swoją specyfikę może być z powodzeniem stosowany jako uzupełnienie wyżej wymienionych systemów, dostarczając informacji na temat nowych globalnych zagrożeń pojawiających się w Internecie, a także zagrożeń lokalnych związanych z konkretną, chronioną lokalizacją.

Unikalną cechą systemu ARAKIS-GOV jest to, że w żaden sposób nie monitoruje on treści informacji wymienianych przez chronioną instytucję z Internetem. Sondy systemu instalowane są bowiem poza chronioną siecią wewnętrzną danej instytucji, po stronie sieci Internet. Od momentu uzyskania pełnej funkcjonalności przez system ARAKIS-GOV (w połowie 2009 r.) za jego pośrednictwem zgłoszono 3367 alarmów.

W celu kształtowania świadomości do zagrożeń cyberprzestrzeni ABW uruchomiła witrynę internetową cert.gov.pl, na której publikowane są bieżące informacje na temat cyberbezpieczeństwa.

Za pośrednictwem tej witryny można zgłaszać incydenty naruszenia bezpieczeństwa w systemach lub sieciach teleinfomatycznych wykorzystywanych przez organy państwa. Na stronie zamieszczane są również kwartalne raporty dotyczące cyberbezpieczeństwa oraz biuletyny bezpieczeństwa udostępniane przez producentów sprzętu i oprogramowania informatycznego.

W czerwcu i listopadzie 2009 r. funkcjonariusze ABW z CERT.GOV.PL i Laboratorium Elektronicznych Nośników Informacji reprezentowali Polskę w dwóch kolejnych edycjach międzynarodowych warsztatów International Cyber Defence Workshop. Celem ćwiczeń zorganizowanych przez Departament Obrony USA było podniesienie poziomu kompetencji rządowych i wojskowych służb odpowiedzialnych za cyberbezpieczeństwo w swoich krajach. Organizowane cyklicznie International Cyber Defence Workshop to międzynarodowe ćwiczenia mające na celu doskonalenie technik obrony przed zagrożeniami cyberprzestrzeni oraz analizę incydentów z wykorzystaniem narzędzi informatyki śledczej. W konsekwencji, podczas ćwiczeń dochodzi do wymiany informacji i wzajemnego doskonalenia ekspertów narodowych, a także do wypracowania metod współdziałania międzynarodowego w przypadku wystapienia zagrożeń pochodzących z Internetu.

Funkcjonariusze ABW odnieśli dwukrotne zwycięstwo w zawodach kończących warsztaty. Wśród uczestników zawodów były reprezentacje m.in. Francji, Niemiec, USA, Korei Południowej i Australii.

Dotychczasowe doświadczenia Zespołu CERT.GOV.PL, jak choćby z zakresu wykrytych incydentów, przeprowadzonych testów i analiz oraz wsparcia udzielonego instytucjom administracji publicznej wskazują, że stworzenie w ABW tego typu komórki umożliwia skuteczny monitoring i analizę prób ataków na sieci informatycz-

ne. Funkcjonariusze ABW dysponują specjalistycznym sprzętem i oprogramowaniem umożliwiającym analizę oraz ewentualne zabezpieczanie śladów ataku metodami informatyki śledczej.

3. Kontrwywiadowcza ochrona RP

Sytuacja polityczna i gospodarcza Polski, zarówno w wymiarze bilateralnym, jak i globalnym, jest stałym obiektem intensywnego zainteresowania operacyjnego większości liczących się na świecie służb wywiadowczych. Aktywność obcych wywiadów wynika z członkostwa Polski w NATO i UE, naszej obecności wojskowej w rejonach konfliktów oraz dążenia innych państw do rozszerzenia możliwości realizacji własnych interesów w regionie Europy Środkowo-wschodniej. ABW monitoruje sytuację w Polsce pod względem potencjalnego zagrożenia ze strony zagranicznych służb specjalnych.

Cechą charakterystyczną działalności współczesnych służb wywiadowczych jest stała modyfikacja ich metod pracy i poszerzanie obszarów zainteresowań. Część z nich nadal stosuje pełny wachlarz tradycyjnych instrumentów operacyjnych, takich jak werbunek i współpraca z osobowymi źródłami informacji. Inne rezygnują z klasycznego pozyskiwania agentury na rzecz m.in. białego wywiadu i metod stosowanych w lobbingu. Celem działań wywiadowczych jest rozpoznawanie mechanizmów procesów decyzyjnych w polityce i gospodarce oraz uzyskiwanie informacji wyprzedzających istotnych z punktu widzenia zainteresowanych państw.

W lutym 2009 r. ABW zatrzymała obywatela Federacji Rosyjskiej podejrzanego o działalność na rzecz rosyjskiego wywiadu wojskowego GRU. Zatrzymany od kilkunastu lat mieszkał w Polsce i działał na szkodę RP. Za realizację tej sprawy Prezydent RP Lech Kaczyński wręczył odznaczenia pięciu funkcjonariuszom kontrwywiadu ABW.

Przed Sądem Okręgowym w Białymstoku toczy się sprawa przeciwko byłemu funkcjonariuszowi ABW, który oskarżony jest o działanie na rzecz obcego wywiadu oraz ujawnienie tajemnicy państwowej i służbowej. Oskarżony utrzymywał kontakty z Olgą Solomenik, obywatelką Białorusi podejrzewaną przez ABW o działanie na rzecz białoruskiego wywiadu. Ujawnienie działalności szpiegowskiej oskarżonego oraz jego zatrzymanie w lutym 2008 r. było wynikiem rozpracowania dokonanego przez ABW. W tej sprawie wyłączono materiały dotyczące O.Solomenik, podejrzanej o prowadzenie działalności szpiegowskiej na szkodę RP, za którą Prokuratura wydała list gończy.

4. Ochrona ekonomicznych interesów państwa

Agencja Bezpieczeństwa Wewnętrznego zajmuje się tymi spośród przestępstw o charakterze ekonomicznym, które z uwagi na skalę lub udział w nich osób pełniących funkcje publiczne zagrażają bezpieczeństwu RP. Istotne znaczenie dla interesów ekonomicznych państwa ma bezpieczeństwo energetyczne. Zagrożenia w tym zakresie dotyczą: potencjalnych zakłóceń lub okresowego przerwania dostaw surowców energetycznych (głównie ropy naftowej i gazu ziemnego), działań, których efektem może być wstrzymanie lub spowolnienie realizacji projektów dywersyfikacyjnych (w tym budowy terminalu gazu skroplonego w Świnoujściu), możliwości ograniczenia roli Polski jako pośrednika tranzytowego w transporcie surowców energetycznych

do Europy Zachodniej. Agencja Bezpieczeństwa Wewnętrznego zajmuje się także rozpoznawaniem negatywnych zjawisk wpływających na funkcjonowanie krajowego sektora energetycznego, a także na obrót oraz wydobywanie i przetwarzanie surowców energetycznych.

Zagrożenia dla systemu finansowego państwa wykrywane przez ABW dotyczą przede wszystkim, przestępczości skarbowej, podatkowej, przestępstw giełdowych, nieprawidłowości w sektorze bankowym i ubezpieczeniowym, przestępstw celnych oraz prania pieniędzy. ABW prowadzi monitoring w tym zakresie we współpracy m.in. z Generalnym Inspektorem Informacji Finansowych oraz Komisją Nadzoru Finansowgo. W ramach przestępstw podatkowych największe szkody dla budżetu państwa wyrządzane są przez przemyt do Polski towarów bez naliczania należnego podatku akcyzowego oraz wyłudzenia zwrotów podatku od towarów i usług (VAT). Z powodu wysokich stawek podatku akcyzowego opłacalny jest przemyt do Polski wyrobów tytoniowych, alkoholowych i paliw płynnych. ABW rozpoznaje, przeciwdziała i zwalcza przemyt towarów z pominięciem opłat celnych, akcyzy, podatku VAT i innych należności wobec państwa.

W ubiegłym roku Agencja Bezpieczeństwa Wewnętrznego prowadziła ogółem 310 śledztw w sprawach ekonomicznych, w tym 78 postępowań dotyczyło uszczupleń podatków VAT, akcyzy i ceł, 176 – wyrządzenia szkody w mieniu Skarbu Państwa, 30 – prania pieniędzy.

Istotne znaczenie ma również rozpoznawanie przez Agencję zagrożeń dla sektora zbrojeniowego w zakresie nieprawidłowości w procesach i procedurach prywatyzacyjnych oraz konsolidacyjnych podmiotów z branży zbrojeniowej czy realizacji umów offsetowych związanych z dostawami przez kontrahentów zagranicznych uzbrojenia na potrzeby polskich sił zbrojnych. W sprawach tych Agencja Bezpieczeństwa Wewnętrznego prowadzi ścisłą współpracę ze Służbą Kontrwywiadu Wojskowego.

5. Walka z korupcją

Do kompetencji ABW należy zwalczanie korupcji z udziałem osób pełniących funkcje publiczne, jeśli przestępstwo to godzi w bezpieczeństwo państwa. Dotyczy to głównie urzędników administracji rządowej i samorządowej oraz osób odpowiedzialnych za środki publiczne, w tym za przetargi i przekształcenia własnościowe.

ABW uczestniczy w realizacji projektu Tarcza Antykorupcyjna, którego celem jest ochrona procesów prywatyzacyjnych wybranych podmiotów z udziałem Skarbu Państwa oraz zamówień publicznych istotnych dla bezpieczeństwa naszego kraju przed patologiami korupcyjnymi. Projekt ten ma przede wszystkim charakter profilaktyczny i należy do priorytetowych działań ABW.

Elementem profilaktyki antykorupcyjnej jest realizacja szkoleń w zakresie zagadnień związanych z zabezpieczaniem urzędów przed korupcją i nieuprawnionym lobbingiem oraz zagrożeniami ze strony zorganizowanych grup przestępczych. W zorganizowanych dotychczas przez ABW kilkudziesięciu wykładach dotyczących przedmiotowej problematyki uczestniczyło ok. 500 urzędników. Wśród nich znalazły się osoby reprezentujące różne stanowiska i urzędy, w tym m.in. resorty gospodarki, finansów i sprawiedliwości.

ABW monitoruje prywatyzację 82 spółek z udziałem Skarbu Państwa, w tym podmiotów figurujących na opublikowanej w serwisie internetowym rządu *Liście pod-*

miotów, których prywatyzacja będzie miała największe znaczenie dla interesów i bezpieczeństwa państwa.

W związku z funkcjonowaniem Tarczy Antykorupcyjnej ABW prowadzi aktualnie kilkadziesiąt śledztw. Dotyczą one nieprawidłowości w przetargach publicznych rozpisanych przez resorty: obrony narodowej, finansów, spraw wewnętrznych i administracji, sprawiedliwości, środowiska, a także w Generalnej Dyrekcji Dróg Krajowych i Autostrad oraz PP Porty Lotnicze. Priorytetowe znaczenie w ramach Tarczy ma ochrona przetargów na dostawę systemów i sprzętu informatycznego do urzędów państwowych. Agencja monitoruje również działalność firm doradczych uczestniczących w prywatyzacji i przetargach, które w wielu przypadkach mają decydujący wpływ na przebieg tych procesów. W zainteresowaniu ABW są również ewentualne nieprawidłowości mogące wystąpić podczas procesów legislacyjnych. rowadzone są także śledztwa w sprawach nieprawidłowości dotyczących podmiotów przeznaczonych do prywatyzacji (m.in. Giełda Papierów Wartościowych, ENEA SA, Cefarm Białystok).

Zjawisko korupcji występuje również przy procesie absorpcji funduszy unijnych. Ma miejsce m.in. podczas zatwierdzania wniosków pomocowych oraz zarządzania środkami.

W ubiegłym roku do sądu w Krakowie wpłynął akt oskarżenia wobec funkcjonariusza publicznego zatrudnionego w Małopolskim Oddziale Regionalnym Agencji Restrukturyzacji i Modernizacji Rolnictwa w Krakowie oraz dwóch współpracujących z nim osób. Oskarżonym zarzuca się popełnienie przestępstw polegających na wspólnym działaniu w celu osiągnięcia korzyści majątkowych w związku ze sporządzaniem i rozpatrywaniem wniosków o dofinansowanie inwestycji ze środków publicznych pochodzących z funduszy Unii Europejskiej.

W 2009 r. funkcjonariusze ABW podjęli szereg działań mających na celu eliminację zjawisk korupcyjnych dotyczących w szczególności osób pełniących funkcje publiczne oraz urzędników, w tym m.in. urzędów centralnych.

Na polecenie szczecińskiej prokuratury ABW zatrzymała, pod zarzutem korupcji, prezesa ZUS oraz dyrektora, zastępcę i kierownika referatu remontów, inwestycji i zamówień publicznych szczecińskiego oddziału ZUS oraz prywatnego przedsiębiorcę. Były prezes ZUS jest podejrzany o popełnienie sześciu przestępstw o charakterze korupcyjnym.

ABW prowadzi również śledztwo w sprawie korupcji w branży węglowej, w toku którego zatrzymano dotychczas kilka osób podejrzanych o wręczanie i przyjmowanie korzyści majątkowych. Skala ujawnionego procederu ma szeroki wymiar, a wartość wręczonych łapówek jest bardzo wysoka.

6. Zwalczanie przestępczości zorganizowanej

ABW zajmuje się rozpoznawaniem struktur i metod działania zorganizowanych grup przestępczych. Z uwagi na międzynarodowy zakres ich działalności, prowadzona jest stała współpraca ze służbami specjalnymi, policyjnymi i celnymi innych państw.

W ocenie ABW, zorganizowane grupy przestępcze, aby zapewnić sobie realizację własnych celów, często podejmują próby wywierania wpływu na organy ścigania, sądy, urzędników państwowych, polityków, a także media.

Głównymi obszarami działania polskich grup przestępczych są: produkcja, przemyt i handel narkotykami, handel bronią, przemyt towarów akcyzowych (m.in. alkoholu, papierosów, paliw płynnych), wyłudzenia i oszustwa. Zorganizowane grupy prze-

stępcze przejawiają aktywność również na płaszczyźnie nowych technologii, w tym Internetu. Za jego pośrednictwem dochodzi do ataków na systemy komputerowe, kradzieży danych i środków finansowych.

Przestępczość narkotykowa stwarza zagrożenie nie tylko dla pojedynczych osób, ma także negatywny wpływ na funkcjonowanie struktur państwowych i gospodarczych m.in. poprzez:

- tworzenie i rozwój rozległych zorganizowanych grup i sieci przestępczych o zasięgu międzynarodowym;
- korumpowanie służb granicznych oraz organów ścigania;
- legalizację dochodów uzyskanych z biznesu narkotykowego.

Popularnym kierunkiem przemytu amfetaminy są kraje skandynawskie – Szwecja i Norwegia. Z Polski narkotyk ten trafia również na rynki wschodnie. Od pewnego czasu obserwujemy, iż polscy przestępcy zajmujący się wytwarzaniem narkotyków szkolą producentów z innych krajów. Do Warszawy przyjeżdżają „kursanci" np. z Ukrainy. Szkolenia przechodzą też Polacy mieszkający na emigracji, m.in. w Anglii i Irlandii. Związane jest to z budową w tych państwach laboratoriów do produkcji amfetaminy, co w rezultacie ma wyeliminować ryzykowny proceder przemytu narkotyków. W Polsce nielegalne laboratoria wytwarzające amfetaminę są lokalizowane w miejscach mało uczęszczanych, najczęściej na terenach wiejskich i często są przenoszone. Do pracy w nich werbowani są wykwalifikowani chemicy, którzy nieustannie modyfikują proces produkcji narkotyków. W 2009 r. ABW zlikwidowała trzy tego typu laboratoria.

Głównym dostawcą kokainy jest Kolumbia, a podstawowe punkty wwozu tego narkotyku do Europy stanowią Półwysep Iberyjski (przede wszystkim Hiszpania) oraz Holandia. W przemycie kokainy kluczową rolę odgrywa transport morski i lotniczy. Narkotyk ten trafia do Polski obiema drogami, a następnie jest rozprowadzany na naszym rynku lub też przerzucany do innych państw UE.

W ubiegłym roku Agencja Bezpieczeństwa Wewnętrznego – współpracując ze Strażą Graniczną – rozbiła międzynarodową grupę przestępczą zajmującą się przemytem kokainy na skalę masową. Funkcjonariusze Agencji przejęli 1134 kg tego narkotyku o wartości czarnorynkowej ponad 500 mln złotych. Zatrzymano osiem osób: trzech obywateli Kolumbii, jednego obywatela Wenezueli, dwóch obywateli Holandii i dwóch obywateli Austrii. Są to przedstawiciele karteli kolumbijskich oraz członkowie grup przestępczych z Europy Zachodniej.

Jak do tej pory był to największy ładunek tego narkotyku przejęty na terytorium Polski. Sukces operacji był możliwy dzięki wielomiesięcznej współpracy z amerykańską służbą ds. zwalczania przestępczości narkotykowej (DEA) oraz policją kolumbijską. Celem wspólnego przedsięwzięcia było rozpoznanie i rozpracowanie sieci karteli z terenu Kolumbii, Wenezueli i Meksyku oraz współpracujących z nimi zorganizowanych grup przestępczych, które zajmują się narkobiznesem w Europie. W wyniku polsko - amerykańskiej akcji zlikwidowany został kanał przemytu kokainy z Ameryki Południowej przez Polskę do krajów Europy Zachodniej. Oficerowie ABW, którzy przyczynili się do tego sukcesu, otrzymali z rąk Premiera RP Donalda Tuska okolicznościowe listy gratulacyjne oraz nagrody pieniężne.

Premier zwracając się do funkcjonariuszy podkreślił, że [...] *tego typu zdarzenia budują w Polakach, wszystkich Polakach bez wyjątku, poczucie większego bezpieczeństwa, ale też poczucie dumy, że nasze państwo może działać tak, jak wy to zaprezentowaliście*.

Zorganizowane grupy przestępcze są również aktywne w sferze przemytu towarów z pominięciem opłat celnych, akcyzy, podatku VAT i innych należności wobec państwa, na którego terytorium wwieziono towar. Na teren RP w sposób nielegalny trafiają produkty przede wszystkim ze Wschodu. Z powodu wysokich stawek podatku akcyzowego opłacalny jest przemyt wyrobów tytoniowych, alkoholowych i paliw płynnych. ABW rozpoznaje, przeciwdziała i zwalcza działalność zorganizowanych grup przestępczych zaangażowanych w przemyt towarów akcyzowych.

W 2009 roku trafił do sądu w Lublinie akt oskarżenia przeciwko dwóm obywatelom Mongolii, którzy - posługując się paszportami dyplomatycznymi - przemycali papierosy w poczcie dyplomatycznej. Zostali oni zatrzymani przez ABW, która prowadziła śledztwo w tej sprawie. Zarzuca się im udział w zorganizowanej grupie przestępczej oraz narażenie budżetu Wspólnoty Europejskiej i budżetu Skarbu Państwa RP na uszczuplenie należności celnej w łącznej wysokości nie mniejszej niż 2,2 mln zł, należności podatku VAT w wysokości blisko 6 mln zł i należnego podatku akcyzowego w kwocie około 20 mln zł.

Agencja Bezpieczeństwa Wewnętrznego zajmuje się również rozpoznawaniem i zwalczaniem przestępstw związanych z nielegalną produkcją i międzynarodowym obrotem sprzętem wojskowym i uzbrojeniem. Nasze działania mają na celu eliminację możliwości pozyskiwania na terenie Polski broni przez państwa objęte embargiem, międzynarodowe grupy przestępcze oraz organizacje terrorystyczne. Aspekt kryminalny (np. nielegalny handel pojedynczymi egzemplarzami broni) pozostaje w zakresie kompetencji innych służb, przede wszystkim Policji.

7. Zwalczanie nielegalnego rozprzestrzeniania technologii podwójnego zastosowania

W Polsce nie występują bezpośrednie zagrożenia związane z proliferacją broni masowego rażenia, ponieważ nasz kraj nie posiada zapasów broni ABC ani jej komponentów. Nie można jednak wykluczyć funkcjonowania na terenie RP firm „przykrycia" bądź pojedynczych przedsiębiorców wspomagających działalność związaną z jej rozprzestrzenianiem. Takie działania to przede wszystkim pozyskiwanie towarów, surowców lub technologii, a także pośrednictwo lub organizacja transportu. Przeciwdziałanie takiemu zagrożeniu jest utrudnione z uwagi na dużą ilość towarów, które są wykorzystywane zarówno w produkcji cywilnej, jak i w technice wojskowej. Ponadto, w tego typu działaniach stosuje się szereg metod kamuflażu, np. mnożenie ogniw transakcji, zaniżania parametrów technicznych urządzeń, eksportowanie towaru w kilku transportach. Aktywność podmiotów działających na rzecz „krajów ryzyka" koncentruje się na pozyskiwaniu w Polsce różnego rodzaju wyrobów przemysłu ciężkiego. W szczególności dotyczy to zaawansowanych technologicznie urządzeń do obróbki materiałów, czy też wysokiej jakości wyrobów hutniczych.

Obserwowana jest również praktyka wykorzystywania polskiego dorobku naukowego przez tzw. kraje ryzyka na rzecz produkcji i udoskonalania elementów broni masowego rażenia lub środków jej przenoszenia. Naukowcy z tych państw są uczestnikami konferencji i sympozjów naukowych z zakresu m.in. technik jądrowych, fizyki teoretycznej, mechatroniki, materiałoznawstwa i informatyki. Ich obecność nie ma wyłącznie charakteru naukowego, ale wiąże się również z inicjowaniem prywatnych kontaktów biznesowych lub rozpoznawaniem możliwości zakupu w Polsce wyrobów technicznych.

Czynnikiem potęgującym zagrożenie nielegalnego rozprzestrzeniania technologii podwójnego zastosowania jest gwałtowny rozwój technik informatycznych, który ułatwia dokonywanie tzw. nieuchwytnego transferu technologii poprzez przekazywanie przez Internet kopii dokumentów, planów technicznych czy kluczy szyfrujących.

W 2009 r. ABW wspólnie z Ministerstwem Spraw Zagranicznych, była jednym z organizatorów regionalnego spotkania ekspertów tzw. Inicjatywy Krakowskiej – Proliferation Security Initiative (ROEG PSI) w Sopocie. W spotkaniu tym uczestniczyli przedstawiciele 39 państw wspierających Inicjatywę, w tym reprezentanci Unii Europejskiej i NATO. Z uwagi na szczególne znaczenie spotkań ROEG PSI oraz fakt, iż ABW od chwili powołania Inicjatywy Krakowskiej czynnie uczestniczy w jej pracach, kierownictwo ABW zadecydowało o przejęciu przewodnictwa w Podgrupie ds. Wymiany Informacji skupiającej ekspertów służb specjalnych. Czerwcowe spotkanie umożliwiło wymianę poglądów dotyczących najskuteczniejszych sposobów zapobiegania proliferacji w ramach współpracy Unii Europejskiej, w tym zatrzymywania nielegalnych transportów komponentów do produkcji broni masowego rażenia (BMR).

8. Zwalczanie ekstremizmu politycznego

Kolejnym zadaniem Agencji Bezpieczeństwa Wewnętrznego jest rozpoznawanie i zapobieganie zagrożeniom godzącym w porządek konstytucyjny państwa, wynikającym z działalności ruchów ekstremistycznych, w tym organizacji skrajnie prawicowych oraz lewicowych. W Polsce funkcjonuje kilkanaście tego typu ugrupowań. Ich działania przejawią się głównie poprzez afirmację założeń narodowego socjalizmu lub komunizmu oraz poprzez propagowanie ideologii nazistowskiej albo marksistowskiej.

Aktywność ugrupowań ekstremistycznych nie stanowi jednak – jak do tej pory – bezpośredniego zagrożenia dla bezpieczeństwa państwa. Natomiast niepokojący jest fakt systematycznego wzrostu liczby zwolenników ich ideologii oraz tworzenie bojówek paramilitarnych.

W Polsce najbardziej aktywne są ruchy odwołujące się do haseł skrajnie prawicowych, neofaszystowskich lub nacjonalistycznych. Celem działalności organizacji ultraprawicowych jest rozpowszechnianie ideologii neofaszyzmu, neonazizmu, antysemityzmu oraz głoszenie haseł nienawiści do mniejszości etnicznych, narodowych i seksualnych. Większość skrajnych ugrupowań funkcjonujących w Polsce wzoruje się na analogicznych organizacjach działających w Europie Zachodniej i USA.

Oprócz organizowania obozów szkoleniowych, bojówek paramilitarnych i koncertów, organizacje skrajne aktywne są również w Internecie. Obecnie obserwowany jest wzrost liczby forów dyskusyjnych wykorzystywanych przez organizacje ekstremistyczne. Internet jest też wykorzystywany do przeprowadzania szkoleń i wymiany informacji, np. na temat adresów stron internetowych, na których znajdują się poradniki dotyczące przygotowywania metodą chałupniczą materiałów wybuchowych i bomb. Witryny internetowe wykorzystywane są również do umawiania spotkań oraz dystrybuowania książek, czasopism, płyt CD, DVD i różnego rodzaju emblematów zawierających treści ekstremistyczne. W związku z wynikającym z przepisów polskiego prawa zakazem propagowania w Polsce skrajnych ideologii, ich zwolennicy wykorzystują możliwości zakładania stron internetowych na zagranicznych serwerach.

W ostatnim okresie decyzje podejmowane przez polskie sądy wobec neofaszystów są bardziej restrykcyjne. W styczniu 2009 r. Sąd Okręgowy w Białymstoku skazał

trzech członków ugrupowania „Czwarta Edycja" za publiczne propagowanie ustroju faszystowskiego, a w październiku sąd w Opolu podjął decyzję o rozwiązaniu brzeskiej brygady ONR. 11 maja 2009 r. funkcjonariusze Delegatury ABW we Wrocławiu przeprowadzili czynności procesowe, w wyniku których zabezpieczono m.in. ulotki, plakaty i komputery zawierające treści neofaszystowskie. W związku z tym wydarzeniem zatrzymano sześciu podejrzanych, którym prokurator postawił zarzuty udziału w zorganizowanej grupie przestępczej, propagowania treści faszystowskich i nawoływania do nienawiści na tle różnic narodowościowych i rasowych oraz znieważania grupy ludności ze względu na pochodzenie. Takie decyzje sądów, wsparte działaniami organów ścigania, mogą w przyszłości przyczynić się do zahamowania lekceważenia przez ekstremistów konstytucyjnego porządku prawnego.

9. Ochrona tajemnicy państwowej i służbowej

Obecny system ochrony informacji niejawnych funkcjonuje w Polsce od 11 lat. Jego powstanie było ściśle związane z przystąpieniem naszego kraju do NATO. Jednym ze stawianych wymogów było stworzenie mechanizmu, który gwarantowałby bezpieczeństwo przekazywanych informacji i jednocześnie spełniał standardy Sojuszu Północnoatlantyckiego. Obecnie ochrona informacji niejawnych regulowana jest ustawą z dnia 22 stycznia 1999 r. W wyniku przeprowadzonych analiz oraz zdobytych doświadczeń ABW dostrzega pewne mankamenty istniejących rozwiązań.

Wśród głównych słabości obecnego systemu należy wskazać zbytnie skomplikowanie procedur, które powoduje lekceważenie obowiązujących przepisów. Przyczynia się do tego także brak sparametryzowanego algorytmu szacowania szkód w zakresie ochrony informacji niejawnych oraz niska świadomość urzędników o skutkach niewłaściwego postępowania z informacjami klauzulowanymi. Szczególnie szkodliwe dla bezpieczeństwa państwa są przypadki łamania przepisów ustawy, do których dochodzi w urzędach centralnych. Przykładem tego typu nieodpowiedzialnych zachowań jest przekazanie osobom nieupoważnionym niejawnego raportu CAT ABW o incydencie w Gruzji z udziałem Prezydenta RP, za co w 2009 r. prokuratura przedstawiła zarzuty byłemu Szefowi Kancelarii Prezydenta RP.

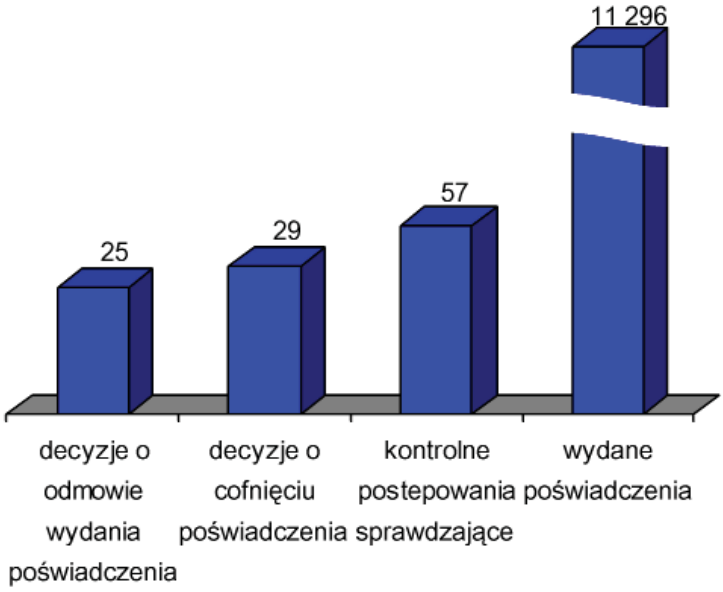
W skontrolowanych przez ABW w 2009 r. instytucjach państwowych wykryto pewne nieprawidłowości. Do najpoważniejszych należy zaliczyć wytwarzanie, przetwarzanie i przechowywanie informacji niejawnych w systemach i sieciach teleinformatycznych, które nie posiadają akredytacji służby ochrony państwa. W większości wypadków wynika to z lekceważenia lub braku wiedzy o tym, że informacje niejawne mogą być sporządzane wyłącznie na tzw. bezpiecznych stanowiskach.

Ustalenia dokonane przez funkcjonariuszy ABW, w tym podczas kontroli, pozwoliły na skierowanie w 2009 r. do prokuratury 20 zawiadomień o podejrzeniu popełnienia przestępstwa. Zawiadomienia dotyczyły przede wszystkim podejrzenia przekroczenia uprawnień lub niedopełnienia obowiązków służbowych przez funkcjonariuszy publicznych, tj. kierowników kontrolowanych jednostek odpowiedzialnych za ochronę informacji niejawnych, a także przez pełnomocników ochrony, odpowiedzialnych za zapewnienie przestrzegania przepisów w tym zakresie.

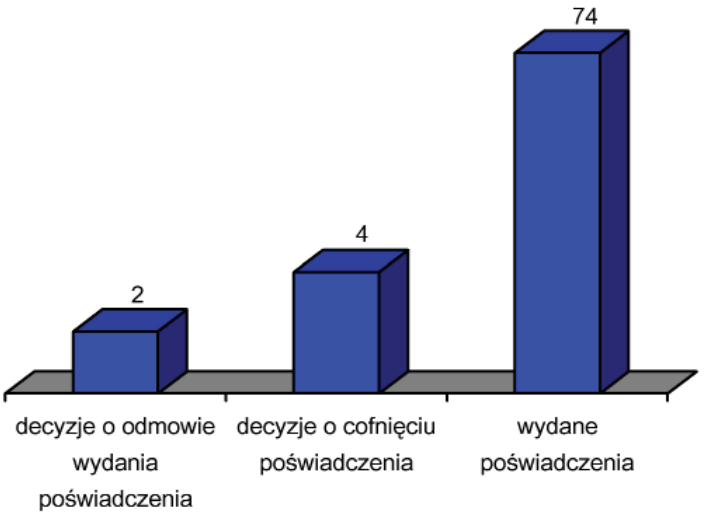
Więcej danych na temat stanu ochrony informacji niejawnych w Polsce w poprzednich latach znajduje się w raporcie opublikowanym na stronie internetowej Agencji (http://www.abw.gov.pl/portal.php?serwis=pl&dzial=8&id=453&search=1936).

Bezpieczeństwo informacji niejawnych jest w głównej mierze zależne od odpowiedzialności i świadomości osób mających dostęp do dokumentów klauzulowanych. Dlatego też tak istotne znaczenie ma przeprowadzanie procedur sprawdzających, podczas których ustala się, czy poszczególne osoby dają rękojmię zachowania tajemnicy. W efekcie takiego postępowania wydawane jest poświadczenie bezpieczeństwa lub odmowa jego wydania. Każda tego typu decyzja podejmowana jest na podstawie informacji zgromadzonych w ramach oddzielnej procedury sprawdzającej.

Postępowania bezpieczeństwa przemysłowego to odrębna kategoria postępowań sprawdzających. Są one prowadzone w celu ustalenia, czy podmioty – realizujące umowy lub wykonujące zadania związane z dostępem do informacji niejawnych stanowiących tajemnicę państwową lub informacji niejawnych organizacji międzynarodowych (Organizacji Traktatu Północnoatlantyckiego, Unii Europejskiej, Unii Zachodnioeuropejskiej), oznaczonych odpowiednikiem klauzuli „poufne" lub wyższym – gwarantują zapewnienie właściwej ochrony tego typu informacjom. Dokumentem wydawanym po zakończeniu postępowania z wynikiem pozytywnym jest świadectwo bezpieczeństwa przemysłowego, które potwierdza zdolność sprawdzanego podmiotu do zapewnienia ochrony informacjom niejawnym.



Rys. 6. Działania ABW w zakresie postępowań sprawdzających w 2009 roku.



Rys. 7. Działania ABW w zakresie postępowań bezpieczeństwa przemysłowego w 2009 roku.

III. DZIAŁANIA PREWENCYJNE

Realizując zadania statutowe, Agencja Bezpieczeństwa Wewnętrznego poświęca dużo uwagi szeroko rozumianej profilaktyce. Poza działaniami wynikającymi z realizacji obowiązków ustawowych (m.in. prowadzenie postępowań sprawdzających wobec osób i firm, a także opiniowanie cudzoziemców starających się o polskie obywatelstwo lub prawo pobytu), ABW stworzyła wielowymiarowy system prewencyjny, na który składają się organizacja szkoleń i działań uświadamiających zagrożenia oraz podnoszących wrażliwość na problematykę bezpieczeństwa. Elementy tego systemu to:

- profilaktyka kontrwywiadowcza;
- profilaktyka w zakresie zasad bezpiecznego korzystania z Internetu i zagrożeń cyberprzestrzeni;
- szkolenia dla urzędników administracji centralnej, w tym profilaktyka antykorupcyjna;
- szkolenia pełnomocników ds. ochrony informacji niejawnych;
- szkolenia administratorów i inspektorów sieci teleinformatycznych;
- studia podyplomowe „BEZPIECZEŃSTWO WEWNĘTRZNE";
- konferencje tematyczne;
- publikacje wydawane przez ABW;
- komunikacja ze społeczeństwem.

Cele systemu:

1. uświadomienie pracownikom administracji państwowej istnienia różnorodnych zagrożeń, z którymi mogą zetknąć się w trakcie wykonywanej pracy oraz pokazanie sposobów zachowań pozwalających uniknąć sytuacji niebezpiecznych z punktu widzenia wewnętrznego bezpieczeństwa państwa;
2. stworzenie efektywnego mechanizmu szkoleń zawodowych dla osób odpowiedzialnych za bezpieczeństwo informacji niejawnych i sieci teleinformatycznych;

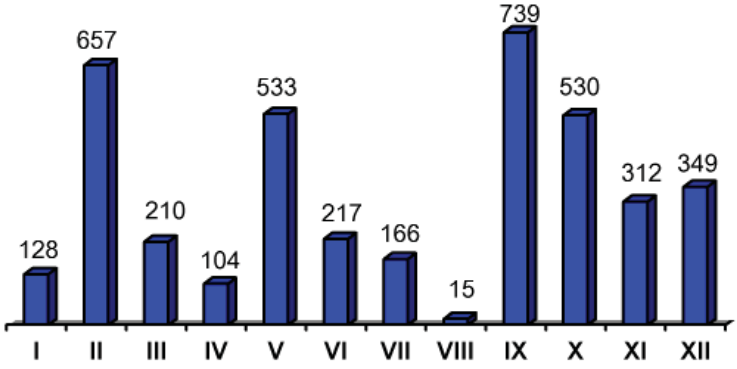
3. stworzenie forum wymiany myśli i poglądów dotyczących bezpieczeństwa wewnętrznego i związanej z nim problematyki, co ma się przełożyć na podniesienie skuteczności realizacji zadań przez Agencję;
4. nawiązanie współpracy ABW z innymi instytucjami w celu stałego podnoszenia kwalifikacji funkcjonariuszy Agencji oraz doskonalenia metodyki ich pracy.

1. Profilaktyka kontrwywiadowcza

Podstawowym zadaniem służb specjalnych jest zapewnienie ochrony przed działaniami wywiadowczymi obcych państw. Z doświadczeń kontrwywiadu wynika, że najlepsze procedury bezpieczeństwa okazują się nieskuteczne, jeżeli zawiedzie jeden kluczowy element – czynnik ludzki. W związku z tym w ABW funkcjonuje wyspecjalizowana komórka odpowiedzialna za realizację programu profilaktyki kontrwywiadowczej, która powstała w 2008 r., a w ubiegłym roku wykonywała swoje zadania już w pełnym zakresie.

Programem profilaktyki kontrwywiadowczej objęci są przede wszystkim urzędnicy administracji centralnej, terenowej i samorządowej, a także pracownicy spółek Skarbu Państwa dysponujący wiedzą interesującą z punktu widzenia obcych służb specjalnych. Skierowany jest on również do tych instytucji państwowych i prywatnych, których pracownicy mają dostęp do informacji niejawnych. Głównym założeniem programu jest przybliżenie zagrożeń ze strony obcych służb specjalnych oraz podstawowych zasad bezpieczeństwa w kontaktach z osobami trzecimi, w szczególności obcokrajowcami. W 2009 r. w ramach ponad 130 spotkań, przeszkolono blisko 4 tys. osób, m.in. 718 urzędników Kancelarii Prezydenta i Prezesa Rady Ministrów, 370 pracowników ministerstw, 626 kandydatów na pełnomocników ds. ochrony informacji niejawnych, 353 urzędników samorządu terytorialnego i 128 funkcjonariuszy Policji.

Dotychczasowe doświadczenia związane z realizacją programu profilaktyki kontrwywiadowczej wskazują, iż spełnia on nie tylko ważną rolę w procesie przybliżania urzędnikom skali potencjalnych zagrożeń, ale wpływa również na usprawnienie wymiany informacji z urzędami państwowymi oraz na poprawę koordynacji działań z instytucjami odpowiedzialnymi za porządek i bezpieczeństwo RP.



Rys. 8. Liczba osób, które uczestniczyły w programie profilaktyki kontrwywiadowczej w poszczególnych miesiącach 2009 roku.

Profilaktyka kontrwywiadowcza jako jedna z metod zwalczania aktywności obcych służb specjalnych, w tym szpiegostwa, pozwala skutecznie zapobiegać często nieodwracalnym stratom wynikającym z utraty informacji istotnych dla bezpieczeństwa i interesów Rzeczypospolitej Polskiej.

2. Profilaktyka w zakresie bezpiecznego korzystania z internetu i zagrożeń cyberprzestrzeni

W ramach ochrony cyberprzestrzeni Rzeczypospolitej Polskiej w 2009 roku zostały uruchomione strony internetowe CERT.GOV.PL oraz SurfujBezpiecznie.pl. Ich celem jest uświadomienie społeczeństwu potencjalnych zagrożeń związanych z korzystaniem z Internetu oraz zapoznanie z metodami zabezpieczania się przed nimi. Nowo powstałe witryny umożliwiają polskim internautom bezpośredni kontakt i konsultacje ze specjalistami w dziedzinie bezpieczeństwa teleinformatycznego. Znajdują się na nich również praktyczne porady oraz zasady, których przestrzeganie zapewni użytkownikom sieci skuteczną ochronę.

3. Szkolenia dla urzędników administracji centralnej, w tym profilaktyka antykorupcyjna

Ważnym aspektem działań prewencyjnych podejmowanych przez ABW jest organizacja szkoleń dla urzędników administracji centralnej. Wiedza posiadana przez funkcjonariuszy Agencji zdobyta w trakcie wieloletniej pracy operacyjno-rozpoznawczej i dochodzeniowo-śledczej stanowi cenne źródło informacji o potencjalnych zagrożeniach, z którymi mogą mieć do czynienia pracownicy administracji państwowej podczas wykonywania obowiązków służbowych. Ponadto, uczestnicy szkoleń są również zapoznawani z funkcjonowaniem systemu bezpieczeństwa wewnętrznego kraju, jego elementami składowymi, obowiązującymi procedurami i zadaniami poszczególnych służb. W ramach szkoleń eksperci wyznaczonych jednostek organizacyjnych ABW poruszają następujące zagadnienia:

- bezpieczeństwo ekonomiczne państwa;
- prewencja antykorupcyjna;
- proliferacja broni masowego rażenia i zagrożenia rozpoznane w tym obszarze;
- funkcjonowanie systemu ochrony antyterrorystycznej RP;
- wybrane zagadnienia z działalności obcych służb specjalnych;
- bezpieczeństwo teleinformatyczne;
- przestępczość zorganizowana;
- bezpieczeństwo informacji niejawnych – zagrożenia i profilaktyka.

W 2009 r. ABW zorganizowała 26 szkoleń dotyczących tematyki bezpieczeństwa wewnętrznego przeznaczonych dla przedstawicieli administracji publicznej, w trakcie których coraz więcej uwagi poświęca się na omawianie zagadnień związanych z profilaktyką antykorupcyjną. Uczestniczyło w nich blisko 700 urzędników.

4. Szkolenia pełnomocników ds. ochrony informacji niejawnych

Zgodnie z art. 2 ust. 3 ustawy z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych, Agencja Bezpieczeństwa Wewnętrznego, obok Służby Kontrwywiadu Wojskowego, zalicza się do Służb Ochrony Państwa. Oznacza to, że jednym z jej obo-

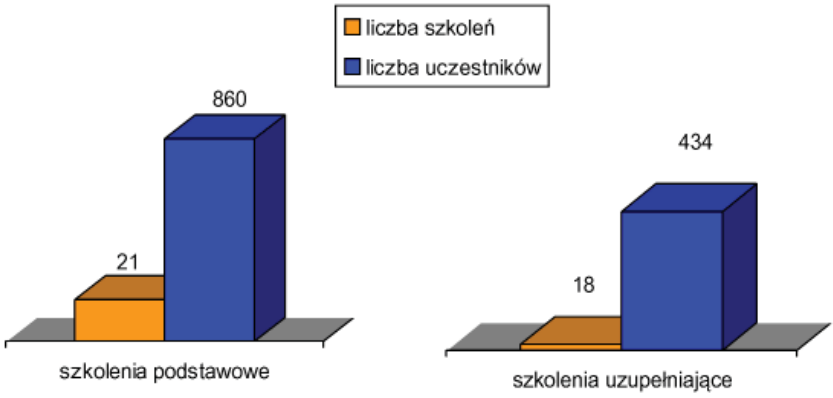
wiązków jest kontrola ochrony informacji niejawnych oraz przepisów obowiązujących w tym zakresie. ABW jest zobligowana do prowadzenia szkoleń i doradztwa w zakresie informacji niejawnych, w tym szkoleń podstawowych i uzupełniających dla pełnomocników ds. ochrony informacji niejawnych.

Szkolenia podstawowe przeznaczone są dla osób ubiegających się o funkcję pełnomocnika ochrony. Obejmują one:

- zapoznanie się z przepisami i zasadami ochrony informacji niejawnych;
- tryb postępowania w sytuacjach zagrożenia dla informacji niejawnych i zakres odpowiedzialności karnej za ich ujawnienie;
- zagadnienia związane z zagrożeniami ze strony obcych służb specjalnych;
- kwestie dotyczące prawidłowości postępowań sprawdzających prowadzonych przez pełnomocników ochrony.

W 2009 r. ABW przeprowadziła 21 szkoleń podstawowych dla pełnomocników ochrony i ich zastępców, które objęły łącznie 860 osób. Szkolenia uzupełniające przeznaczone są dla osób, które pełnią już funkcje pełnomocnika ds. ochrony informacji niejawnych. Są one powtarzane co 5 lat. W 2009 r. zorganizowano 18 szkoleń uzupełniających, w których uczestniczyły 434 osoby.

Nowatorskim przedsięwzięciem było otwarcie na stronie internetowej ABW forum dotyczącego problematyki ochrony informacji niejawnych, na którym pełnomocnicy ochrony mogą wymieniać swoje doświadczenia oraz konsultować się z funkcjonariuszami Agencji.



Rys. 9. Szkolenia dla pełnomocników ds. ochrony informacji niejawnych przeprowadzone przez ABW w 2009 roku

5. Szkolenia administratorów i inspektorów sieci teleinformatycznych

Cyberterroryzm stanowi obecnie jedno z głównych zagrożeń dla bezpieczeństwa wewnętrznego RP. Spowodowane jest to kilkoma czynnikami, m.in.:

- rosnącą liczbą użytkowników sieci internetowej, co potencjalnie może skutkować zwiększeniem ilości źródeł ataku;
- niewielkimi kosztami związanymi z jego stosowaniem;
- globalnym zasięgiem potencjalnego ataku;

- możliwością zachowania praktycznie pełnej anonimowości przez osoby bądź podmioty odpowiedzialne za atak.

Należy również zaznaczyć, że współczesne państwa – w tym Polska – w wysokim stopniu zależne są od sieci i systemów teleinformatycznych. W przypadku ich sparaliżowania może zostać zakłócone funkcjonowanie całego kraju. Przykładem tego nowego typu zagrożenia były wydarzenia w Estonii w 2007 r., gdzie w wyniku zmasowanego ataku hakerów na strony internetowe urzędów i instytucji państwowych na kilkanaście godzin sparaliżowana została ich praca. Do podobnego zdarzenia doszło również w Polsce. W maju 2009 r. został zaatakowany serwer pocztowy Urzędu Miasta w Poznaniu. Spowodowało to trzydniowe zakłócenia w funkcjonowaniu poczty elektronicznej urzędu.

Z uwagi na istnienie realnego zagrożenia ze strony cyberterroryzmu, Agencja Bezpieczeństwa Wewnętrznego postawiła sobie za cel zapewnienie poprawności i ciągłości funkcjonowania systemów i sieci teleinformatycznych wchodzących w skład krytycznej infrastruktury teleinformatycznej kraju oraz bezpieczeństwa przetwarzanych w nich informacji.

W związku z tym, ABW organizuje szkolenia dla administratorów i inspektorów sieci teleinformatycznych, w których przetwarzane są informacje niejawne. W 2009 r. w szkoleniach tych uczestniczyły 3152 osoby. Administrator sieci odpowiada za przestrzeganie zasad i wymogów bezpieczeństwa systemu oraz za jego funkcjonowanie. Natomiast rolą inspektora jest bieżąca kontrola zgodności działań systemu z dokumentacją bezpieczeństwa.

O przeszkolenie przez ABW w zakresie bezpieczeństwa teleinformatycznego mogą ubiegać się zarówno instytucje państwowe, jak i prywatne podmioty gospodarcze.

6. Studia podyplomowe „Bezpieczeństwo Wewnętrzne”

ABW kładzie szczególny nacisk na doskonalenie zawodowe funkcjonariuszy Agencji, uwzględniając przy tym konieczność stałego poszerzania przez nich wiedzy z zakresu politologii, sfery relacji międzynarodowych mogących mieć znaczenie dla bezpieczeństwa wewnętrznego RP, a także prawnych i technicznych aspektów ochrony informacji niejawnych. W tym celu 1 lipca 2008 r. ABW podpisała porozumienie o współpracy naukowo-dydaktycznej z Wydziałem Dziennikarstwa i Nauk Politycznych Uniwersytetu Warszawskiego. Stworzyło ono funkcjonariuszom ABW warunki do dalszego rozwoju zawodowego poprzez możliwość kształcenia się na studiach realizujących program nauczania w zakresie interesującym Agencję. Celem tego przedsięwzięcia jest również rozwój teoretycznej, jak i praktycznej sfery ochrony bezpieczeństwa wewnętrznego kraju poprzez wymianę wzajemnych doświadczeń w tej dziedzinie.

W czerwcu 2009 r. zakończyła się I edycja studiów – specjalizacja „Bezpieczeństwo informacji” i „Terroryzm współczesny”. Naukę ukończyło 60 osób. Program merytoryczny utworzonego kierunku został opracowany przy udziale ekspertów ABW, którzy prowadzili także wybrane zajęcia. Słuchacze zapoznani zostali z różnymi aspektami bezpieczeństwa wewnętrznego, w tym m.in.:

- problemami współczesnego państwa;
- instytucjami i prawem UE dotyczącym bezpieczeństwa wewnętrznego;
- prawno-konstytucyjnymi podstawami bezpieczeństwa narodowego i wewnętrznego;
- bezpieczeństwem teleinformatycznym;

- bezpieczeństwem przemysłowym;
- ochroną informacji niejawnych;
- białym wywiadem;
- rolą służb specjalnych we współczesnym państwie;
- zarządzaniem kryzysowym.

W październiku 2009 r. ruszyła druga edycja studiów.

7. Konferencje tematyczne

Agencja Bezpieczeństwa Wewnętrznego w ramach szeroko rozumianych działań profilaktycznych organizuje konferencje, na które zapraszani są reprezentanci instytucji państwowych, przedstawiciele krajowych i zagranicznych służb specjalnych oraz zewnętrzni eksperci i naukowcy. Celem tych spotkań jest omawianie istniejących zagrożeń dla bezpieczeństwa wewnętrznego RP, perspektyw ich dalszego rozwoju, a także opracowanie nowych metod skutecznego ich zwalczania oraz wymiana wzajemnych doświadczeń.

W Centralnym Ośrodku Szkolenia ABW w Emowie odbyła się konferencja zatytułowana *Proliferacja broni masowego rażenia – wyzwanie dla polskiej administracji rządowej*. Jej współorganizatorem było Ministerstwo Spraw Zagranicznych. W COS ABW miało również miejsce spotkanie poświęcone ochronie informacji niejawnych pt. *10 lat Ustawy o ochronie informacji niejawnych*.

Wspomnieć należy także o otwartej we wrześniu 2009 r. – w związku z 70. rocznicą wybuchu II wojny światowej – wystawie poświęconej działalności służb specjalnych II RP. Wystawę zorganizowano w gmachu Agencji Bezpieczeństwa Wewnętrznego w Warszawie. Zaprezentowano tam m.in. dokumenty operacyjne Oddziału II Sztabu Głównego Wojska Polskiego dotyczące rozpracowania niemieckiego agenta oraz materiały sporządzone przez wywiadowców Armii Krajowej. Główną atrakcję stanowiła jednak unikatowa prezentacja środków pracy służb specjalnych z okresu międzywojennego. Inicjatywa ABW w zakresie szerzenia wiedzy dotyczącej służb specjalnych spotkała się z pozytywnym przyjęciem ze strony władz państwowych, w tym Marszałka Sejmu RP Bronisława Komorowskiego, który w liście do Szefa ABW z najwyższym uznaniem wypowiedział się o zorganizowanej przez Agencję wystawie upamiętniającej wkład służb specjalnych II RP w walkę o wolność i niepodległość kraju.