Kuba Jałoszyński
Waldemar Zubrzycki
Jarosław Jabłoński
Jarosław Stelmach

# KONTRTERRORYZM
# SIŁY SPECJALNE, DZIAŁANIA
# WYDARZENIA W 2018 ROKU


Szczytno 2019

Recenzent
*prof. dr hab. Hubert Królikowski*

Redakcja Wydawcy
*Małgorzata Bukowska*
*Agnieszka Kamińska*

Projekt okładki
*Agnieszka Kamińska*

Zdjęcie na okładce
<http://www.lubuska.policja.gov.pl/go/serwis-informacyjny/aktualnosci/28699,szturm-odbijajacy-zakladnikow-dynamiczne-cwiczenia--antyterrorystow.html>, dostęp: 13 marca 2019 r.

WYDAWNICTWO
WYŻSZEJ SZKOŁY POLICJI
w Szczytnie



ISBN: 978–83–7462–696–5
e-ISBN: 978–83–7462–697–2

Druk i oprawa:
Dział Wydawnictw i Poligrafii Wyższej Szkoły Policji w Szczytnie
12-100 Szczytno, ul. Marszałka Józefa Piłsudskiego 111
tel. 89 621 54 10, fax 89 621 54 48, e-mail: wwip@wspol.edu.pl
Objętość: 16,34 ark. wyd.

# SPIS TREŚCI

*Pamięci:*

***st. chor. sztab. rez. Piotra WYSOCKIEGO***
*Żołnierza Oddziału Specjalnego*
*Żandarmerii Wojskowej w Warszawie*

***Sgt. Matta TONROEA***
*Żołnierza brytyjskiej jednostki SAS*

***Master Sgt. Jonathana J. DUNBARA***
*Żołnierza amerykańskiej jednostki*
*DELTA FORCE*

***asp. sztab. Adama PAWLAKA***
*Zastępcy Dowódcy SPAP w Gorzowie Wielkopolskim*

***st. chor. sztab. rez. Bartosza KANKOWSKIEGO***
*Żołnierza jednostki specjalnej GROM*

*W 2018 roku odeszli na wieczną służbę…*

# Wprowadzenie

Z satysfakcją odnotowuję fakt wydania kolejnej monografii, stanowiącej część corocznych publikacji o wspólnie brzmiącym tytule: *Kontrterroryzm*… Tegoroczna odwołuje się w swej części kalendarium do wydarzeń z obszaru działań kontrterrorystycznych w 2018 r.

Na podstawie rozmów z czytelnikami mogę stwierdzić, że dwie poprzednie monografie zostały pozytywnie przez nich ocenione, uznane za pozycje wartościowe. Mam nadzieję, że zamieszone w tej publikacji teksty również zyskają oceny pozytywne, a ich zawartość merytoryczna będzie stanowiła cenne źródło wiedzy z zakresu kontrterroryzmu. Grono osób zajmujących się tą problematyką, czy to naukowo, czy też hobbystycznie, jest dość znaczne. Siły specjalne, działania specjalne — zawsze były i są obszarem zainteresowania pasjonatów, co wynika m.in. z „tajemniczości" ich charakteru. Wprawdzie zostały one przez ostatnie dwie dekady „odarte" w mediach ze swoich tajemnic, nad czym osobiście ubolewam, to i tak pozostaje jeszcze część aktywności sił kontrterrorystycznych poza zasięgiem medialnej dostępności.

Kiedy poniższa monografia ukaże się na rynku wydawniczym, będą już trwały prace nad kolejną, która to będzie zawierała kalendarium wydarzeń odnoszących się do 2019 r. Zamiarem autorów jest, aby ta kolejna publikacja swoją zawartością tematyczną objęła zarówno siły kontrterrorystyczne w naszym kraju, jak i siły kontrterrorystyczne amerykańskie. Wszystko wskazuje na to, że ten zamiar za rok zostanie zmaterializowany w postaci następnego wydania *Kontrterroryzmu*.

*Kuba Jałoszyński*

*Jarosław Jabłoński*

# 1. Współdziałanie międzyagencyjne w środowisku zagrożeń atakiem terrorystycznym z użyciem broni masowego rażenia

Od kilku dekad wielu analityków uważa, że prawdopodobne jest użycie broni chemicznej i biologicznej przez terrorystów lub państwa bandyckie przeciwko państwom cywilizacji zachodniej. U podstaw takiej opinii jest wzrost świadomości terrorystów i ich mocodawców, że tradycyjne odstraszanie ze strony państw kultury zachodniej — zwłaszcza w aspekcie zbrojnej odpowiedzi — jest obecnie mniej wiarygodne. Do pewnego stopnia organizacje terrorystyczne mogą czuć się odporne na reakcję odwetową państw zachodnich, natomiast dla państw zbójeckich możliwe korzyści płynące z użycia broni masowego rażenia (BMR) przeważają nad potencjalnymi działaniami odwetowymi.

Istnieje wiele czynników, które mogą doprowadzić do zwiększenia ryzyka incydentów terrorystycznych z udziałem BMR:

1. Nieodwracalny postęp nauki i technologii oraz dalsze rozpowszechnianie wiedzy na temat BMR.
2. Rosnący arsenał nuklearny Korei Północnej, postrzegany jako zachęta dla państw zbójeckich w pozyskiwaniu BMR.
3. Zwiększenie współpracy organizacji terrorystycznych.
4. Rosnący arsenał nuklearny Pakistanu i rozwój broni nuklearnych.
5. Postępujący brak współpracy w zakresie bezpieczeństwa jądrowego USA–Rosja po inwazji Rosji na Ukrainę w 2014 r.
6. Erozja zaufania do międzynarodowego systemu kontrproliferacji.
7. Zwiększenie ilości przerobionego plutonu w Chinach i Japonii.

Szczęśliwie istnieje jednak inna grupa czynników, które mogą zmniejszyć ilość zagrożeń płynących z pozyskania i inicjowania przez terrorystów BMR, a wśród nich:

1. Utrzymanie wysokiego tempa fizycznej likwidacji grup terrorystycznych.
2. Dopracowywanie mechanizmów obronnych przed BMR, obejmujących międzyagencyjne współdziałanie oraz fuzje struktur wywiadowczych ukierunkowanych na przeciwdziałanie pozyskiwaniu BMR przez grupy terrorystyczne,
3. Zwiększenie finansowania struktur wywiadowczych.
4. Zwiększenie świadomości społecznej w zakresie zagrożenia terrorystycznego.
5. Amerykańsko-rosyjska współpraca w zakresie bezpieczeństwa jądrowego.
6. Kontynuacja przez Stany Zjednoczone organizacji szczytów bezpieczeństwa nuklearnego, które rozwijają międzynarodowy i narodowe systemy bezpieczeństwa przed BMR.
7. Ograniczenie proliferacji broni jądrowej.
8. Zamknięcie minimum 50 reaktorów badawczych wykorzystujących wzbogacony uran.
9. Powstrzymanie programów nuklearnych Iranu oraz Korei Północnej.

Przed objęciem prezydentury przez Baracka Obamę federalne Centrum Studiów nad Bronią Masowego Rażenia opublikowało raport, w którym, opierając się na czterech możliwych scenariuszach użycia BMR przez terrorystów, przedstawiło wnioski do realizacji przez nową administrację Białego Domu. Przede wszystkim wskazano, że na żaden z tych scenariuszy Stany Zjednoczone nie są przygotowane. Co gorsze, nawet wprowadzenie natychmiastowego programu naprawczego wymaga wieloletniego wysiłku organizacyjnego i finansowego celem zmniejszenia zagrożenia oraz skutków ewentualnego użycia BMR[1].

Konsekwencją takiej oceny było m.in. powołanie w Departamencie Obrony Zadaniowego Zespołu Badawczego ds. Obrony, Odstraszania, Zapobiegania i Reagowania na Zagrożenie lub Użycie Broni Masowego

[1] National Defense University, U.S. Government Printing Office, Center for the tudy of Weapons of Mass Destruction, *Are We Prepared? Four WMD crises that could transform U.S. Security*, Washington, June 2009.

Rażenia (ang. Defense Science Board Task Force on Deterring, Preventing, and Responding to the Threat or Use of Weapons of Mass Destruction, DSB TF DPRTU WMD), który otrzymał szerokie uprawnienie do przeprowadzenia przeglądu systemu obrony przed BMR w strukturach podległych Departamentowi Obrony. Zgromadzone dane pozwoliły przedstawić uwagi w trzech grupach, które odnoszą się w wielu miejscach do różnych podmiotów bezpieczeństwa Departamentu Obrony[2].

Pierwszym obszarem, na który zwrócono uwagę, był podsystem wczesnego ostrzegania. Potwierdzono potrzebę ciągłego monitorowania informacji na temat pojawiających się zagrożeń użycia BMR na najwcześniejszych etapach potencjalnego rozwoju zagrożenia i na wszystkich etapach ewolucji tego zagrożenia. Czas przygotowania użycia BMR przez terrorystów zależy od ciągu wydarzeń, które poprzedzają taki incydent. W odniesieniu do BMR wczesne ostrzeganie obejmuje wykrywanie zamiaru, który może być widoczny na wiele lat przed podjęciem praktycznych działań przez terrorystów, a tym samym na lata przed realizacją zagrożenia. Znaczenie wczesnego ostrzegania opiera się na założeniu, że im wcześniej dotrze ostrzeżenie, tym więcej opcji pozostanie dostępnych dla decydentów poziomu strategicznego i tym skuteczniej pozwoli zapobiec dalszym postępom w rozwoju zagrożenia BMR.

Wskazano na grupę zalecanych usprawnień w obszarze wczesnego ostrzegania, które można osiągnąć dzięki zastosowaniu nowych technologii w zarządzaniu dużymi zbiorami danych i analizie danych. Obowiązek poszukiwania oraz implementacji nowoczesnych narzędzi analitycznych, wymiany danych w działaniach przeciw użyciu BMR spoczywa nadal przede wszystkim na Agencji Redukcji Zagrożeń Obronnych (ang. Defense Threat Reduction Agency, DTRA) w Departamencie Obrony.

Warto więc w tym miejscu przybliżyć, jakim wsparciem technologicznym w zakresie komunikacji, wymiany i analizy danych BMR dysponuje Departament Obrony. Ważną cechą sieciowego połączenia wszystkich elementów współdziałających w zakresie obrony przed BMR jest ich relatywnie niski koszt implementacji. Wprowadzenie technologii polega przede

[2] Office of the Under Secretary of Defense for Research and Engineering, *Task Force On Deterring, Preventing, And Responding to the threat or use of Weapons of Mass Destruction. Executive Summary*, Washington, May 2018.

wszystkim na optymalizacji istniejących systemów telekomunikacyjnych, zamiast wprowadzania drogich nowych systemów łączności.

Szczególnie w proaktywnym, wczesnym ostrzeganiu przed BMR wysokie nasycenie technologiami jest warunkiem koniecznym do efektywnego zapobiegania użyciu BMR. Wraz z rozwojem nauki, w tym nowoczesnych technologii, system kontroli nad materiałami, technologią ich wytwarzania oraz wzrastającą liczbą specjalistów zajmujących się BMR staje się trudny do monitorowania. Technologie produkcji BMR rozwijają się szybciej niż techniki i metody zapobiegania ich użyciu (przykładowo szczepionki przeciw niektórym patogenom są takie same od ponad dwóch dekad). Obecnie zapobieganie w dziedzinie nowoczesnych technologii opiera się na badaniach i wdrażaniu nowych projektów w kilku obszarach. Pośród nich w systemie bezpieczeństwa Stanów Zjednoczonych można wyróżnić obszar szeroko pojętego wykorzystania sztucznej inteligencji (ang. *artificial intelligence*, AI) oraz uczenia maszynowego (ang. *machine learning*, ML) ukierunkowane na[3]:

1. Nawigację/pozycjonowanie i śledzenie elementów BMR.
2. Zasilanie stałej świadomości operacyjnej elementów systemu BMR.
3. Odnajdywanie informacji i danych z zakresu nielegalnej proliferacji BMR.
4. Biometrykę w działaniach BMR.
5. Zapewnienie łączności międzyagencyjnej odpornej na zakłócenia.

Amerykańskie działania odnośnie do BMR w obszarze wczesnego ostrzegania (w zakresie zintegrowanego chemicznego i biologicznego ostrzegania) opierają się przede wszystkim na optymalizacji posiadanych sił i środków (w tym łączności), które nie wymagają znaczących nakładów finansowych[4]. Do tej grupy działań należą: integrowanie różnego rodzaju sensorów (detektorów z aplikacjami na telefonach komórkowych itp.), informowanie o zagrożeniach oraz zastosowanie zaawansowanych

[3] Zagadnienia poruszane podczas udziału w konferencji Special Operation Forces Policy Forum organizowanej przez Global SOF Foundation w siedzibie organizacji New America w Waszyngtonie 13 listopada 2018 r. Szerzej na temat konferencji na stronie internetowej: <https://gsof.org/event/2018-sof-policy-forum/>, dostęp: 16 listopada 2018 r.

[4] R. Nixon, *Increasing Predictability For Enhanced incident Preparedness*, "Security & Border and CST/CBRN" 2018, nr 3, s. 6.

algorytmów postępowania w wielu domenach działań (ochrona przed BMR na poziomie taktycznym i operacyjnym, operacje informacyjne itp.) podczas podejmowania decyzji, dowodzenia i kierowania operacją kontrterrorystyczną.

Najskuteczniejszą metodą zapobiegania użyciu BMR jest więc powiązanie dwóch elementów, odpowiednio wysokiego nasycenia sensorami (detektorami, analizatorami, transmiterami danych) pozyskiwanymi we współpracy z krajowymi i międzynarodowymi ośrodkami naukowymi (Stany Zjednoczone nie są już jedynym liderem w technologiach wykrywania BMR) oraz wprowadzania i uaktualniania procedur w systemie BMR. Utrzymanie jednolitej świadomości operacyjnej podmiotów uczestniczących w operacji BMR obejmować będzie wykorzystanie nowoczesnych technologii w zakresie przesyłania i analizy danych z obszaru BMR do wszystkich podmiotów bezpieczeństwa, tak aby podjęcie decyzji było szybkie i sprawne. Warto w tym jednak miejscu wskazać, że głównym obszarem operacji BMR powinno być skoncentrowanie na tzw. fazie zerowej (wykrycie intencji przejęcia elementów BMR), co zawsze pozwoli na zaoszczędzenie czasu na efektywną reakcję.

Stany Zjednoczone kładą szczególny nacisk na rozwój programów wczesnego ostrzegania oraz międzyagencyjnego informowania w zakresie zagrożeń BMR. Całość działań prowadzona jest w ramach połączonego programu systemów informacyjnych (ang. Joint Project Manager for Information System, JPM-IS) oraz połączonego programu wykonawczego Biura Zagrożeń Chemicznych, Biologicznych, Radiologicznych, Obrony przed Bronią Nuklearną (ang. Joint Program Executive Office for Chemical, Biological, Radiological and Nuclear Defense, JPEO-CBRN)[5].

Zasadniczą częścią połączonego programu systemów informacyjnych jest dostarczenie na czas ostrzeżenia oraz odpowiednich danych celem uniknięcia lub ograniczenia użycia BMR. System informacyjny obejmuje model ochrony przed BMR, zarządzanie sytuacją kryzysową, analizę sposobu działania oraz posiadanie pakietu narzędzi teleinformatycznych do

[5] Szerzej na temat połączonego programu wykonawczego Biura Zagrożeń Chemicznych, Biologicznych, Radiologicznych, Obrony przed Bronią Nuklearną na stronie internetowej: <https://gsof.org/event/2018-sof-policy-forum/>, dostęp: 3 marca 2019 r.

podjęcia decyzji. Całość JMP-IS wspiera podmioty bezpieczeństwa za pomocą takich narzędzi funkcjonalnych jak[6]:

1. System informacyjny o zagrożeniach chemicznych, biologicznych, radiologicznych i nuklearnych (ang. CBRN Information System, CBRN-IS).
2. Połączony model odziaływania (ang. Joint Effect Model, JEM).
3. Połączona sieć ostrzegania i meldowania (ang. Joint Warming and Reporting Network, JWARN).
4. Połączony program odziaływania operacyjnego (ang. Joint Operational Effects Program, JOEF).
5. Wsparcie oprogramowania (ang. Softwear Support Activity, SSA).
6. Globalny portal rozpoznania biologicznego (ang. Global Biosurveillance Portal, G-BSP).

Zasadniczym wyzwaniem w ramach współpracy międzyagencyjnej w zakresie BMR jest wzmocnienie oraz systematyczne zasilanie świadomości operacyjnej wszystkich podmiotów podsystemu bezpieczeństwa przez użyciem BMR. Dostarczenie narzędzi oraz algorytmu postępowania podczas zagrożenia atakiem do wszystkich sił współdziałających w zakresie BMR znacząco skróci czas reakcji na zagrożenia i zwiększy efektywność działania podmiotów bezpieczeństwa. Stąd połączony program systemów informacyjnych został umieszczony jako program jawny, dostarczający w tzw. chmurze narzędzia do współdziałania w ramach zapobiegania atakowi terrorystycznemu z wykorzystaniem broni biologicznej pomiędzy podmiotami bezpieczeństwa państwa i zarządzania skutkami przeprowadzenia takiego ataku.

Obecnie narodowe systemy BMR w Stanach Zjednoczonych napotykają dwa zasadnicze problemy. Pierwszy to utrzymanie wysokiej transmisji danych wymaganych do realizacji zadań kontrproliferacji w środowisku wysokiej mobilności grup terrorystycznych (od poziomu taktycznego) oraz transfer danych pomiędzy systemami dowodzenia i łączności poszczególnych podmiotów bezpieczeństwa. Postępy w ramach pierwszego obszaru problemów w systemach amerykańskich monitorowane są przy

[6] *Promoting Information Evaluation and Diffusion*, "Security & Border and CST/CBRN" 2018, nr 3, s. 22.

użyciu technologii „chmury", w tym przypadku z wykorzystaniem teleinformatycznej (militarnej) platformy, przez którą dokonywana jest wymiana danych jawnych i niejawnych.

Kolejnym krokiem w zakresie wczesnego ostrzegania jest koordynacja całości przedsięwzięć w zakresie obrony przed BMR przez jeden podmiot bezpieczeństwa państwa szczebla strategicznego. Zadaniowa grupa Departamentu Obrony wskazała na zasadne utrzymanie decyzji podjętej przez Kongres Stanów Zjednoczonych w grudniu 2016 r. o przejęciu przez Dowództwo Sił Specjalnych Stanów Zjednoczonych (ang. US Special Operation Command, USSOCOM) od Strategicznego Dowództwa Stanów Zjednoczonych (ang. US Strategic Command, USSTRATCOM) odpowiedzialności za obronę państwa przed BMR. Planowanie zmiany struktury szczebla strategicznego trwało od początków 2015 r. W tym czasie wzrosła liczba możliwych zagrożeń płynących z prób pozyskania przez struktury terrorystyczne elementów BMR[7]. Stopień zagrożeń płynących z użycia BMR na terenie Stanów Zjednoczonych wpływa znacząco na opinie panujące wśród społeczności amerykańskiej. Dwóch na pięciu Amerykanów wierzy, że w ciągu 5 lat terroryści zdetonują ładunek jądrowy na terenie ich kraju. Statystycznie wierzy w to więcej osób niż w okresie zimnej wojny[8]. Jeżeli nawet wynik ten nie odzwierciedla realnego zagrożenia, należy przyznać, że terrorystom udało się zbudować atmosferę strachu i przyczynić się do zwiększenia nakładów państw na zabezpieczenie przed użyciem BMR. Jest więc dokładnie tak, jak terroryści chcą, aby było.

Stąd też przyczyną decyzji o przekazaniu dowodzenia w tego rodzaju operacjach jednemu ze swoich czterech podstawowych dowództw bojowych (ang. *combatant command*) był fakt braku posiadania przez USSTRATCOM odpowiednich sił i środków do zwalczania współczesnych zagrożeń BMR[9]. Standardem jest w systemie militarnego bezpieczeństwa

[7] G. Ackerman, M. Jacome, *WMD Terrorism. The Once and Future Threat*, "Prism" 2018, Vol. 7, No. 3, s. 25.

[8] B.M. Jenkins, *Will Terrorists Go Nuclear?*, New York 2008, <https://www.princeton.edu/~ota/disk3/1977/9586/958605>, dostęp: 16 stycznia 2018 r.

[9] T.M. Cronk, *Special Operations Leaders Testify Before Senate on SOF Global Posture*, <https://dod.defense.gov/News/Article/Article/1758218/special-operations-leaders-testify-before-senate-on-sof-global-posture/>, dostęp: 15 lutego 2019 r.

Stanów Zjednoczonych przyjęcie jednego odpowiedzialnego (gestora podsystemu bezpieczeństwa) spośród rodzajów sił zbrojnych, który przyjmuje rolę koordynatora działań pomiędzy pozostałymi rodzajami sił zbrojnych i agencjami rządowymi podsystemu bezpieczeństwa (w tym przypadku obrony przed BMR). Ponadto USSOCOM to nie tylko kolejne dowództwo posiadające uprawnienia dowództwa rodzaju wojsk, jest to przede wszystkim struktura, która odpowiada za koordynację działań globalnych, w tym przypadku amerykańskich i koalicyjnych sił specjalnych. Dodatkowo od 2018 r. USSOCOM posiada uprawnienia globalnego działania w trzech obszarach: działań kontrterrorystycznych, zwalczania zagrożeń użycia BMR oraz prowadzenia operacji informacyjnych. Najważniejszy jest jednak fakt posiadania uprawnień do działań międzyagencyjnych poza Departamentem Obrony w obszarze bezpieczeństwa państwa.

Drugim obszarem wskazanym przez Zadaniowy Zespół Badawczy ds. Obrony, Odstraszania, Zapobiegania i Reagowania na Zagrożenie lub Użycie Broni Masowego Rażenia Departamentu Obrony był wzrost zagrożeń chemicznych i biologicznych. Potwierdzono, że poziom świadomości zagrożeń płynących z użycia tego rodzaju BMR jest wprost proporcjonalny do ilości wykrytych zagrożeń. Cechą wspólną wielu państw jest podejście proaktywne, międzyagencyjne zintensyfikowanie działań tylko w przypadku zaistnienia zagrożenia; spada ono do niskiego poziomu w okresie braku takich zagrożeń. W rezultacie często postęp w zakresie współpracy międzyagencyjnej i międzynarodowej zostaje ograniczony, a priorytety działań obrony przed bronią biologiczną i chemiczną podlegają resetowaniu, tak jak to miało miejsce w ciągu ostatnich dwóch dekad. Jednocześnie postęp techniczny w zakresie elementów broni chemicznej i biologicznej sprawia, że składniki produkcji oraz wiedza w zakresie ich budowy i użycia stają się coraz bardziej dostępne zarówno dla wrogich (upadłych) państw, jak i „samotnych wilków", którzy mogą osiągnąć zdolność do przeprowadzenia ograniczonych ataków z użyciem elementów BMR i, „pozostając w ukryciu", maskować wysiłki związane z nabywaniem elementów broni chemicznej lub biologicznej wśród innych legalnych działań.

Wskazano więc w tym obszarze na potrzebę strategicznej obrony państw w zakresie użycia broni chemicznej i biologicznej, która powinna

opierać się na działaniach obronnych oraz reagowaniu na wykryte zagrożenia. Zadaniowy Zespół Badawczy ds. Obrony, Odstraszania, Zapobiegania i Reagowania na Zagrożenie lub Użycie Broni Masowego Rażenia Departamentu Obrony założył, że posiadając wysokie nasycenie technologiami powiązanych sieciowo podmiotów bezpieczeństwa, można zyskać wystarczającą ilość czasu do zorganizowania i zaplanowania działań kontrterrorystycznych w stosunku do grup terrorystycznych zmierzających do użycia broni chemicznej lub biologicznej. Kluczowe jest przyjęcie strategii dogłębnej obrony, polegającej na zintegrowaniu pomiotów bezpieczeństwa bez nadmiernie rozbudowanej hierarchicznej struktury dowodzenia współdziałających w każdej fazie zagrożenia podmiotów bezpieczeństwa oraz po zaistnieniu incydentu z użyciem broni chemicznej lub biologicznej. Każdy rodzaj hierarchicznej odpowiedzi w stosunku do użycia broni chemicznej i biologicznej doprowadzi do nieadekwatnego rozwiązania i popełnienia błędów podczas działań struktur bezpieczeństwa w ramach ochrony przed BMR. Jest to poprawna i efektywna strategia, zamiast funkcjonowania samodzielnych komponentów, zgrywanych w razie potrzeb z różnych departamentów.

Jedocześnie w ramach Departamentu Obrony wskazano, że każdy komponent przeznaczony do realizacji głębokiej strategii obrony przed użyciem broni chemicznej i biologicznej podejmował własne programy rozwojowe i badawcze, testował plany operacyjne oraz dzielił się nimi przez zintegrowany system łączności z innymi podmiotami bezpieczeństwa. Tak jest w przypadku Armii Stanów Zjednoczonych, która pozyskiwany specjalistyczny sprzęt obejmuje programem testowym, a rezultatami z jego użytkowania dzieli się z innymi rodzajami wojsk[10]. Tego rodzaju zrównoważone działania wszystkich podmiotów w tym obszarze przynoszą dużo lepszy efekt niż te oparte na epizodycznej współpracy (ćwiczenia, treningi), tak jak to miało miejsce w przeszłości.

Osobną kwestią jest strategia reagowania na zagrożenia użycia broni nuklearnej. Broń nuklearna ponownie stała się ważnym elementem stosunków międzynarodowych. Rodzący się konflikt interesów pomiędzy

[10] *Robotic Research to expand US Army's AUSTC for counter-WMD mission*, <https://www.army-technology.com/news/robotic-research-to-support-us-armys-austc-effort-for-counter-wmd-mission/>, dostęp: 15 lutego 2019 r.

Stanami Zjednoczonymi i Rosją, powolny proces denuklearyzacji Półwyspu Koreańskiego, ambicje atomowe Iraku oraz Arabii Saudyjskiej doprowadziły do powrotu tematyki zagrożeń użyciem broni nuklearnej w stosunkach międzynarodowych. Co gorsze, od zakończenia zimnej wojny pojawiły się znaczące asymetrie zagrożeń jądrowych, co w połączeniu z możliwościami w nowych domenach zagrożeń (np. cyberprzestrzeń) doprowadza do sytuacji, w której przeciwnicy Stanów Zjednoczonych dokonują szybkiej korekty własnych działań celem ograniczenia interesów USA. Stany Zjednoczone nie tylko muszą utrzymywać odpowiedni poziom odstraszania przed wybuchem wojny nuklearnej, lecz także stawić czoła wyzwaniu konieczności walki z przeciwnikami uzbrojonymi w broń nuklearną.

Współczesne działania państw w zakresie obrony przed użyciem broni nuklearnej powinny zatem obejmować wysiłek w ramach trzech wzajemnie powiązanych linii:

1. Wzmocnienie zintegrowanej koncepcji strategicznego odstraszania, wykorzystującej zdolności konwencjonalne, jądrowe i niekinetyczne połączone z komunikacją oraz elastyczność operacyjną podmiotów bezpieczeństwa.
2. Integracja podsystemu wczesnego ostrzegania w planowaniu obronnym, prowadzonym nieprzerwanie jako kampania zapewniająca trwały wgląd w intencje, możliwości i plany terrorystów, w celu zmaksymalizowania możliwości powstrzymywania i/lub likwidacji grup terrorystycznych jeszcze przed podjęciem próby użycia BMR.
3. Działania zabezpieczające przed przyszłymi zagrożeniami poprzez badania naukowe zawansowanych technologii nuklearnych, które ograniczą możliwość ich proliferacji.

Potencjalne zagrożenia związane z użyciem BMR zarówno przeciwko celom wojskowym, jak i cywilnym rosną z roku na rok i wielokrotnie wyprzedzają działania podmiotów bezpieczeństwa[11]. Zadaniowy

[11] Oświadczenie dowódcy USSOCOM gen. Raymonda A. Thomasa przed Komisją Sił Zbrojnych Senatu Stanów Zjednoczonych, Waszyngton, 14 lutego 2019 r., <https://www.armed-services.senate.gov/imo/media/doc/Thomas_02-14-19.pdf>, dostęp: 15 lutego 2019 r.

Zespół Badawczy ds. Obrony, Odstraszania, Zapobiegania i Reagowania na Zagrożenie lub Użycie Broni Masowego Rażenia Departamentu Obrony potwierdził w swoim raporcie, że amerykański międzyresortowy system przeciwdziałania BMR pozostaje w tyle w stosunku do współczesnych zagrożeń, szczególnie w zakresie analizy, gromadzenia i dystrybucji danych do podmiotów systemu. Wskazano na potrzebę integrowania większej ilości danych z wielu rozproszonych źródeł informacji (w tym również otwartych źródeł) celem znalezienia wrogich intencji na długo przed pozyskaniem elementów BMR przez nieuprawnione nieautoryzowane osoby. Obecnie wielodyscyplinarne aplikacje przetwarzania i analizy dużej ilości danych umożliwiły znaczne postępy we wczesnym wykrywaniu zagrożeń w wielu domenach. Częściej ma to miejsce w aplikacjach taktycznych, wskazany jest więc dalszy rozwój tych aplikacji celem ich jednolitego zastosowania od poziomu taktycznego do strategicznego.

Wyzwania związane z wczesnym ostrzeganiem przed BMR to przede wszystkim wyzwania techniczne i organizacyjne. Technicznie wyzwania wymagają utrzymania ciągłej gotowości środków technicznych do analizy danych celem zapewnienia wczesnego ostrzegania przed intencją pozyskania i użycia BMR w czasie zbliżonym do rzeczywistego. Gromadzenie i analiza danych muszą być zapewnione w skali globalnej przez okres miesięcy lub nawet lat. Architektury systemów teleinformatycznych od szczebla taktycznego do strategicznego muszą być dostosowane do konkretnych domen: zagrożeń jądrowych, chemicznych i biologicznych, z jedoczesnym zapewnieniem dzielenia się oraz wymianą danych (wyników) pomiędzy zespołami analitycznymi. Obecne algorytmy analityczne są ograniczone, muszą więc być tak rozwijane, aby uzyskać jak największe zaufanie do precyzyjności ich wyników.

Wskazano na otwarte źródła informacji, których dynamiczny rozwój jest obecnie obserwowany. Ich rosnąca liczba, prędkość funkcjonowania, różnorodność i wartość mogą dostarczyć szczegółowych informacji o ludziach, organizacjach, relacjach, danych biometrycznych, geografii i transakcjach, niezależnie od tego, czy są ukierunkowane na zbieranie danych. Istnieje wiele platform i narzędzi informatycznych do wykorzystywania otwartych

źródeł, które są dostępne, a ich liczba oraz możliwości funkcjonalne wzrastają. Biorąc dodatkowo pod uwagę fakt, że terroryści komunikują się również z wykorzystaniem otwartych źródeł informacji, powinno to determinować jeszcze mocniej do rozbudowy platform analitycznych otwartych źródeł informacji. Obecnie otwarte źródła pozwalają na ocenę skutków zastosowania BMR oraz do pewnego stopnia na zapewnienie dostępu do rejonów o ograniczonym dostępie (ang. Anti-Access/Area Denial, A2AD), gdyż nawet mocno odizolowane grupy terrorystyczne muszą korzystać z usług bankowych czy też telefonii komórkowej. Wreszcie otwarte źródła mają dodatkową zaletę, że można się nimi dzielić z sojusznikami i innymi partnerami w przeciwdziałaniu użyciu BMR z zachowaniem ochrony źródeł informacyjnych oraz metod ich działania. Obecnie pod względem organizacyjnym systemy bezpieczeństwa przed BMR opierają się przede wszystkim na swojego rodzaju „koalicji chętnych do współpracy".

Biorąc pod uwagę kwestie techniczne i organizacyjne oraz możliwości wskazane przez Zadaniowy Zespół Badawczy ds. Obrony, Odstraszania, Zapobiegania i Reagowania na Zagrożenie lub Użycie Broni Masowego Rażenia Departamentu Obrony, przedstawiono następujące zalecenia:

1. Zwiększenie wykorzystywania potencjału otwartych źródeł informacji w zakresie wykrywania i monitorowania nielegalnych działań związanych z pozyskiwaniem BMR poprzez zorganizowanie krajowego centrum kontrproliferacji opartego na wirtualnym laboratorium współpracującym z analitykami, operatorami, planistami oraz ekspertami BMR.
2. Rozbudowa sieci informatorów wywiadu powiązanych z wirtualnym laboratorium analitycznym pozwalającym m.in. na połączenie otwartych i klasyfikowanych źródeł, których połączenie wpłynie na wzajemne dopasowywanie w celu poprawy skuteczności wczesnego ostrzegania o BMR (np. tworzenie zautomatyzowanych zestawów danych i modeli wczesnego ostrzegania w celu wspierania sygnalizacji zagrożeń oraz wymiany taktyki, techniki i procedury współdziałania).
3. Tworzenie i włączanie otwartych i niejawnych architektur wymiany informacji celem łączenia i wykonywania wspólnych funkcji (np. wykrywanie ścieżki logistycznej i ukrytego finansowania) we wszystkich domenach BMR z jednoczesnym zachowaniem możliwości głębokiego penetrowa-

nia danych w specyficznych wyzwaniach (np. kryminalistyka jądrowa i mapowanie rozprzestrzeniania chorób).

4. Zmiana organizacyjnego podejścia wielu podmiotów bezpieczeństwa do szerszego współdziałania w zakresie wykrywania inicjatyw pozyskania BMR poprzez wyznaczenie jednego agenta wykonawczego (np. w Stanach Zjednoczonych zostało nim Dowództwo Sił Specjalnych wyznaczone pomiędzy Sekretarzem Obrony), który pokieruje międzyagencyjnym połączonym zespołem zadaniowym (ang. Joint Interagency Task Force, JIATF)[12].
5. Inwestowanie w szkolenie kadr wraz z kształtowaniem ich nowoczesnej świadomości ukierunkowanej na międzyagencyjne, kreatywne i proaktywne wykrywanie działań inicjujących próby pozyskania BMR przez terrorystów.

W obszarze zdolności Departamentu Obrony do obrony przed atakami chemicznymi lub biologicznymi stwierdzono, że gotowość systemu bezpieczeństwa zdominowana jest przez skupienie się na niebezpiecznych, ale dobrze rozumianych zagrożeniach z okresu zimnej wojny. Najbardziej widocznym przykładem obaw przed bronią chemiczną jest użycie chloru, komercyjnej substancji chemicznej, której rząd syryjski użył przeciwko własnym obywatelom, naruszając konwencję o broni chemicznej[13]. Podobna sytuacja jest z bronią biologiczną, gdzie wraz z szybkim postępem w dziedzinie biologii syntetycznej istnieje potencjał dla zupełnie nowych klas zagrożeń biologicznych, które są trudne do detekcji z technicznego punktu widzenia. Stąd konkluzja, że proste dostosowanie istniejących technologii do nowych technologii produkcji BMR będzie niewystarczające. Historyczny nacisk na ochronę pojedynczego operatora, żołnierza, obywatela powinien ustąpić rozwiązaniu sytuacji od początku

[12] Przykładem zadaniowego zespołu jest połączony międzyagencyjny Zespół Zadaniowy — Południe (ang. Joint Interagency Task Force — South, JIATF-S), którego głównym zadaniem jest zapobieganie nielegalnemu przemytowi narkotyków z rejonów Ameryki Łacińskiej i Południowej na terytorium Stanów Zjednoczonych. Szerzej na temat JIATF-S na stronie internetowej: <https://www.jiatfs.southcom.mil>, dostęp: 28 lutego 2019 r.

[13] *Broń chemiczna w syryjskiej wojnie domowej 2011–2018*, „Biuletyn Centrum Szkolenia OPBMR", <http://www.akademia.mil.pl/biuletyn-centrum-szkolenia-opbmr/detail,nID,3603>, dostęp: 20 lutego 2019 r.

do końca. Inaczej mówiąc, zamiast ćwiczyć tylko te same punktowe scenariusze (przejęcie laboratorium z terrorystami, detekcja i dekontaminacja ludzi i infrastruktury krytycznej), należy rozbudowywać ciąg długoterminowych, międzyagencyjnych scenariuszy treningów i ćwiczeń obejmujących etapy: inicjacji zagrożenia BMR, braku jego wykrycia, dalszego rozwoju zagrożenia, neutralizacji grupy terrorystycznej i skutków użycia BMR, wyciągnięcia wniosków, ich implementacji oraz zatwierdzenie kolejnego etapu w postaci kolejnego ćwiczenia.

Sama strategia obrony przed atakami chemicznymi lub biologicznymi przez tzw. dogłębną obronę powinna być skoncentrowana na takich działaniach, aby przeciwnik był zmuszony do wyboru najbardziej korzystnego dla nas postępowania. Podobnie jak w przypadku odstraszania nuklearnego, sukces odstraszania od użycia broni chemicznej i biologicznej definiowany jest jako brak ataku (incydentu) z użyciem tego rodzaju broni, a nie atak, który został skutecznie odparty. Solidna, zintegrowana strategia głębokiej obrony zapewni efekt odstraszający i sprawi, że przeciwnicy będą niepewni, czy atak się powiedzie i czy odwet nie przekroczy akceptowalnego poziomu.

Obrona głęboka przed BMR musi być systemem opartym na zintegrowanych, współpracujących elementach, a nie na zestawie autonomicznych programów poszczególnych podmiotów bezpieczeństwa narodowego. Zalety i potencjał jednego podmiotu systemu powinny zrekompensować słabe strony innych podmiotów. Nadrzędnym przekazem dla chętnych inicjujących pozyskanie BMR jest wywołanie stanu niepewności oraz budowanie ograniczeń w możliwości działania terrorystów.

Z organizacyjnego i administracyjnego punktu widzenia zagrożenia bronią biologiczną i chemiczną były traktowane jako jedna klasa zagrożeń. Broń chemiczna i broń biologiczna mają podobieństwa (np. niskie bariery wejścia i prawie zawsze są przeznaczone do zabijania lub obezwładniania ludzi, a nie niszczenia struktur lub innych systemów broni). Różnią się jednak w istotny i konkretny sposób, obie ewoluowały jako oddzielne klasy zagrożeń, w dużej mierze dlatego, że efekty ich działania są różne, podobnie jak technologie, które mają im przeciwdziałać. Perspektywy dalszego rozwoju zagrożenia również się różnią, a szybki postęp w dziedzinie biologii i biotechnologii stwarza większe ryzyko zaskoczenia w zakresie

broni biologicznej. Charakter podobieństw i różnic między bronią biologiczną i chemiczną dowodzi, że strategię obrony głębokiej można oprzeć na wspólnych elementach, ale wdrożenie strategii powinno być inne dla broni biologicznej i chemicznej.

Opierając się na doświadczeniach oraz kierunkach rozwoju międzyagencyjnego sytemu bezpieczeństwa Stanów Zjednoczonych w zakresie zapobiegania użyciu BMR, należałoby przyjąć pewne rozwiązania. Przede wszystkim należy zlikwidować zróżnicowanie systemów łączności posiadanych przez podmioty zobligowane do działania w ramach operacji BMR. Jednocześnie należy doprowadzać do zwiększenia poziomu zaangażowania podmiotów bezpieczeństwa poprzez zwiększanie ich zaangażowania we wszelkiego rodzaju treningi i ćwiczenia z zakresu ochrony przed BMR, wspólne planowanie oraz wzajemne wykorzystywanie posiadanych sił i środków.

Jeśli chodzi o współdziałanie, należy promować wszelkie techniki i technologie zwiększające poziom analizy danych, informacji i wiedzy z zakresu BMR. Celem uzupełnienia działań w obszarze ochrony należy przyjąć krajową strategię głębokiej obrony przed BMR obejmującą:

1. Prewencję — działania dyplomatyczne i kontrolne w obszarze BMR (np. międzynarodowa współpraca w dziedzinie wymiany informacji, danych wywiadowczych oraz dobrych praktyk w zakresie BMR), wymiana danych i doświadczeń pomiędzy ośrodkami naukowymi (laboratoriami), kontrola materiałów wykorzystywanych do produkcji BMR.
2. Utrzymanie aktywnej świadomości w zakresie BMR — wczesne ostrzeganie, eksploracja otwartych źródeł wiedzy na korzyść osób/ ośrodków decyzyjnych, zastosowanie modelowania i gier symulacyjnych, operacje *red teaming*[14].

[14] Operacje *red teaming* — to testy bezpieczeństwa polegające na przeprowadzeniu kontrolowanego ataku na podstawie realistycznych scenariuszy, pozwalające strukturom bezpieczeństwa ocenić ich świadomość zagrożeń cybernetycznych oraz stopień gotowości na prawdziwy atak. *Red teaming* wykracza poza znaczenie testu podatności i napędza transformację organizacji w aspekcie cyberbezpieczeństwo, co w rezultacie pozwala zwiększyć dojrzałość procesów bezpieczeństwa. Zob. *Bezpieczeństwo fizyczne, zasoby ludzkie, a może cyberbezpieczeństwo? Czy znasz swoje słabe strony? Operacje Red Teaming*, <https://www2.deloitte.com/content/dam/Deloitte/pl/Documents/Brochures/pl_Cyber_RedTeam_flyer_web_270717.pdf>, dostęp: 18 lutego 2019 r.

3. Prowadzenie operacji międzyresortowych (w tym operacji mylących), ćwiczeń, treningów, seminariów, konferencji z mocnym przekazem informacyjnym.
4. Fizyczną neutralizację grup terrorystycznych (likwidacja grup w fazie pozyskiwania BMR).
5. Wzmocnienie działań kont proliferacyjnych.
6. Budowę silnej bazy technologicznej — wzmacniającej działania kontrterrorystyczne przed BMR (np. integracja zdolności wywiadowczych z detekcją), rozwój kadr w systemie zwalczania zagrożeń (wzrost finansowania celem szerszej rekrutacji i pozyskiwania wyspecjalizowanego personelu oraz utrzymania go w strukturach bezpieczeństwa), wzmocnienie znaczenia ośrodków/ centrów współpracy naukowców, firm oraz użytkowników technologii zwalczania BMR.
7. Wykorzystywanie i testowanie międzyresortowego systemu zwalczania zagrożeń BMR podczas klęsk żywiołowych.

Z całą pewnością możemy wskazać na pewną grupę zadań, które charakteryzują prawidłowo funkcjonujący zadaniowy zespół BMR. Takiego rodzaju zespół zadaniowy powinien być powołany na szczeblu międzyresortowym w krajowym systemie bezpieczeństwa. Wśród możliwości tego typu zespołu powinno znajdować się[15]:

1. Wypełnienie powierzonych zadań (zarówno wskazanych, jak i sugerowanych).
2. Usunięcie (zabicie, przejęcie) przywódców grup terrorystycznych i realizatorów.
3. Zniszczenie sieciowego połączenia grupy pozyskującej BMR.
4. Zablokowanie/zniszczenie aktywów finansowych, zdolności planistycznych i komunikacji grupy pozyskującej BMR.
5. Zidentyfikowanie i usunięcie kluczowych członków grupy pozyskującej BMR (finansistów, planistów, strategów, rekruterów oraz propagandzistów).
6. Zmniejszenie prawdopodobieństwa przeprowadzenia ataku BMR.
7. Zmniejszenie liczby bezpośrednich i inspirowanych ataków.

[15] The Joint Special Operations University Press, *Countering Transregional Terrorism*, Florida, sierpień 2018, s. 146–149.

8. Zwiększenie liczby informatorów oraz zwerbowanych terrorystów.
9. Zwiększenie procesów integracyjnych podmiotów bezpieczeństwa.
10. Zwiększenie liczby partnerów koalicyjnych w zakresie BMR.
11. Zwiększenie efektywności podsystemu sądowniczego oraz profesjonalnego egzekwowania prawa.
12. Zwiększenie możliwości zakłócania głębokiego sieci informatycznych.
13. Wymuszenie na terrorystach zmiany sposobu działania.
14. Zmniejszenie możliwości pozyskiwania przez terrorystów wsparcia ze strony grup kryminalnych.
15. Likwidacja bojowników zagranicznych w grupach terrorystycznych.
16. Zakłócenie narracji walki informacyjnej ze strony terrorystów.
17. Zmniejszenie wpływów terrorystów w Internecie i mediach społecznościowych.
18. Budowa mocnej narracji opartej na szerokim rozpowszechnianiu istotnych, zgodnych oraz płynnych informacji.

*Waldemar Zubrzycki*

## 2. Głos w dyskusji o służbie kontrterrorystycznej

Działania kontrterrorystyczne, jak w art. 2 pkt 2 definiuje je ustawa o działaniach antyterrorystycznych[1], to działania wobec sprawców przestępstwa o charakterze terrorystycznym, osób je przygotowujących lub pomagających w jego dokonaniu[2], prowadzone w celu wyeliminowania bezpośredniego zagrożenia życia, zdrowia lub wolności osób lub mienia przy wykorzystaniu specjalistycznych sił i środków oraz specjalistycznej taktyki działania. Działania kontrterrorystyczne są prowadzone przez wyspecjalizowane policyjne i wojskowe formacje państwowe, wchodzące w skład pododdziałów kontrterrorystycznych, które należy utożsamiać ze zbrojnym ramieniem działań antyterrorystycznych[3]. Obejmują one m.in. operacje reagowania kryzysowego, stanowiące odpowiedź na bezpośrednie zagrożenia terrorystyczne lub incydenty o takim charakterze, gdy zapobieganie im nie przynosi rezultatów[4]. W Polsce prowadzenie działań kontrterrorystycznych to jedno z podstawowych zadań Policji[5],

---

[1] Ustawa z 10 czerwca 2016 r. o działaniach antyterrorystycznych, DzU z 2016 r., poz. 904 ze zm.

[2] Przestępstwem o charakterze terrorystycznym jest czyn zabroniony zagrożony karą pozbawienia wolności, której górna granica wynosi co najmniej 5 lat, popełniony w celu: 1) poważnego zastraszenia wielu osób, 2) zmuszenia organu władzy publicznej Rzeczypospolitej Polskiej lub innego państwa albo organu organizacji międzynarodowej do podjęcia lub zaniechania określonych czynności, 3) wywołania poważnych zakłóceń w ustroju lub gospodarce Rzeczypospolitej Polskiej, innego państwa lub organizacji międzynarodowej — a także groźba popełnienia takiego czynu. Zob. ustawa z 6 czerwca 1997 r. — Kodeks karny, DzU z 1997 r., nr 88, poz. 553 ze zm., art. 115 § 20.

[3] K. Jałoszyński, *Jednostka kontrterrorystyczna — element działań bojowych w systemie bezpieczeństwa antyterrorystycznego,* Szczytno 2011, s. 46.

[4] T. Blackmon, *Anti-Terrorism v. Counter-Terrorism*, <https://www.linkedin.com/pulse/anti-terrorism-v-counter-terrorism-tony-blackmon>, dostęp: 15.12.2018 r.

[5] Ustawa z 6 kwietnia 1990 r. o Policji, DzU z 2015 r., poz. 355 ze zm., art. 1 ust. 2 pkt 3a wprowadzony art. 27 pkt 1 ustawy o działaniach antyterrorystycznych.

zaś specjalistycznymi siłami, o których mowa w definicji, są — na tę chwilę[6] — pododdziały antyterrorystyczne Policji[7]. Są to wyodrębnione w strukturze Policji etatowe jednostki i komórka organizacyjna, odpowiednio przeszkolone i wyposażone do działań o charakterze specjalnym[8], a zasadniczym celem ich utrzymywania jest przygotowanie Policji do fizycznego zwalczania aktów terrorystycznych, tj. fizycznej reakcji na fakt popełnienia przestępstwa o takim charakterze[9].

W historii policyjnych pododdziałów antyterrorystycznych zdarzały się zarówno okresy dynamicznego rozwoju, jak i liczne problemy utrudniające funkcjonowanie nawet w elementarnych obszarach. Od wielu lat toczą się również dyskusje na temat sposobu zorganizowania policyjnego systemu fizycznej walki z terrorem i terroryzmem[10]. Jednak, zdaniem współczesnych komentatorów „od mniej więcej 3 lat, dzięki wysiłkom zarówno ludzi wywodzących się bezpośrednio z tych jednostek, jak i komendantów głównych policji oraz kolejnych kierownictw ministerstwa spraw wewnętrznych, pozwalających na wdrażanie właściwych działań, polski policyjny »antyterroryzm« (choć właściwsze byłoby tu określenie »kontrterroryzm«) wychodzi na prostą. Bez wielkiej przesady można powiedzieć, że w Polsce wreszcie powstają i są przyjmowane takie rozwiązania prawne i organizacyjne, które nie tylko odwracają dotychczasowe trendy traktowania policyjnych jednostek kontrterrorystycznych jako nielubianego »zła koniecznego«, z którym nie wiadomo co zrobić, ale nawiązują do najlepszych wzorców, a może nawet i je tworzą"[11]. Z zamieszczonym fragmentem, który reprezentuje pewien nurt adoracyjnego aplauzu wobec przyjmowanych rozwiązań, nie można zgodzić się ani odnośnie do okresu tzw. sensownych poczynań, ani z tezą o teraz dopiero powstających pomysłach na

[6] Tekst powstaje w grudniu 2018 r.

[7] W. Zubrzycki, *Kontrterroryzm po polsku* [w:] K. Jałoszyński, W. Zubrzycki, J. Jabłoński, *Kontrterroryzm. Siły specjalne, działania, wydarzenia w 2016 r.,* Szczytno 2017, s. 112.

[8] W. Zubrzycki, *How to improve physical combat with terrorism In the Republic of Poland? Selected Issues*, „Przegląd Policyjny" 2011, nr 2(102), s. 156.

[9] W. Zubrzycki, *Antyterrorystyczne formacje Policji w przypadku zbrojnej agresji na RP,* Szczytno 2014, s. 44.

[10] W. Zubrzycki, *Pododdziały antyterrorystyczne Policji,* Warszawa 2010, s. 5–6.

[11] R.M. Machnikowski, *Zmiany w policyjnym AT (analiza),* <https://www.infosecurity24.pl/zmiany-w-policyjnym-at-analiza>, dostęp: 2 grudnia 2018 r.

takie; polemizować wreszcie można z ostateczną jego konkluzją. Trudno powiedzieć, czy to poruszanie tematu na zapotrzebowanie, czy jego zaledwie pobieżna znajomość, czy może nieprecyzyjny przekaz spowodowały taki, a nie inny kształt prezentowanych tez. Posłużą one jednak za kanwę innej nieco narracji na ten sam temat.

Specyfika pododdziałów antyterrorystycznych polega m.in. na realizacji zadań odmiennych od tych, jakie stoją przed policjantami w toku codziennej służby. Wynikają one z sytuacji krytycznych, wymagających zastosowania środków ostatecznych. Odwrócone są m.in. proporcje pomiędzy czynnościami realizacyjnymi a przygotowaniem do nich, zaś trening pochłaniać powinien ok. 90 proc. aktywności pododdziału. Specyfiki tej często jednak nie rozumieją przełożeni, oczekując od tego typu formacji wzbogacania statystyk, z których sami są rozliczani. W praktyce oznacza to, że znikome wykorzystanie pododdziału antyterrorystycznego w powszechnych działaniach Policji, a także przeciągające się okresy spokoju i jego pozornej bezczynności powodują „uśpienie" zwierzchników i lekceważenie zagrożeń, przejawiające się w ubocznym traktowaniu potrzeb pododdziału, szukaniu oszczędności finansowych kosztem jego przygotowania do działań, a przez to znaczne obniżenie jego jakości. Traktując zatem występujące zagrożenia z należytą powagą, należy podkreślić, że system policyjnych działań antyterrorystycznych nie może być obiektem manipulacji i niekończących się zmian organizacyjnych, ponieważ wstrzymują one jego aktywność, ograniczają inicjatywy i podważają sens kontynuacji już rozpoczętych procesów. W opinii funkcjonariuszy wykonujących takie zadania, marnotrawienie czasu i energii na udowadnianie swojej przydatności i konieczności istnienia w określonej formie powoduje zaniedbywanie nałożonych obowiązków[12].

Kształtowanie dzisiejszego obrazu policyjnych działań kontrterrorystycznych było przez lata swoistą „drogą przez mękę", w trakcie której kolejne postaci, wywodzące się w prostej linii ze środowiska — dotąd — antyterrorystów, wykorzystywały niespożyte pokłady energii, aby wytłumaczyć decydentom sens własnego przekazu lub absurdalność pojawiających

[12] W. Zubrzycki, *Oddział antyterrorystyczny Policji w zwalczaniu terroryzmu*, Warszawa 2011 (seria: „Zeszyty Naukowe Akademii Obrony Narodowej"), s. 104–105.

się „z boku" pomysłów. Podkreślić trzeba zatem, że „droga" ta miała swój początek nie 3 lata, ale prawie dwie dekady temu, kiedy pododdziały antyterrorystyczne nie znały nawet eksponowanych dzisiaj bohaterów.

## 2.1. Działania kontrterrorystyczne w Polsce w aspekcie historycznym

Pierwsza w Polsce jednostka przeznaczona do realizacji zadań specjalnych została utworzona 28 lutego 1976 r. w byłej Komendzie Stołecznej MO jako Wydział Zabezpieczenia Stołecznego Urzędu Spraw Wewnętrznych[13]. W 1978 r. w strukturach wybranych oddziałów ZOMO (Zmotoryzowane Odwody Milicji Obywatelskiej) powstało dodatkowo siedem plutonów specjalnych[14], a w 1985 r. dwa kolejne[15]. W 1982 r. powołano również Pluton Specjalny Komisariatu Milicji MDL Okęcie jako niezależną komórkę przeznaczoną do ochrony portu lotniczego i przeciwdziałania — dość częstym wówczas — próbom uprowadzenia samolotów, podejmowanym z zamiarem ucieczki obywateli polskich na Zachód. Po przekształceniu Milicji Obywatelskiej w Policję, w 1990 r.[16], w miejsce plutonów specjalnych pojawiły się kompanie antyterrorystyczne, umieszczone w strukturach oddziałów prewencji Policji, a w miejsce Wydziału Zabezpieczenia powołano Wydział Antyterrorystyczny Komendy Stołecznej Policji[17]. W 2000 r. rozwiązano kompanie antyterrorystyczne i Wydział Antyterrorystyczny, powołując w ich miejsce samodzielne pododdziały antyterrorystyczne Policji (SPAP). Pluton Antyterrorystyczny Komisariatu Policji Warszawa Okęcie został wchłonięty przez Samodzielny Pododdział Antyterrorystyczny w Warszawie[18]. Do 2002 r. funkcjonowało w Polsce dziesięć samodzielnych pododdziałów antyterrorystycznych Policji, podległych odpowiednim komendantom wojewódzkim i komendantowi stołecznemu Policji[19]. W 2003 r. na bazie funkcjonujących dotychczas nieetatowych

[13] W. Zubrzycki, *Pododdziały…*, wyd. cyt., s. 7.
[14] W Gdańsku, Katowicach, Krakowie, Łodzi, Poznaniu, Szczecinie i Wrocławiu.
[15] W Rzeszowie i Białymstoku.
[16] Ustawa z 6 kwietnia 1990 r. o Policji, DzU z 1990 r., nr 30, poz. 179.
[17] W. Zubrzycki, *Pododdziały…*, wyd. cyt., s. 8–9.
[18] Tamże, s. 10.
[19] Tamże, s. 11.

form powstały sekcje antyterrorystyczne komend wojewódzkich w Bydgoszczy, Gorzowie Wielkopolskim, Kielcach, Lublinie, Olsztynie, Opolu oraz Radomiu[20]. Decyzją komendanta głównego Policji w 2017 r. zostały one, wraz z Wydziałem Realizacyjnym Komendy Stołecznej Policji, przekształcone w samodzielne pododdziały antyterrorystyczne, powiększając ich liczbę do siedemnastu.

We wrześniu 2002 r. na mocy decyzji komendanta głównego Policji rozpoczęto prace związane z tworzeniem nowego systemu funkcjonowania pododdziałów antyterrorystycznych Policji, z założeniem wyodrębnienia pododdziału centralnego. Na bazie Wydziału Antyterrorystycznego KSP 15 lutego 2003 r. powstały: Zarząd Bojowy i Zarząd Wsparcia Bojowego Centralnego Biura Śledczego[21], poszerzające zakres właściwości CBŚ o fizyczne zwalczanie terroryzmu[22]. Zadanie to zostało zdjęte 16 czerwca 2003 r.[23], kiedy do życia w Komendzie Głównej Policji powołane zostało Biuro Operacji Antyterrorystycznych[24] (BOA KGP)[25]. Po roku funkcjonowania BOA KGP 1 czerwca 2004 r. przekształciło się w Zarząd Operacji Antyterrorystycznych, wchodząc w skład Biura Główny Sztab Policji KGP[26]. Tym samym centralny pododdział antyterrorystyczny Policji pozbawiony został jednego ze swoich najistotniejszych atrybutów — samodzielności. Spowodowało to jego degradację, a zmiana struktury organizacyjnej wiązała się nie tylko ze zmianą podległości służbowej, lecz także

[20] Decyzja nr 28 komendanta głównego Policji z 6 lutego 2003 r. w sprawie powołania pododdziałów antyterrorystycznych Policji.

[21] Rozkaz organizacyjny nr 5/2003 komendanta głównego Policji z 30 stycznia 2003 r. w sprawie zmiany Etatu Centralnego Biura Śledczego KGP.

[22] Zarządzenie nr 5 komendanta głównego Policji z 30 stycznia 2003 r. zmieniające zarządzenie w sprawie powołania oraz określenia organizacji, zakresu działania i właściwości terytorialnej służby śledczej, Dz. Urz. KGP z 2003 r., nr 4, poz. 9.

[23] Zarządzenie nr 346 komendanta głównego Policji z 16 czerwca 2003 r. zmieniające zarządzenie w sprawie powołania oraz określenia organizacji, zakresu działania i właściwości terytorialnej służby śledczej, Dz. Urz. KGP z 2003 r., nr 12, poz. 62.

[24] Zarządzenie nr 345 komendanta głównego Policji z 16 czerwca 2003 r. zmieniające zarządzenie w sprawie regulaminu Komendy Głównej Policji, Dz. Urz. KGP z 2003 r., nr 12, poz. 61; rozkaz organizacyjny komendanta głównego Policji nr 19/03 z 3 czerwca 2003 r. w sprawie zmian w strukturze organizacyjnej Komendy Głównej Policji.

[25] W. Zubrzycki, *Pododdziały…*, wyd. cyt., s. 11.

[26] Rozkaz organizacyjny nr 15/04 komendanta głównego Policji w sprawie zmian organizacyjno-etatowych w Komendzie Głównej Policji (niepublik.).

z potrzebą tworzenia niemal od podstaw kolejnych systemów koordynacji i nadzoru[27]. Pozbawienie Biura Operacji Antyterrorystycznych autonomii pośrednio świadczyć może o lekceważeniu przez ówczesne kierownictwo Komendy Głównej Policji istniejących zagrożeń, na skutek sporadycznych „zaledwie" incydentów, a zadania związane z przygotowaniem do ewentualnych tylko działań traktowane były w sposób podrzędny, zdominowany przez realizację zadań dnia codziennego, związanych z wydarzeniami pospolitymi[28]. Biuro Operacji Antyterrorystycznych zajmowało się problematyką fizycznego zwalczania terroryzmu kompleksowo, począwszy od realizacji zadań bojowych, poprzez unifikację szkolenia wszystkich pododdziałów, aż po prace koncepcyjne. Niestety, rozwiązanie takie budziło wątpliwości zmieniającej się kadry kierowniczej Komendy Głównej Policji, zaś kolejne zmiany organizacyjne w komendzie sprawiły, że stało się ono idealnym celem niekorzystnej „reorganizacji". Spowodowało to zahamowanie lub uniemożliwienie kontynuacji rozpoczętych procesów, a przede wszystkim ostudzenie zapału policjantów, którzy weszli w jego skład, i stopniowe przenoszenie ich zainteresowania z poziomu jakości pododdziału na dbałość o własne korzyści[29].

Odchudzenie i ucywilnienie Komendy Głównej stanowiło priorytet kolejnych składów kierownictwa Policji, a negatywne tego skutki zawsze odczuwał centralny pododdział, jako komórka organizacyjna KGP. W takich właśnie okolicznościach rodziły się pomysły rozwiązań, które przynieść by mogły oczekiwaną stabilizację, leżały one także u podstaw rozpoczęcia prac koncepcyjnych dotyczących powołania odrębnej służby Policji.

Formuła centralnego pododdziału w formie samodzielnego biura powróciła w 2008 r.[30], zauważyć jednak należy, że jednym z założeń było wówczas uwolnienie etatów w Komendzie Głównej Policji[31]. Kolejna

[27] K. Jałoszyński, *Propozycja organizacji działań antyterrorystycznych Rzeczypospolitej Polskiej w obliczu współczesnego zagrożenia terroryzmem,* „Policja" 2005, nr 1, s. 50.

[28] W. Zubrzycki, *Oddział antyterrorystyczny…,* wyd. cyt., s. 104.

[29] Tamże, s. 103.

[30] Zarządzenie nr 372 komendanta głównego Policji z 14 kwietnia 2008 r. w sprawie regulaminu Komendy Głównej Policji, Dz. Urz. KGP z 2008 r., nr 8, poz. 47, § 4 ust. 1 pkt 2 lit. d.

[31] W 2003 r. BOA liczyło 193 etaty, w 2008 r. — 168.