75

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ BEZPIECZEŃSTWA NARODOWEGO

OCHRONA CYWILNO-WOJSKOWA MIAST POLSKICH W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH

II.1.5.1.0

Biblioteka Główna
Akademii Obrony Narodowej
S/7640
05-007640-003-0

WARSZAWA

74984

AKADEMIA OBRONY NARODOWEJ

WYDZIAŁ BEZPIECZEŃSTWA NARODOWEGO

Egz. Nr.....

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 74984
II
Akademii Obrony Narodowej

OCHRONA CYWILNO-WOJSKOWA MIAST POLSKICH W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH

II Etap badań

II.1.5.1.0

Kierownik naukowy

płk dr inż. Zbigniew SKWAREK

Nr ewid. 74984
II
Akademii Obrony Narodowej

WARSZAWA 2009

	1	2	3	A

4

Tytuł: **Ochrona cywilno-wojskowa miast polskich w warunkach zagrożeń terrorystycznych**

5	6	7
Rozpoczęto: 08.06.2009 Zakończono: 25.11.2009	Kart: 195	

8	9

ZESPÓŁ AUTORÓW:

Kierownik pracy: płk dr inż. Zbigniew **SKWAREK**: rozdział 1; rozdział 2 - podrozdział 2.1., 2.2.; rozdział 3 - podrozdział 3.1., 3.2., rozdział 4 - podrozdział 4.1.; rozdział 5.

Członkowie:

dr hab. inż. Andrzej **GLEN**: wstęp; rozdział 1, podrozdział 4.2., zakończenie.

dr inż. Roman **KWEĆKA**: podrozdział 2.3., podrozdział 3.3.

Recenzent: płk rez. dr hab. Józef MARCZAK

WSTĘP **5**

1. ZAŁOŻENIA BADAWCZE **8**

2. WYBRANE PODMIOTY PRZECIWDZIAŁANIA ZAGROŻENIOM TERRORYSTYCZNYM MIAST POLSKI **12**

2.1. Podmioty podległe Premierowi Rządu 19

2.2. Podmioty podległe MSWiA 25

2.3. Podmioty podległe MON 51

3. ANALIZA I OCENA ORAZ ZARZĄDZANIE RYZYKIEM W SYSTEMIE CYWILNO – WOJSKOWEJ OCHRONY MIAST POLSKICH W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH **76**

3.1. Analizy podatności na zagrożenia terrorystyczne w miastach polskich 76

3.2. Istota ryzyka w systemie cywilno – wojskowej ochrony miast polskich w warunkach zagrożeń terrorystycznych. 89

3.3. Cechy i zdolności sił przeznaczonych do zwalczania zjawiska terroryzmu w aglomeracjach miejskich 111

4. SPOSOBY PRZECIWDZIAŁANIA ZAGROŻENIOM TERRORYSTYCZNYM ... 128

4.1. Przeciwdziałanie zagrożeniom terrorystycznym założenia ogólne 131

4.2. Organizacja przeciwdziałania zagrożeniom lotnisk jako szczególnego elementu aglomeracji miejskiej. 134

5. KONCEPCJA SYSTEMU OCHRONY MIAST POLSKICH W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH **166**

ZAKOŃCZENIE **185**

BIBLIOGRAFIA **187**

WYKAZ TABEL **194**

WYKAZ RYSUNKÓW **195**

WSTĘP

Obecnie terroryzm stał się największym zagrożeniem dla bezpieczeństwa narodowego większości państw świata. Każde państwo musi mieć wdrożony system przeciwdziałania temu zjawisku, będący częścią narodowej strategii bezpieczeństwa. Nie inaczej rzecz ma się w przypadku Polski. Nasz kraj nie miał, na szczęście, okazji doświadczyć aktów terroryzmu, skierowanych wobec ludności polskiej na terytorium Polski. Natomiast za granicą, 28.09.2008 w północno-zachodnim Pakistanie grupa uzbrojonych mężczyzn porwała polskiego inżyniera, pracownika firmy naftowej Geofizyka Kraków Limited, która badał zasoby naturalne w Basal. Zastrzelili trzech towarzyszących mu Pakistańczyków, kierowcę oraz dwóch ochroniarzy. Do zdarzenia doszło w wiosce Pind Sultani, około 85 kilometrów od stolicy Pakistanu, Islamabadu. Kilkadziesiąt dni później Polaka zamordowano z zimną krwią.

Zaangażowanie Polski w walkę ze światowym terroryzmem w Afganistanie, ponoszone tam straty, prowadzone akcje odwetowe, jawne deklaracje polityczne o kontynuowaniu tej walki, pozwalają przypuszczać, że zjawisko terroryzmu może zaistnieć także na terytorium Polski. Pytanie zatem nie brzmi czy?, a raczej kiedy? i gdzie?, w jaki sposób?

Większość dotychczasowych ataków terrorystycznych realizowana była w miastach i kończyła się sukcesem terrorystów. Systemy antyterrorystyczne zwykle przygotowane były do przeciwstawiania się przeszłym akcjom terrorystycznym. Tymczasem terroryści nigdy nie powtarzali poprzednio stosowanych metod ataku, utrzymywali przewagę informacyjną.

Pytanie czy Polska lub jakikolwiek inny kraj na świecie posiada perfekcyjnie przygotowany, stuprocentowo skuteczny system walki z terroryzmem, jest pytaniem retorycznym. Kilkadziesiąt lat działań terrorystycznych pozwala uznać za generalizację historyczną tezę, że nie jest możliwe zbudowanie systemu walki z terroryzmem zdolnego przeciwstawiać się temu zjawisku w skali taktycznej, w warunkach entropii informacyjnej.

Stworzenie sprzyjających okoliczności do walki z terroryzmem zarówno w skali strategicznej, jak i taktycznej jest dosyć trudne, ponieważ aktualnie, rozwój cywilizacyjny świata sprawia, że dokonywanie zamachów terrorystycznych jest stosunkowo łatwe i politycznie opłacalne. Do głównych czynników, które umożliwiają działalność terrorystyczną, należy zaliczyć:

- szeroki dostęp do informacji,

- łatwość podróżowania,
- szybki i trudny do kontrolowania przepływ kapitału,
- duża liczba niebezpiecznych ładunków chemicznych w zakładach przemysłowych i przewożonych drogami publicznymi,
- zorganizowana przestępczość - organizacje o charakterze mafijnym są dostawcami broni, materiałów wybuchowych, substancji służących do produkcji broni masowego rażenia, fałszywych dokumentów itp.,
- handel narkotykami, który staje się podstawowym źródłem finansowania większości organizacji terrorystycznych.

Kluczem do wygrania walki z terroryzmem w skali strategiczne wydaje się usunięcie źródeł światowego terroryzmu, które niezmiennie pokrywają się z obszarami biedy i zacofania cywilizacyjnego na świecie. W skali taktycznej zwiększyć prawdopodobieństwo wygrania walki z terrorystami może lokalna przewaga informacyjna, przygotowany, zgrany, dobrze wyposażony system antyterrorystyczny i przygotowane obronnie, świadome zagrożeń, zdolne do poświęceń społeczeństwo.

Przygotowanie struktur państwa na ewentualność wystąpienia ataku terrorystycznego powinno mieć kompleksowy, systemowy charakter. System taki powinien przede wszystkim działać w granicach i na podstawie celowo przygotowanych aktów prawnych. Integrować wewnętrznie i koordynować zewnętrznie niezbędne podmioty państwowe i pozapaństwowe. Przedmiotowy system należy ukierunkować na ochronę polskich miast, ponieważ poza nimi trudno odnaleźć opłacalne obiekty uderzeń dla terrorystów. W systemie takim istotne wyznacznik sprawności jego działania stanowiło będzie akceptowalne w systemie ryzyko, wyznaczające pośrednio właściwy, adekwatny do zagrożeń poziom reakcji systemu.

Niniejsze opracowanie jest wynikiem realizacji drugiego etapu badań problemu naukowo – badawczego, ujętego w programie prac naukowo – badawczych AON na rok 2008 pod kryptonimem MUR. Zgodnie z „planem" realizacji problemu i zadaniem naukowym, głównym (końcowym) celem badań było *opracowanie koncepcji* ochrony *cywilno – wojskowej miast polskich w warunkach zagrożeń terrorystycznych.*

Badania i opracowanie ich wyników zostały podzielone na dwa etapy: 2008r. – pierwszy etap, 2009 r. – drugi etap. Dla całości prac i dla każdego etapów opracowano szczegółowe założenia badawcze. W odniesieniu do etapu drugiego zostały one ujęte w rozdziale pierwszym niniejszego opracowania. W rozdziale tym scharak-

teryzowano także sposób ujęcia problemu i treści pozostałych rozdziałów opracowania.

1. ZAŁOŻENIA BADAWCZE

W świetle obiektywnych i subiektywnych czynników mających wpływ na stan ochrony miast w warunkach zagrożeń terrorystycznych, główny problem badawczy, wynikający z celu badań, sformułowano w postaci pytania: **Jakimi siłami i w jaki sposób realizowana jest cywilno – wojskowa ochrona miast polskich przed zagrożeniami terrorystycznymi?**

Rozwiązanie głównego problemu badawczego i osiągnięcie założonego celu pierwszego etapu badań wiązało się z uzyskaniem odpowiedzi na następujące problemy szczegółowe:

Jaki jest charakter współczesnych zagrożeń terrorystycznych w polskich miastach w pierwszej połowie XXI w.?

1) Jakimi cechami charakteryzują się duże aglomeracje miejskie, jako obiekty potencjalnych ataków terrorystycznych?
2) Jakie dla aglomeracji miejskich, a przede wszystkim obiektów infrastruktury krytycznej (porty lotnicze) mogą być generowane powietrzne zagrożenia terrorystyczne?
3) Jakie są aktualnie rozwiązania prawne dotyczące przeciwdziałania zagrożeniom terrorystycznym?

Główny problem badawczy w niniejszej części pracy sformułowano w postaci pytania: **Do czego zmierzający, przy pomocy jakich środków i technologii działania cywilno-wojskowy system antyterrorystyczny zapewni możliwie najpełniejszą ochronę miast polskich przed atakami terrorystycznymi?**

Na tak postawione pytanie odpowiedzi udzielono przez rozwiązanie następujących problemów szczegółowych:

1. **Jakie militarne i niemilitarne podmioty państwa powinny przeciwstawić się zagrożeniom terrorystycznym miast polskich?**
2. **Jak zarządzać ryzykiem w systemie cywilno-wojskowej ochrony miast polskich w warunkach zagrożeń terrorystycznych?**
3. **Jakie metody, sposoby przeciwdziałania podejmowane w systemie cywilno-wojskowym uchronią elementy infrastruktury krytycznej miast polskich przed atakiem terrorystycznym lub zminimalizują jego skutki?**
4. **Jaka koncepcja systemu ochrony miast polskich zapewni sprawne jego działania w warunkach zagrożeń terrorystycznych?**

Przed przystąpieniem do prac badawczych założono, że opracowanie koncepcji cywilno – wojskowej obrony miast polskich przed zagrożeniem terrorystycznym wymagało przede wszystkim będzie zdefiniowania trzech podstawowych obszarów:

1.) Jaki jest główny cel i jaki ma być stan końcowy, co chcemy osiągnąć postępując na podstawie przyjętej taktyki działania (ends):

- ochrona i obrona obywateli oraz ich własności,
- wykrywanie i neutralizowanie planowanych operacji terrorystycznych,
- ograniczenie skali zjawiska do poziomu, w którym stanie się on odizolowanym i sporadycznym incydentem przestępczym bez międzynarodowych powiązań,
- zidentyfikowanie i wyeliminowanie korzeni terroryzmu,
- zniszczenie istniejących grup terrorystycznych i ideologii, na której bazują.

2.) Określenie sposobów osiągnięcia założonego celu *(ways)* – m.in. poprzez:

- diagnozę podmiotów odpowiedzialnych za ochronę miast w warunkach zagrożeń terrorystycznych,
- ze względu na dynamikę „rozwoju" zagrożenia – bieżące identyfikowanie zasobów i środków, niezbędnych do przeciwstawienia się tym zagrożeniom oraz podejmowanie działań zmierzających do ich eliminacji,
- ocenę wystarczalności narzędzi (mechanizmów), pozostających do dyspozycji instytucji (służb) zaangażowanych i w zależności od wyników wyposażanie ich w brakujące instrumenty,
- ocenę skuteczności podejmowanych działań służących sprzeciwianiu się ideologii ugrupowań terrorystycznych i udzielaniu wsparcia terrorystom, a także zapobiegających szerzeniu się radykalizacji postaw wśród obywateli,
- wypracowanie zasad współdziałania w ochronie miast,

3.) Określenie posiadanych i koniecznych środków do osiągnięcia celu *(means)* uwzględniając elementy narodowej siły w zakresie walki z terroryzmem:

- narodowe jednostki i centra wyznaczone do walki z terroryzmem,
- wsparcie wojskowe - jednostki militarne (jednostki wyznaczone do operacji specjalnych poza granicami kraju oraz wsparcia działań na terenie Polski),
- jednostki policyjne i inne wyznaczone do egzekwowania prawa w zakresie przeciwdziałania terroryzmowi i ścigania sprawców ataków terrorystycznych,
- siły pozamilitarne,
- potencjał (siły) przeznaczony do ochrony (VIP, bezpieczeństwo w ruchu lotniczym, ochrona infrastruktury, itp.),

W celu rozwiązania postawionych problemów i osiągnięcia celu badań zastosowano następujące metody badawcze:

- analizy, ze względu na złożoność problematyki uwarunkowań i funkcjonowania cywilno-wojskowego systemu ochrony miast polskich przed zagrożeniem terrorystycznym;
- syntezy, gdyż problemy rozwiązywane były przez dedukcję, ta zaś wymagać będzie zarówno analizy, jak i syntezy, szczególnie podczas redukcji i porównania uzyskanych wyników badawczych ze stanem istniejącym w rzeczywistości;
- wnioskowania indukcyjnego z wykorzystaniem kanonów Milla, szczególnie kanonów jedynej różnicy i zmian towarzyszących;
- abstrahowania, w szczególności metodą wyłączania cech, która pozwoliła skupić uwagę jedynie na interesujących nas właściwościach przedmiotu badań.

W badaniach zastosowano klasyczny i powszechnie stosowany w naukach empirycznych, w tym w naukach wojskowych, indukcyjno-hipotetyczno-dedukcyjno-redukcyjny układ czynności procesu badawczego. Na początku procesu badań rzeczywistość spełniła w badaniach funkcję motoryczną, dostarczyła faktów, które pozyskane metodami naukowymi stały się faktami naukowymi. Pozwoliły one sprecyzować, w zderzeniu ze stanem teorii, sytuację problemową badań. Następnie tworzono na drodze indukcyjnych uogólnień hipotezy robocze. W kolejnym etapie stosując na przemian indukcję enumeracyjna niezupełną i dedukcję, głownie w formie dowodzenia probabilistycznego zwiększano prawdopodobieństwo słuszności hipotez do momentu, kiedy można je było uznać za hipotezy naukowe, to znaczy za hipotezy wystarczająco uzasadnione. O słuszności uzyskanych wyników badań upewniano się, wykorzystując funkcję kryterialną, jaką spełnia rzeczywistość podczas weryfikacji hipotezy naukowej.

Rezultaty przeprowadzonych badań dotyczące problemów badawczych etapu drugiego, opracowano pisarsko i zamieszczono w pięciu rozdziałach, które opatrzono wstępem i zakończeniem, uzupełniono wykazem bibliografii, tabel i rysunków.

We **wstępie** wprowadzono czytelnika w ogólną sytuacje problemową. W **rozdziale pierwszym** zawarto założenia badawcze pracy: cel całej pracy, problemy rozwiązywane w jej pierwszym etapie, a także te, którym poświęcono niniejszą pracę. Ponadto w rozdziale tym wyjaśniono przyjęte założenia, zastosowane metody ba-

dawcze oraz wprowadzono czytelnika w układ pracy. Z kolei **rozdział drugi** poświęcono charakterystyce podstawowych niemilitarnych i militarnych podmiotów angażowanych w walkę z terroryzmem. Natomiast w **rozdziale trzecim** zamieszczono opis badań zagadnień ryzyka, analizy i oceny zagrożeń terrorystycznych. **Rozdział czwarty** zawiera charakterystykę sposobów przeciwdziałania zagrożeniom terrorystycznym, także tym podejmowanym na lotnisku, jako jednym z najbardziej charakterystycznych obiektów potencjalnego ataku terrorystycznego w mieście. Wreszcie **rozdział piąty**, wynikowy poświęcono opisowi koncepcji systemu ochrony miast polskich w warunkach zagrożeń terrorystycznych. W zakończeniu zawarto refleksję odnoszącą się do całości pracy, oceniono poziom osiągnięcia jej celu oraz wskazano kierunek dalszych badań.

W ustaleniu racjonalnych rozwiązań kierowano się argumentami zdobywanymi na drodze sprawdzania i wyjaśniania, mozolnie gromadzonymi w trakcie badań. Wyniki tychże, przedstawiono w niniejszym opracowaniu.

2. WYBRANE PODMIOTY PRZECIWDZIAŁANIA ZAGROŻENIOM TERRORYSTYCZNYM MIAST POLSKI

Ochrona cywilno – wojskowa miast polskich w warunkach zagrożeń terrorystycznych nie powinna kojarzyć się jedynie z fizyczną eliminacją terrorystów przy udziale jednostek antyterrorystycznych, lecz zgodnie z koncepcją systemową powinniśmy uwzględnić zasadnicze aspekty działań wchodzących w jej skład. Ochrona cywilno – wojskowa obejmuje zatem rozpoznanie, zapobieganie, zwalczanie oraz likwidację skutków. Za każdy z tych aspektów odpowiadają inne służby. Nie bez znaczenia jest więc wielopoziomowa koordynacja ich działań.

Rozpoznanie zagrożeń terrorystycznych polega na monitorowaniu działalności jednostek oraz grup, mogących zastosować metody terrorystyczne w celu osiągnięcia jakiegoś działania o podłożu politycznym. Głównymi instytucjami lecz nie jedynymi, odpowiedzialnymi za rozpoznanie zagrożenia terroryzmem w Polsce są: Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu (w kontekście zagrożenia zewnętrznego) oraz Służba Wywiadu i Kontrwywiadu Wojskowego. Ustawa z dnia 24 maja 2002 roku o utworzeniu Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu szczegółowo określiła zakres ich kompetencji. W ustawie możemy przeczytać między innymi, że w gestii Agencja Bezpieczeństwa Wewnętrznego leży[1]: rozpoznawanie, zapobieganie i wykrywanie przestępstw, szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i innych przestępstw godzących w bezpieczeństwo państwa.

ABW nie spełnia zadań wyłącznie informacyjnych – posiada kompetencje śledcze, dzięki czemu to jej przekazywane są wszelkie zadania związane z rozpoznaniem na terenie kraju zagrożenia terroryzmem. Wewnątrz ABW znajduje się Departament Przeciwdziałania Korupcji, Terroryzmowi i Przestępczości Zorganizowanej.

Drugim, niezmiernie ważnym składnikiem systemu rozpoznania jest Agencja Wywiadu, w jej kompetencjach leży między innymi: Rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej[2]. AW zajmuje się więc przede wszystkim rozpoznaniem zagrożeń znajdu-

---

[1] „Dziennik Ustaw" nr 74 z 2002 r., poz. 676.
[2] Tamże

jących się poza terytorium naszego kraju, monitorując działalność zagranicznych organizacji terrorystycznych.

Służba Wywiadu Wojskowego (SWW) jest służbą specjalną, właściwą w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej SZ RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej.

SWW powstała z dniem 1 października 2006 r. i działa na podstawie Ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego.

SWW jest członkiem międzynarodowej wspólnoty wywiadowczej. Aktywnie uczestniczy w wymianie informacji i doświadczeń pomiędzy wiodącymi służbami wywiadowczymi państw NATO i UE, przyczyniając się jednocześnie do budowania bezpieczeństwa w wymiarze międzynarodowym.

Ustawą z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego i Służbie Wywiadu Wojskowego (Dz.U. Nr 104, poz.709 z późn. zm.) utworzono z dniem 1 października 2006 r. **Służbę Kontrwywiadu Wojskowego**, będącą urzędem administracji rządowej, podległą – na podstawie art. 5 ust. 1a ustawy o urzędzie Ministra Obrony Narodowej (Dz.U. z 1996 r., Nr 10, poz. 56 z późn. zm.) - Ministrowi Obrony Narodowej.

Służba Kontrwywiadu Wojskowego jest służbą specjalną i służbą ochrony państwa, właściwą w sprawach ochrony przed zagrożeniami wewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej Sił Zbrojnych Rzeczypospolitej Polskiej oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej.

Szef Służby Kontrwywiadu Wojskowego jest centralnym organem administracji rządowej i podlega Ministrowi Obrony Narodowej, z zastrzeżeniem uprawnień Prezesa Rady Ministrów lub Ministra Koordynatora Służb Specjalnych, w przypadku jego powołania. Działalność Szefa SKW podlega kontroli Sejmu.

Kompetencje SWW i SKW w kwestii zwalczania terroryzmu dotyczą zwalczania przestępstw, podlegających orzecznictwu sądów wojskowych. W ustawie zapisano, że zadania SWW i SKW polegają między innymi na rozpoznawaniu, zapobieganiu i wykrywaniu przestępstw terroryzmu. SWW i SKW są także odpowiedzialne za działania w rejonach konfliktów i rozpoznawanie tam zagrożeń dla bezpieczeństwa państwowego, między innymi terrorystycznych. Na tej płaszczyźnie wymagana jest

bliska współpraca z Agencją Wywiadu, co wymaga koordynacji poczynań tych służb specjalnych.

Z powodu wielu pokrywających się zadań ABW, AW oraz SWW i SKW (wcześniej WSI) konieczne było szczegółowe rozdzielnie ich kompetencji oraz określenie zasad, zakresu i trybu współdziałania pomiędzy tymi instytucjami. W tym celu 12 września 2003 roku zostało wydane, na mocy delegacji ustaw o ABW i AW oraz o WSI, Zarządzenie nr 79 Prezesa Rady Ministrów[3].

W ramach Kolegium do Spraw Służb Specjalnych został powołany, na wniosek szefa ABW Zespół ds. Koordynacji Działań Operacyjno-Rozpoznawczych w Zakresie Zwalczania Terroryzmu Politycznego[4]. W skład tego zespołu wchodzą przedstawiciele AW, SWW i SKW, Policji, Straży Granicznej, Służby Celnej i Generalnego Inspektoratu Informacji Finansowej. Zespół jest strukturą o charakterze mobilnym, a jego spotkania zwoływane są stosunkowo często. W ramach pracy tego zespołu udało się m.in. skoordynować w skali całego kraju działania wszystkich struktur operacyjno-rozpoznawczych na kierunku antyterrorystycznym[5].

Innymi elementami systemu rozpoznawczego są placówki monitorujące skażenia (radiologiczne, chemiczne, anomalie biologiczne, mogące być wynikiem aktu terroryzmu). Jednakże odgrywają one mniejszą rolę w systemie, zważywszy na mniejszy stopień zagrożenia atakami terrorystycznymi z użyciem broni masowej zagłady[6].

Zapobieganie aktom terrorystycznym polega na niedopuszczeniu jednostek bądź grup do użycia metod terrorystycznych. Zapobieganie nie może istnieć bez rozpoznania, gdyż jedynie rozpoznanie konkretnego zagrożenia może prowadzić do jego identyfikacji i podjęcia odpowiednich środków bezpieczeństwa, mających na celu nie dopuszczenie do tego zagrożenia. W ramach zapobiegania mieszczą się także działania prewencyjne. W zakresie zapobiegania należy wyróżnić działania instytucji państwowych oraz organizacji pozapaństwowych. Wśród instytucji państwowych poza omówionymi wyżej służbami specjalnymi (ABW, AW, SWW, SKW), możemy wyróżnić przede wszystkim Policję, Straż Graniczną oraz Biuro Ochrony Rządu. Z kolei

---

[3] „Monitor Polski" nr 44 z 2003 r., poz. 656.

[4] Por. Zagrożenie atakami terrorystycznymi w Polsce jest niskie, 15 września 2004, http://www.mswia.gov.pl/aktual_150904_raport.html.

[5] Agencja Bezpieczeństwa Wewnętrznego rok po reformie (lipiec 2003), http://www.abw.gov.pl/Raporty/raport_02.htm.

[6] Por. B. M. Jenkins, The Likelihood of Nuclear Terrorism, RAND Corporation P-7119, Santa Monica, lipiec 1986, s. 6, także B. Hoffman, Oblicza terroryzmu, Warszawa 2001, s. 190, oraz B. Bolechów, Terroryzm w świecie podwubiegunowym, Toruń 2002, s. 501-509.

pozapaństwowe to przede wszystkim różnego rodzaju agencje ochrony oraz służby wewnętrzne bezpośrednio zapobiegające przed dokonaniem aktu terroryzmu.

Działania zapobiegawcze Policji polegają na zapewnieniu ogólnego bezpieczeństwa, poprzez zapobieganie dokonywaniu przestępstw, a do takich należy zaliczyć działania metodami terrorystycznymi (szczegółowe kompetencje Policji reguluje Ustawa o Policji z 6 kwietnia 1990 r. z późniejszymi zmianami[7]. Policja może więc być użyta na podstawie informacji operacyjnych, pochodzących od służb specjalnych, w celu niedopuszczenia do dokonania aktu terrorystycznego, oczywiście o ile okoliczności tego wymagają (np. wymaga tego nieprecyzyjność informacji operacyjnych, na podstawie których nie zawsze można zidentyfikować zagrożenie).

Zadania Straży Granicznej polegają przede wszystkim na kontroli granic w celu zapobiegnięcia przedostaniu się osób podejrzanych o działalność terrorystyczną, natomiast Biuro Ochrony Rządu, jest organem odpowiedzialnym za bezpieczeństwo osób, wykonujących ważne funkcje publiczne, ale także polskich placówek dyplomatycznych oraz obiektów i urządzeń o szczególnym znaczeniu.

W zakresie zapobiegania bardzo ważną rolę w systemie przeciwdziałania terroryzmowi w Polsce odgrywa sformowane w 2002 roku Międzyresortowe Centrum do spraw Zwalczania Przestępczości Zorganizowanej i Międzynarodowego Terroryzmu, które działa przy MSWiA. Powołane zostało na mocy niepublikowanego Zarządzenia nr 54 Prezesa Rady Ministrów z dnia 30 kwietnia 2002 roku. Jest ono podstawową instytucją koordynującą działania antyterrorystyczne w zakresie operacyjnym.

W skład Centrum wchodzą: Szef Centrum, którym jest Minister Spraw Wewnętrznych i Administracji, Zastępcy Szefa Centrum, którymi są Ministrowie Finansów i Obrony Narodowej, Sekretarz Centrum – powoływany przez Prezesa Rady Ministrów na wniosek Szefa Centrum, członkowie: Komendant Główny Policji, Komendant Główny Straży Granicznej, Szef ABW, Szef WSI, Komendant Główny Żandarmerii Wojskowej, Generalny Inspektor Kontroli Skarbowej, Generalny Inspektor Informacji Finansowej oraz Generalny Inspektor Celny (obecnie Departament Kontroli Celnej i Biuro Dokumentacji Skarbowej Ministerstwa Finansów).

Głównymi zadaniami Centrum w dziedzinie zapobiegania terroryzmowi są: monitorowanie aktów terroryzmu, dokonywanie ich analiz i ocen oraz przedstawianie opinii i wniosków; projektowanie kierunków przedsięwzięć przeciwdziałających aktom

---

[7] „Dziennik Ustaw" nr 7 z 2002 r., poz.58.

terroryzmu; organizowanie operacji przy wykorzystaniu obiektów służbowych, środków transportu oraz posiadanych możliwości operacyjnych.

W Centrum tworzone są także zespoły zadaniowe, zajmujące się ważnymi zagadnieniami związanymi z kompleksowym funkcjonowaniem oraz koordynacją systemu przeciwdziałania terroryzmowi w Polsce (dla przykładu: zespół do spraw bioterroryzmu, czy też zespół do spraw opracowania podstaw formalnych i organizacyjno-strukturalnych funkcjonowania Krajowego Koordynatora do Spraw Przeciwdziałania Terroryzmowi). Zadania Centrum nie ograniczają się do zapobiegania aktom terroryzmu – jego główna funkcja polega na koordynacji i podejmowaniu odpowiednich do sytuacji środków (w przyszłości odpowiedzialnym za to ma być Krajowy Koordynator ds. Przeciwdziałania Terroryzmowi). Centrum zapewnia także organizację współpracy zagranicznej z organami innych państw w zakresie likwidacji aktów terroryzmu poprzez przeprowadzanie wspólnych operacji. Centrum może inicjować prace legislacyjne, zmierzające do usprawnienia systemu zwalczania przestępczości (w tym terroryzmu)[8].

W czerwcu 2005 roku w Departamencie Bezpieczeństwa i Porządku Publicznego Ministerstwa Spraw Wewnętrznych i Administracji powstał Wydział ds. Terroryzmu. Jego głównymi zadaniami są właśnie analiza informacji związanych z terroryzmem i koordynacja funkcjonowania elementów systemu przeciwdziałania terroryzmowi w Polsce podległych MSWiA.

Działalność Wydziału ds. Terroryzmu polega głównie na analizach przeprowadzanych dla Ministra Spraw Wewnętrznych i Administracji dotyczących całokształtu zagadnienia terroryzmu, ale także na koordynacji funkcjonowania elementów systemu przeciwdziałania terroryzmowi w służbach jemu podległych. Ważnym zadaniem Wydziału jest także organizowanie współpracy zagranicznej związanej ze zwalczaniem terroryzmu. Tu przykładem może być współpraca w ramach polsko-amerykańskiej grupy roboczej do spraw zwalczania terroryzmu.

Wydział prowadzi analizy dotyczące tego, co się dzieje na świecie, nowych rozwiązań prawnych, nowych metod i technik zwalczania terroryzmu oraz technologicznych rozwiązań. Wyciąganie z tego wniosków, które następnie są przekazywane Ministrowi daje z całą pewnością podstawy, aby sądzić, że przygotowanie Polski na zamach terrorystyczny jest coraz lepsze.

---

[8] Zarządzenie nr 54 Prezesa Rady Ministrów z dnia 30 kwietnia 2002, niepublikowane

Wydział udziela także wsparcia merytorycznego instytucjom podległym MSWiA.

Konieczność istnienia komórki organizacyjnej w MSWiA zajmującej się problemem terroryzmu podyktowana jest złożonością tego problemu. Ministerstwo nie zajmuje się bowiem stroną typowo praktyczną – do zadań operacyjnych służą wyspecjalizowane służby, nad większością których MSWiA sprawuje nadzór.

Zwalczanie zagrożeń terrorystycznych polega na likwidacji jednostek, lub też grup, stosujących metody terrorystyczne. Zwalczanie, podobnie jak zapobieganie, ściśle łączy się z rozpoznaniem, jednakże w przeciwieństwie do zapobiegania przy zwalczaniu musi dojść do aktu terroryzmu. W polskim systemie przeciwdziałania terroryzmowi jest wiele środków, które mogą być podjęte w celu zwalczania terroryzmu.

Poza środkami typowo siłowymi (fizycznym zwalczaniem) są także środki formalno-prawne, które mogą być użyte na przykład w kwestii zwalczania finansowania terroryzmu[9]. Zwalczanie aktów terroryzmu determinowane jest przez rodzaj tych ataków. W ramach zwalczania należy także zawrzeć wszystkie działania, zmierzające do schwytania i osądzenia sprawców tych aktów.

W Polsce głównymi służbami odpowiedzialnymi bezpośrednio za zwalczanie aktów terroryzmu są: Policja (w tym pododdziały antyterrorystyczne, w kwestii bezpośredniego zwalczania siłowego – fizycznej eliminacji), Agencja Bezpieczeństwa Wewnętrznego, Agencja Wywiadu, SKW i SWW, specjalne jednostki wojskowe (poza granicami kraju, lub też po wprowadzeniu adekwatnego stanu nadzwyczajnego) oraz Siły Powietrzne RP (w gestii obrony granicy lotniczej) oraz Straż Graniczna (kwestia ochrony granicy państwowej), Służba Celna i Generalny Inspektorat Informacji Finansowej.

W Komendzie Głównej Policji powołano Biuro Operacji Antyterrorystycznych, które zajmuje się fizyczną likwidacją zagrożeń związanych z terroryzmem (ale głównym jego zadaniem jest walka z terrorem kryminalnym).

Gdyby doszło do aktu terroryzmu na terenie kraju śledztwo przekazane zostałoby ABW, gdyż to w jej właściwościach leży prowadzenie tego typu spraw, bowiem ABW została wyposażona w uprawnienia śledcze. Jednakże akty terroryzmu na obywatelach i obiektach (jak: budynki, statki morskie i powietrzne) polskich mogą być dokonywane poza granicami naszego kraju, gdzie Policja oraz ABW nie mają takich

---

[9] Por. Konwencja w sprawie zwalczania finansowania terroryzmu, podpisana 9 grudnia 1999 roku w Nowym Jorku, ratyfikowana przez Polskę ustawą z dnia 9 stycznia 2003 r.

uprawnień jak na terenie kraju. Za zwalczanie aktów terroryzmu za granicami odpowiadają więc AW oraz SKW i SWW (w gestiach określonych wspomnianymi wyżej ustawami, regulującymi działanie tych służb). Trzeba też zaznaczyć, że poza granicami Polski fizyczne zwalczanie terroryzmu leży w kompetencjach wojskowych jednostek specjalnych. W przypadku, gdyby terroryści chcieli użyć do ataku samolotu, bądź śmigłowca, zgodnie z zapisami nowelizacji z dnia 2 lipca 2003 roku do ustawy o ochronie granicy państwowej z dnia 12 października 1990 roku, Minister Obrony może podjąć decyzję o zestrzeleniu przechwyconego statku powietrznego – fizyczna eliminacja leży w kompetencjach Sił Powietrznych RP[10].

Likwidacja skutków aktu terrorystycznego polega na zarządzaniu akcją ratunkową i zabezpieczeniu przed atakiem wtórnym (fizyczna likwidacja skutków). Zarządzanie kryzysowe odbywa się na wszystkich szczeblach administracji rządowej i samorządowej. Centra Zarządzania Kryzysowego przygotowują także scenariusze potencjalnych ataków terrorystycznych, włącznie z wewnętrznymi procedurami likwidacji skutków takiego działania. Ponadto w chwili kryzysu, wywołanego aktem terroryzmu, zazwyczaj zostaje powołany sztab antykryzysowy. Sztaby są organami politycznymi, chociaż w ich skład mogą wchodzić także specjaliści z konkretnych dziedzin. To właśnie w sztabach antykryzysowych podejmowane są najważniejsze decyzje polityczne w kwestii działań, zmierzających do likwidacji skutków ataku.

Czy Polska jest przygotowana na atak terrorystyczny? To pytanie pozostanie bez odpowiedzi do czasu, kiedy dojdzie do takiego ataku. Faktem jest, że działania w kierunku jak najlepszego przygotowania się na takie zdarzenie są intensywnie prowadzone. Nie zmienia to jednak faktu, że nadal są pewne dziury w tym systemie.

Przykładem może być chociażby kwestia użycia wojsk na terenie kraju, bez wprowadzenia stanu nadzwyczajnego, czy też brak jednolitego systemu łączności.

Terroryzm jest zjawiskiem dynamicznym i zaskoczyć może nawet najlepiej przygotowane służby (czego dowodami mogą być chociażby ataki w Izraelu oraz USA), dlatego też gdy dojdzie do ataku terrorystycznego należy być odpowiednio przygotowanym na wszystkie ewentualności związane z jego wystąpieniem.

Omawiając system przeciwterrorystyczny istniejący w Polsce, konieczne jest wskazanie podmiotów odpowiedzialnych za bezpieczeństwo wewnętrzne kraju. Art. 146 ust 4 pkt 7 Konstytucji RP[11] mówi o tym, że w zakresie i na zasadach określo-

---

[10] Dziennik Ustaw" nr 172 z 2004 r., poz. 1805.
[11] Konstytucji RP z dnia 2 kwietnia 1997 roku – (Dz. U. Nr 78 z 1997 r., poz. 483).

nych w Konstytucji i ustawach Rada Ministrów w szczególności: zapewnia bezpieczeństwo wewnętrzne państwa oraz porządek publiczny. Następnie, zgodnie z art. 29 ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. nr 141, z 1997 r., poz. 943) kwestie ochrony bezpieczeństwa i porządku publicznego, jak również przeciwdziałanie skutkom klęsk żywiołowych i innych podobnych zdarzeń zagrażających bezpieczeństwu powszechnemu są w gestii działu spraw wewnętrznych. Minister odpowiedzialny za sprawy wewnętrzne sprawuje w tej kwestii nadzór nad działalnością Biura Ochrony Rządu, Policji, Straży Granicznej, Państwowej Straży Pożarnej, Obrony Cywilnej Kraju, Prezesa Urzędu ds. Repatriacji i Cudzoziemców, oraz Krajowego Centrum Informacji Kryminalnej[12]. Natomiast osobą właściwą do nadzorowanie pracy wszystkich służb specjalnych RP na polu walki z terroryzmem jest Minister - członek Rady Ministrów, Koordynator do spraw Służb Specjalnych.

2.1. Podmioty podległe Premierowi Rządu

2.1.1. Agencja Bezpieczeństwa Wewnętrznego i Agencja Wywiadu

Agencja Bezpieczeństwa Wewnętrznego ma na celu ochronę bezpieczeństwa wewnętrznego państwa oraz jego porządku konstytucyjnego, natomiast za bezpieczeństwo zewnętrzne państwa odpowiedzialna jest Agencja Wywiadu. Szef Agencji Bezpieczeństwa Wewnętrznego i Szef Agencji Wywiadu są centralnymi organami administracji rządowej, działającymi odpowiednio przy pomocy Agencji Bezpieczeństwa Wewnętrznego i Agencji Wywiadu, będącymi urzędami administracji rządowej.

Do zadań Agencji Bezpieczeństwa Wewnętrznego należy:

- 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;
- rozpoznawanie, zapobieganie i wykrywanie przestępstw oraz ściganie ich sprawców, m. in.: szpiegostwa, terroryzmu, naruszenia tajemnicy państwowej i

---

[12] Za: D. Góralski, K. Liedel, System przeciwdziałania terroryzmowi w Polsce, (w:) pod red. K. Liedela, J. Marszałek-Kawa., Sz. Wudarski, Polityczne metody zwalczania terroryzmu, Toruń 2006 r., s. 130.

innych przestępstw godzących w bezpieczeństwo państwa; godzących w podstawy ekonomiczne państwa; korupcji osób pełniących funkcje publiczne; w zakresie produkcji i obrotu towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa; nielegalnego wytwarzania, posiadania i obrotu bronią, amunicją i materiałami wybuchowymi, bronią masowej zagłady oraz środkami odurzającymi i substancjami psychotropowymi, w obrocie międzynarodowym;

- realizowanie w granicach swojej właściwości, zadań służby ochrony państwa oraz wykonywanie funkcji krajowej władzy bezpieczeństwa w zakresie ochrony informacji niejawnych w stosunkach międzynarodowych;
- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla ochrony bezpieczeństwa wewnętrznego państwa i jego porządku konstytucyjnego;
- podejmowanie innych działań określonych w odrębnych ustawach i umowach międzynarodowych;
- działania w celu ograniczenia dostępu do pewnych kategorii informacji i objęcia ich specjalnym systemem bezpieczeństwa, aby zapewnić ochronę podstawowych interesów Rzeczypospolitej Polskiej, w zakresie bezpieczeństwa osobowego, przemysłowego, teleinformatycznego, monitorowania importu[13].

Agencja Wywiadu realizuje zadania poza granicami kraju, jej działalność na terytorium RP może być prowadzona tylko w ograniczonym zakresie - wyłącznie w związku z jej zagraniczną działalnością. Do obowiązków Agencji Wywiadu należy:

- uzyskiwanie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla bezpieczeństwa i międzynarodowej pozycji RP oraz jej potencjału ekonomicznego i obronnego;
- rozpoznawanie i przeciwdziałanie zagrożeniom zewnętrznym godzącym w bezpieczeństwo, obronność, niepodległość i nienaruszalność terytorium RP;
- ochrona zagranicznych przedstawicielstw RP i ich pracowników przed działaniami obcych służb specjalnych i innymi działaniami mogącymi przynieść szkodę interesom RP; - zapewnienie ochrony kryptograficznej łączności z polskimi placówkami dyplomatycznymi i konsularnymi oraz poczty kurierskiej;

---

[13] www.abw.gov.pl, z dnia 01.03.2008r.

- rozpoznawanie międzynarodowego terroryzmu, ekstremizmu oraz międzynarodowych grup przestępczości zorganizowanej;
- rozpoznawanie międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi, środkami odurzającymi i substancjami psychotropowymi oraz towarami, technologiami usługowymi o znaczeniu strategicznym dla bezpieczeństwa, a także rozpoznawanie międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z rozprzestrzenianiem tej broni oraz środków jej przenoszenia;
- rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na bezpieczeństwo państwa oraz podejmowanie działań mających na celu eliminowanie tych zagrożeń; - prowadzenie wywiadu elektronicznego;
- podejmowanie innych działań określonych w odrębnych ustawach, umowach międzynarodowych[14].

2.1.2. Ministerstwo Sprawiedliwości

Ministerstwo Sprawiedliwości (organy: sąd, prokuratura). Ma obowiązek sądzić za dokonywanie przestępstw o charakterze terrorystycznym[15] zawartych w aktualnym (marzec 2007) kodeksie karnym pośrednio m.in. w: art. 18, art. 19, art. 109-114, art. 120, art. 121, art. 127-128, art. 134-136, art. 140, art. 148, art. 156, art. 160, art. 163, art. 165-167, art. 172, art. 173, art. 183, art. 191, art. 252, art. 269, art. 299 – (są to przestępstwa posiadające znamiona w większym lub mniejszym stopniu poszczególnych przestępstw terrorystycznych)[16]; bezpośrednio w: art. 65 § 1, art. 115 § 20 - (spiritus movens powstania tego art. była Decyzja Ramowa Rady UE z dnia 13 czerwca 2002 r. o zwalczaniu terroryzmu - 2002/475/JHA), art. 258 § 2.

---

[14] Ustawa z dnia 24 maja 2002r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. z 2002r., nr 74, poz. 676

[15] Zgodnie z art. 115 § 20 kk. 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 lub 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.

[16] Polska wobec terroryzmu, Instytut Studiów Strategicznych, Zeszyt nr 49, Kraków 2002 r., s. 96-101, Por. M. Filar, Terroryzm w polskim prawie karnym na tle prawa międzynarodowego i porównawczego, (w:) pod. red. R.Bäcker, Od Blokad ulicznych do World Trade Center, Toruń 2002 r., s. 19-29.

Istotne są również istniejące w polskim prawie przepisy prewencyjne np. wobec cudzoziemca prowadzącego działalność, którą można uznać za propagowanie terroryzmu, istnieje możliwość nieprzedłużenia mu zezwolenia na pobyt w Polsce[17]. Kolejnymi nowymi i skutecznymi narzędziami w walce z międzynarodowym terroryzmem są, obowiązujące na terenie UE: Europejski Nakaz Aresztowania, który Polska jako kraj członkowski inkorporowała do narodowego systemu prawnego i honoruje od 1 maja 2004 r. – (kodeks postępowania karnego, art. 607a – 607zc.), Wspólne Zespoły Śledcze – (kodeks postępowania karnego art. 589b – 589f) oraz przepisy w sprawie zatrzymania dowodów lub zabezpieczenia mienia – (kodeks postępowania karnego art. 62a i 62 b);

Generalny Inspektor Informacji Finansowej – (GIF)[18] posiada umocowanie prawne w Ustawie o przeciwdziałaniu wprowadzaniu do obrotu finansowego wartości majątkowych pochodzących z nielegalnych lub nieujawnionych źródeł oraz przeciwdziałaniu finansowania terroryzmu z dnia 16 listopada 2000 roku. Instytucja ta nie posiada specjalnej grupy ds. rozpoznawania źródeł finansowania terroryzmu. Wykonywać to zadanie może jednak każdy pracownik GIF w zależności od potrzeb i nakazów ABW oraz Policji[19].

Międzyresortowy Zespół do Spraw Zagrożeń Terrorystycznych - powołany do życia z dniem 25 października 2006 r., winien zapewniać współdziałanie administracji rządowej w zakresie rozpoznawania, przeciwdziałania i zwalczania terroryzmu. zadań Zespołu należy. W tym celu Zespól wykonuje następujące zadania:

- monitorowanie zagrożeń o charakterze terrorystycznym, ich analiza i ocena, a także prezentowanie opinii oraz wniosków dla członków rządu;
- sporządzanie projektów standardów i procedur w zakresie zwalczania terroryzmu, przed wszystkim standardów oceny występowania zagrożenia oraz określania jego poziomu;
- inicjowanie, koordynowanie i monitorowanie działań podejmowanych przez odpowiednie organy administracji państwowej, w szczególności na polu

---

[17] Przepis ten zastosowano dotychczas raz wobec pełniącego obowiązki wielkopolskiego immama, obywatela Jemenu Ahmeda Ammara, wydalonego z Polski 01.06.2004 r. przez wojewodę wielkopolskiego, po przedstawieniu przez ABW opinii, że jego dalszy pobyt w Polsce zagraża bezpieczeństwu państwa.

[18] Podlega pod Ministra Finansów.

[19] K. Liedel, Podmioty systemowego przeciwdziałania terroryzmowi, w: http://liedel.pl/terroryzm.20.04.2007 r.,

wykorzystania informacji oraz rozpoznawania, przeciwdziałania i zwalczania terroryzmu;

- występowanie z wnioskiem do właściwych ministrów w celu podjęcia kroków prawnych zmierzających do usprawnienia metod i form zwalczania terroryzmu;
- organizowanie kooperacji z innymi państwami w zakresie zwalczania terroryzmu oraz koordynacja wymiany danych oraz organizowanych wspólnych operacji;
- inicjowanie szkoleń i konferencji dotyczących sposobów zwalczania terroryzmu.

W skład gremium wchodzą: przewodniczący Minister SWiA, zastępcy przewodniczącego – Minister Finansów, Minister Obrony Narodowej i Minister Spraw Zagranicznych oraz minister-członek Rady Ministrów - Koordynator Służb Specjalnych, sekretarz Zespołu – osoba wyznaczona przez przewodniczącego, członkowie: sekretarz lub podsekretarz stany wskazany przez Ministra SWiA, Szef Obrony Cywilnej Kraju, Szef ABW, Szef AW, Szef BOR, Komendant Główny Policji, Straży Granicznej, Państwowej Straży Pożarnej i Żandarmerii Wojskowej, Szef Służby Wywiadu Wojskowego, Szef Służby Kontrwywiadu Wojskowego, Generalny Inspektor Kontroli Skarbowej, Generalny Inspektor Informacji Finansowej oraz Szef Służby Celnej.

W Międzyresortowym Zespole do Spraw Zagrożeń Terrorystycznych funkcjonują powoływane przez Ministra SWiA zespoły zadaniowe, zajmujące się realizowanie zadań przypisanych temu gremium (np. na mocy Decyzją nr 2 przewodniczącego Zespołu z dnia 8 grudnia 2006 r. powołana została Stała Grupa Ekspercka, w skład której wchodzą przedstawiciele podmiotów będących członkami Międzyresortowego Zespołu do Spraw Zagrożeń Terrorystycznych). W celu dalszego uszczegółowienia i pogłębienia kwestii powiązanych z aktywnością na polu przeciwdziałania terroryzmowi, powołuje się podzespoły, które odpowiadają za realizację zadań związanych z konkretnymi wyzwaniami w dziedzinie ochrony bezpieczeństwa państwa w kontekście przeciwdziałania terroryzmowi[20].

§ Kolegium do Spraw Służb Specjalnych - Kolegium funkcjonuje w oparciu o rozdział 2 tj. art. art. 11-13 ustawy z dnia 24 maja 2002 r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu (Dziennik Urzędowy z 2002 r. nr 74, poz. 676

---

[20] w http://liedel.pl/terroryzm.20.04.2007 r.

z późn. zm.). Kwestie organizacyjne reguluje Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 roku. Do priorytetowych zadań Kolegium należy przygotowywanie ocen lub wyrażanie opinii w takich kwestiach jak: kierunki i plany działania służb specjalnych - (w tym ich nadzór i koordynowanie działań), projekty aktów normatywnych i innych dokumentów rządowych dotyczących działalności służb specjalnych[21].

W skład Kolegium wchodzą[22]:

1) przewodniczący - Prezes Rady Ministrów,

2) sekretarz Kolegium,

3) członkowie:

a) minister właściwy do spraw wewnętrznych,

b) minister właściwy do spraw zagranicznych,

c) Minister Obrony Narodowej,

d) minister właściwy do spraw finansów publicznych,

e) Szef Biura Bezpieczeństwa Narodowego,

4) minister-członek Rady Ministrów właściwy do spraw koordynowania działalności służb specjalnych, jeśli został wyznaczony przez Prezesa Rady Ministrów.

W posiedzeniach Kolegium uczestniczą także:

Szef ABW,

Szef AW,

Szef Centralnego Biura Antykorupcyjnego,

Szef Służby Kontrwywiadu Wojskowego,

Szef Służby Wywiadu Wojskowego,

Przewodniczący Sejmowej Komisji do Spraw Służb Specjalnych.

Prezydent Rzeczypospolitej Polskiej może delegować swojego przedstawiciela do udziału w posiedzeniach Kolegium, spełniającego wymagania określone w przepisach o ochronie informacji niejawnych w zakresie dostępu do informacji stanowiących tajemnicę państwową, oznaczonych klauzulą "ściśle tajne".

Przewodniczący Kolegium może zapraszać do udziału w posiedzeniach Kolegium przewodniczących właściwych komisji sejmowych, przedstawicieli organów państwowych oraz inne osoby, których uczestnictwo jest niezbędne ze względu na tematykę obrad.

---

[21] Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 r.Dz.U.02.103.929

[22] http://bip.abw.gov.pl/palm/bip/19/18/Kolegium_ds_sluzb_specjalnych.html

2.2. Podmioty podległe MSWiA

2.2.1. Biuro Ochrony Rządu

Jedną z ważniejszych organizacji, wykonującą zadania z zakresu ochrony osób, obiektów i urządzeń jest Biuro Ochrony Rządu. Jest to jednolita, umundurowana, uzbrojona formacja do zadań, której należy ochrona:

- Prezydenta RP;
- Marszałka Sejmu;
- Marszałka Senatu;
- Prezesa Rady Ministrów;
- wiceprezesa Rady Ministrów;
- ministra właściwego do spraw wewnętrznych oraz ministra właściwego do spraw zagranicznych;
- innych osób ze względu na dobro państwa;
- byłych prezydentów RP na podstawie Ustawy z dnia 30 maja 1996r. *o uposażeniu byłego Prezydenta RP*;
- delegacji danych państw przebywających na terytorium RP;
- polskich przedstawicielstw dyplomatycznych, urzędów konsularnych oraz przedstawicielstw przy organizacjach międzynarodowych poza granicami RP;
- obiektów i urządzeń o szczególnym znaczeniu;
- prowadzenie rozpoznania pirotechniczno – radiologicznego obiektów Sejmu i Senatu; - obiektów służących Prezydentowi RP, Prezesowi Rady Ministrów, ministrowi właściwemu do spraw wewnętrznych oraz ministrowi właściwemu do spraw zagranicznych.

Szef Biura Ochrony Rządu zapewnia sprawne oraz efektywne wykonywanie zadań tej formacji, poprzez:

- organizowanie ochrony;
- prowadzenie polityki kadrowej;
- opracowanie, wykonanie programu szkolenia funkcjonariuszy i doskonalenia zawodowego pracowników, zapewnienie im właściwych warunków i trybu szkolenia;
- współdziałanie z centralnymi organami administracji rządowej podległymi ministrowi właściwemu do spraw wewnętrznych, jednostkami organizacyjnymi podporządkowanymi, podległymi, nadzorowanymi przez ministra właściwego do spraw

wewnętrznych lub ministra obrony narodowej, a także innymi organami administracji rządowej i samorządu terytorialnego w zakresie zadań realizowanych przez Biuro Ochrony Rządu i te organy.

W celu zapewnienia ochrony Biuro Ochrony Rządu:

- planuje zabezpieczenia osób, obiektów i urządzeń;
- rozpoznaje, analizuje zagrożenia oraz zapobiega ich powstawaniu, koordynuje realizowane działania ochronne;
- wykonuje bezpośrednią ochronę;
- zabezpiecza obiekty i urządzenia;
- doskonali metody pracy.

Biuro Ochrony Rządu wykonuje również czynności administracyjno – porządkowe oraz podejmuje działania profilaktyczne. W zakresie koniecznym do wykonywania zadań może korzystać z pomocy i informacji uzyskanych przez: Policję, Agencję Bezpieczeństwa Wewnętrznego, Straż Graniczną oraz Żandarmerię Wojskową[23].

Podczas wykonywania zadania funkcjonariusz ma prawo:

- wydawać polecenia osobom, których zachowanie może stworzyć zagrożenie dla bezpieczeństwa osób, obiektów i urządzeń podlegających ochronie Biurze Ochrony Rządu;
- legitymować osoby w celu ustalenia ich tożsamości;
- zatrzymywać osoby stwarzające bezpośrednie zagrożenie dla życia lub zdrowia ludzkiego oraz dla mienia, a także osoby naruszające porządek publiczny;
- dokonywać kontroli osobistej, przeglądać zawartość bagaży, sprawdzać ładunki i pomieszczenia w celu zapewnienia bezpieczeństwa ochranianych osób, obiektów i urządzeń;
- żądać pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz jednostek gospodarczych prowadzących działalność w zakresie użyteczności publicznej, zwracać się o pomoc do innych jednostek gospodarczych i organizacji społecznych.

Podczas czynności służbowych funkcjonariusz jest obowiązany do poszanowania godności ludzkiej oraz przestrzegania i ochrony praw człowieka. Może stosować środki przymusu bezpośredniego, odpowiadające potrzebom wynikającym z istniejącej sytuacji i niezbędne do osiągania podporządkowania się wydanym polece-

---

[23] Ustawa z dnia 16 marca 2001r. o Biurze Ochrony Rządu, Dz. U. z 2004r., nr 163, poz. 1712

niom. Są to fizyczne, techniczne, chemiczne środki służące do obezwładnienia lub konwojowania osób oraz do zatrzymywania pojazdów; pałki i psy służbowe. Funkcjonariusz ma prawo użycia broni palnej, jednak powinno to następować w sposób wyrządzający najmniejszą szkodę osobie, przeciwko której użyto broni, nie może zmierzać do pozbawienia jej życia, jak również narażać na niebezpieczeństwo utraty życia, zdrowia innych osób.

Biuro Ochrony Rządu zapobiega popełnianiu przestępstw wobec osób ochranianych; ujawnia osoby i zdarzenia, rozpoznaje miejsca i zjawiska, które mogą mieć związek z bezpieczeństwem osób ochranianych oraz bezpieczeństwem obiektów i urządzeń objętych ochroną; współdziała z Policją, z Agencją Bezpieczeństwa Wewnętrznego, Żandarmerią Wojskową, Strażą Graniczną oraz Państwową Strażą Pożarną w zakresie uzyskiwania informacji o zagrożeniach dla osób, obiektów i urządzeń chronionych; utrzymuje kontakty z osobami, których pomoc może okazać się bardzo przydatna.

Biuro Ochrony Rządu prowadzi działania poprzez: gromadzenie i przetwarzanie informacji wpływających na realizację zadań; planowanie i systematyczne kontrolowanie obiektów i urządzeń objętych ochroną, w celu zapewnienia bezpiecznej realizacji zadań; korzystanie z informacji i danych, przechowywanych w zbiorach ewidencji kryminalnej i zbiorach archiwalnych, dla wyeliminowania zagrożenia dla osób, obiektów i urządzeń ochranianych. Biuro Ochrony Rządu może prowadzić przetwarzanie danych osobowych bez wiedzy i zgody, której one dotyczą, jeśli służy to realizacji zadań. Może również korzystać z pomocy osób niebędących funkcjonariuszami, ale tylko w szczególnie uzasadnionych przypadkach. Ujawnianie danych o osobach udzielających pomocy Biurze Ochrony Rządu jest zabronione[24].

2.2.2. Policja

Zasadnicza rola w walce z terroryzmem spoczywa na Policji i Straży Granicznej, zaś na Państwowej Straży Pożarnej jedynie w zakresie zwalczania skutków ewentualnego ataku terrorystycznego.

---

[24] www.bor.gov.pl, z dnia 01.03.2008r.

Zgodnie z ustawą z dnia 6 kwietnia 1990 roku, art. 1 ust. 1 Policja to formacja umundurowana i uzbrojona powołana do zapewnienia bezpieczeństwa i porządku publicznego, służąca społeczeństwu[25].

Zadania, do jakich przewidziano Policję, określono w art. 1, ust. 2, jako[26]:

1. ochrona życia i zdrowia ludzi oraz mienia przed bezprawnymi zamachami naruszającymi te dobro;
2. ochrona bezpieczeństwa i porządku publicznego, w tym zapewnienie spokoju w miejscach publicznych oraz środkach publicznego transportu i komunikacji publicznej, w ruchu drogowym i na wodach przeznaczonych do powszechnego korzystania;
3. inicjowanie i organizowanie działań mających na celu zapobieganie popełnianiu przestępstw i wykroczeń oraz zjawisk kryminogennych i współdziałanie w tym zakresie z organami samorządowymi i organizacjami społecznymi;
4. wykrywanie przestępstw i wykroczeń oraz ściganie ich sprawców;
5. nadzór nad strażami miejskimi tworzonymi na podstawie ustawy oraz nad specjalistycznymi uzbrojonymi formacjami ochronnymi w zakresie określonym odrębnymi przepisami;
6. kontrola przestrzegania przepisów porządkowych i administracyjnych związanych z działalnością publiczną lub obowiązujących w miejscach publicznych;
7. współdziałanie z policjami innych państw oraz ich organizacjami międzynarodowymi na podstawie umów i porozumień międzynarodowych oraz odrębnych przepisów;
8. gromadzenie, przetwarzanie i przekazywanie informacji kryminalnych;
9. prowadzenie bazy danych zawierających informacje o wynikach analizy kwasu dezoksyrybonukleinowego (DNA).

Policja - mimo że w ustawie nie zawarto bezpośredniego i dosłownego zadania zwalczania terroryzmu, może to czynić dzięki nowym właściwym zapisom z kodeksu karnego (art. 115 § 20) określających przestępstwo terrorystyczne. Polska Policja bierze czynny udział w kilku stałych inicjatywach współpracy w sferze rozpoznania i zwalczania terroryzmu z: Interpolem, Europolem, Grupą Roboczą ds. terroryzmu III filaru Unii Europejskiej - (TWG), Europejską Policyjną Grupą Roboczą ds. Zwalczania Terroryzmu – (PWGT). W Komendzie Głównej Policji funkcjonuje Biuro Ope-

---

[25] Ustawa o Policji z dnia 6 kwietnia 1990 roku (tj. Dz. U. Nr 7, poz. 58 z późn. zm.)
[26] Art. 2 Ustawy o Policji z dnia 6 kwietnia 1990 roku (tj. Dz. U. Nr 7, poz. 58 z późn. zm.)

racji Antyterrorystycznych – (BOA), zajmujące się fizyczną likwidacją zagrożeń związanych z terroryzmem;

Jedną z form działania Policji, której celem jest między innymi zwalczanie terroryzmu, działalności wywrotowej przeciwko instytucją państwa czy groźnej przestępczości zorganizowanej, jest praca niejawna, powszechnie określana jako praca operacyjna. Dotyczy ona działań ukierunkowanych na wykrywanie i zatrzymywanie przestępców w drodze uzyskiwania informacji od pozyskiwanych agentów (tzw. osobowych źródeł informacji), będących członkami organizacji przestępczych.

Policja w swych strukturach posiada wyodrębnione ustawowo pododdziały antyterrorystyczne, które należy rozumieć jako jedną z odpowiedzi Policji na groźbę ataku terrorystycznego w naszym kraju.

Pododdziały antyterrorystyczne powołano w celu zapobiegania i fizycznego zwalczania aktów terrorystycznych, zwłaszcza w postaci wybuchu i zagrożenia wybuchu, zawładnięcia środkami komunikacji powietrznej, wodnej lub lądowej, zamachu na osobę lub uprowadzenia osoby, bądź też opanowania obiektu stałego lub zamachu na ważne urządzenia czy instalację. Ponadto w razie potrzeby pododdziały antyterrorystyczne wykonują także zadania przewidziane dla oddziałów prewencji[27]. Zakres zadań został zmodyfikowany z chwilą wejścia w życie Zarządzenia Nr 25 Komendanta Głównego Policji i określone zostały w § 35 tego aktu[28].

Do zakresu działań samodzielnego pododdziału antyterrorystycznego Policji (SPAP) należy:

- fizyczne zwalczanie terroryzmu poprzez prowadzenie działań rozpoznawczych oraz bojowych przy użyciu taktyki antyterrorystycznej, zmierzających do likwidowania zamachów terrorystycznych, a także przeciwdziałania zdarzeniom o takim charakterze;
- prowadzenie działań minersko-pirotechnicznych;
- wykonywanie innych działań niż określone w pkt 1 i 2, wymagających użycia specjalistycznych sił i środków będących na wyposażeniu pododdziału lub konieczności stosowania specjalnej taktyki działania.

---

[27] C. Gołota, Struktura organizacyjna i zadania Policji polskiej, [in] Policja polska wobec przestępczości zorganizowanej, Szczytno 1994, s. 39.

[28] Zarządzenie Nr 25 Komendanta Głównego Policji z dnia 31 grudnia 2002 r. w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji (Dz. Urz. KGP z 2003 r. Nr 2, poz. 4, zmiany: Dz. Urz. Z 2003 r. Nr 22, poz. 127 i z 2004 r. Nr 10, poz. 44).

Pierwszy pododdział antyterrorystyczny w Polsce utworzono w 1976 roku na mocy Decyzji Ministra Spraw Wewnętrznych(MSW)[29]. Jednostkę utworzono na podstawie wzorców fińskich[30]. Rok wcześniej delegacja polskiego MSW była z wizytą w Finlandii, gdzie jej zaprezentowana jednostka antyterrorystyczna *Niedźwiedź*. Główną przesłanką, która zdecydowała o powstaniu pododdziału była fala ataków terrorystycznych, jaka przeszła przez kraje europejskie. Ministerstwo Spraw Wewnętrznych nie mogło przejść obojętnie obok tych wydarzeń. Wyciągnięto wnioski, że również Polska może stać się miejscem ataku terrorystów, postanowiono utworzyć milicyjną jednostkę specjalną[31].

Tworzenie nowego pododdziału podzielono na trzy etapy[32].

W pierwszym etapie Wydział Kadr Komendy Stołecznej Milicji Obywatelskiej wytypował funkcjonariuszy, którzy spełniali określone kryteria[33]:

Wstępna selekcja wyłoniła 300 kandydatów, których poddano drugiemu etapowi weryfikacji – sprawdzianowi wydolności fizycznej i strzeleckiej.

Trzeci etap, do którego przebrnęło 100 funkcjonariuszy, polegał na przeprowadzeniu kandydatami rozmów kwalifikacyjnych, po której wybrano 47 pierwszych, którzy stali się trzonem oddziału.

Tworzenie tego typu formacji podporządkowane było następującemu schematowi: określenie celu, zadań, metod szkolenia, taktyki działania, i na tej podstawie środków walki, w jakie powinien być wyposażony pododdział antyterrorystyczny[34](rys.1), by efektywnie realizować swoje zadania.

---

[29] Decyzja Ministra Spraw Wewnętrznych z dnia 28 lutego 1976 r. w sprawie utworzenia Wydziału Zabezpieczenia Komendy Stołecznej Milicji Obywatelskiej do zwalczania aktów przemocy.

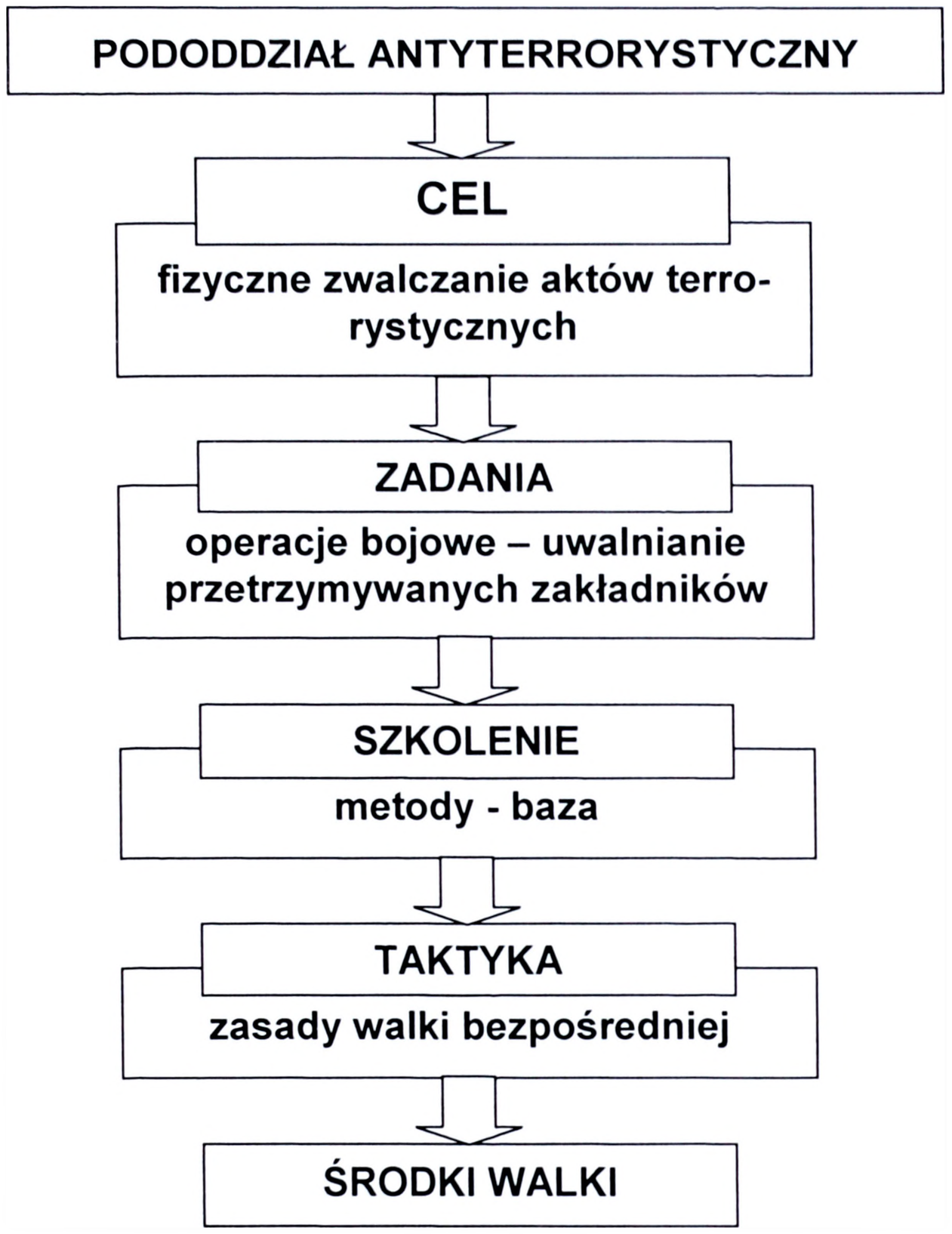
[30] K. Jałoszyński, Krajowe pododdziały antyterrorystyczne – historia i dzień dzisiejszy, „Policja" 2000, Nr 1-2, s. 98.

[31] K. Jałoszyński, op. cit., s. 49.

[32] J. Pawlik, M. Żywczyk, Organizacja i przeznaczenie pododdziałów specjalnych MO, Warszawa 1985, s. 5.

[33] K. Jałoszyński, op. cit., s. 49.

[34] K. Jałoszyński, op. cit., s. 150.



Rys. 1. Schemat tworzenia pododdziału antyterrorystycznego (Źródło: K. Jałoszyński, Koncepcja współczesnych działań antyterrorystycznych, Rozprawa habilitacyjna „Zeszyty Naukowe AON" 2003, dodatek, s. 151).

Po 1990 roku w nazwach jednostek specjalnych wykonujących zadania w zakresie zwalczania terroryzmu pojawiło się oficjalne określenie antyterrorystyczne. Zmiany ustrojowe spowodowały wówczas głębokie przeobrażenia w polskich organach bezpieczeństwa publicznego. W miejsce MO powołano Policję[35], Wydział Zabezpieczenia zmienił nazwę na Wydział Antyterrorystyczny Komendy Stołecznej Policji, a lokalne plutony specjalne przemianowano na Kompanie Antyterrorystyczne, zwiększając ich stan osobowy do 50 funkcjonariuszy. Nowością w zmianach jakie dotknęły jednostki specjalne Policji było powołanie, w każdej z nich sekcji pirotechnicznych, których zadaniem było rozbrajanie niekonwencjonalnych ładunków wybuchowych. Przy Komisariacie Policji Portu Lotniczego Warszawa – Okęcie utworzono

[35] Ustawa o Policji z dnia 6 kwietnia 1990 roku (tj. Dz. U. Nr 7, poz. 58 z późn. zm.)

pluton antyterrorystyczny do prewencyjnego, antyterrorystycznego zabezpieczenia portu lotniczego. Wszystkie te zmiany wprowadzone zostały zarządzeniem Komendanta Głównego Policji[36]. Przepis cedujący walkę z terroryzmem na Milicje Obywatelską został uchylony[37].

Od 2000 roku wszystkie etatowe pododdziały antyterrorystyczne w kraju będące w strukturach Policji nosiły nazwę: *Samodzielnych Pododdziałów Antyterrorystycznych* (SPAT)[38]. Pluton Antyterrorystyczny Komisariatu Policji Warszawa – Okęcie od tego roku jest integralną częścią pododdziały warszawskiego[39].

Decyzją nr 296 Komendant Główny Policji[40] w grudniu 2000 roku utworzył na bazie już istniejących *Samodzielnych Pododdziałów Antyterrorystycznych* (SPAT), *Samodzielne Pododdziały Antyterrorystyczne Policji* (SPAP) w Warszawie, Białymstoku, Gdańsku, Katowicach, Krakowie, Łodzi, Poznaniu, Rzeszowie, Szczecinie i Wrocławiu. Decyzja ta określa również ich liczebność, zasadę podległości oraz zasięg terytorialny działania. W ten sposób została określona nowa struktura organizacyjna SPAP w Polsce (rys. 2).

---

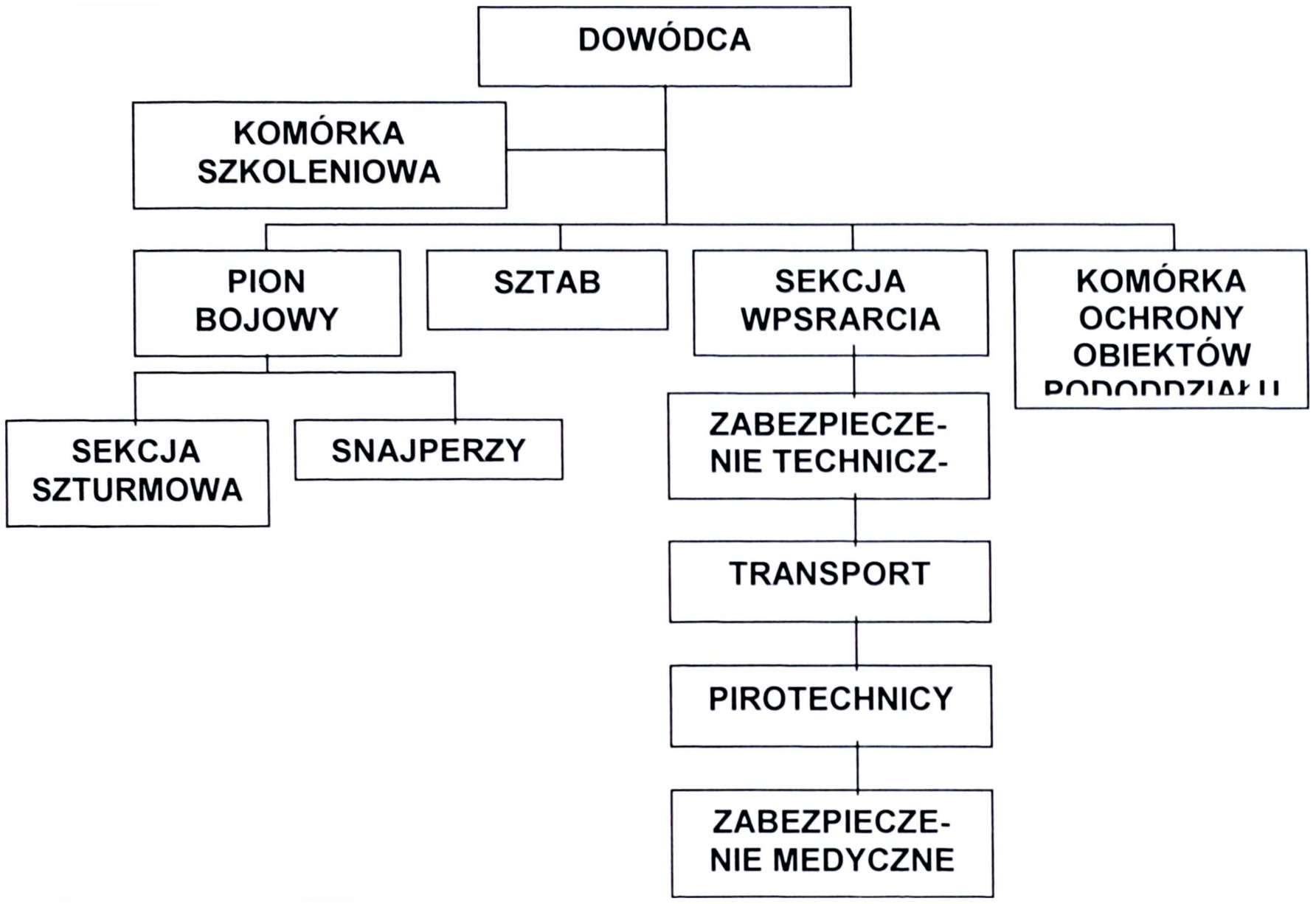
[36] Zarządzenie Komendanta Głównego Policji Nr 6/90 z dnia 3 sierpnia 1990 r. w sprawie organizacji oddziałów prewencji i pododdziałów antyterrorystycznych Policji.

[37] Zarządzenie Ministra Spraw Wewnętrznych Nr 067/90 z dnia 3 lipca 1990 r. w sprawie uchylenia niektórych tajnych i tajnych specjalnego znaczenia aktów normatywnych obowiązujących w resorcie spraw wewnętrznych.

[38] Zarządzenie Komendanta Głównego Policji Nr 14/00 z dnia 18 października 2000 r. zmieniające zarządzenie w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji.

[39] K. Jałoszyński, op. cit., s. 42.

[40] Decyzja Nr 296 Komendanta Głównego Policji z dnia 29 grudnia 2000 r. w sprawie powołania pododdziałów antyterrorystycznych Policji.



Rys. 2. Organizacja pododdziału antyterrorystycznego (Źródło: K. Jałoszyński, Pododdziały antyterrorystyczne – uzbrojenie i wyposażenie, Warszawa 2001, s. 14).

W 2001 roku Komendant Główny Policji wydał zarządzenie określające zadania pododdziału antyterrorystycznego: zwalczanie zamachów terrorystycznych mających na celu uzyskanie efektu zastraszenia i polegające w szczególności na[41]:

- dokonaniu lub groźbą dokonania zamachu bombowego;
- uprowadzeniu pojazdów lądowych;
- uprowadzeniu statków wodnych, powietrznych lub innych środków transportu;
- porwaniu osób lub osoby;
- dokonaniu lub groźbą dokonania zabójstwa;
- dokonaniu lub groźbą dokonania podpalenia;
- braniu zakładników.

[41] K. Jałoszyński, op. cit., s. 169.

Zarządzenie nakładało obowiązek na komendantów wojewódzkich Policji wyznaczenia dowódcy akcji lub operacji w wypadku zaistnienia aktu mającego cechy aktu terrorystycznego. Określa czynności, jakie powinien wykonać dowódca (zastępca dowódcy) pododdziału antyterrorystycznego przed podjęciem działań bojowych, daje uprawnienia dowódcy pododdziału do wykorzystania uzbrojenia i wyposażenia specjalistycznego podczas prowadzonych akcji lub operacji. Stwierdza się w nim: *policjanci pododdziału antyterrorystycznego podczas działań antyterrorystycznych, wykorzystują uzbrojenie, umundurowanie i wyposażenie, w zależności od potrzeb wynikających z konkretnego zadania*[42].

W 2002 roku Komenda Główna Policji podjęła czynności organizacyjno-prawne zmierzające do utworzenia w polskiej policji centralnego oddziału antyterrorystycznego[43] w drodze przekształcenia strukturalno-etatowego warszawskiego SPAP[44]. Efektem podjętych działań jest przeniesienie w miesiącu lutym 2003 roku ze struktur Komendy Stołecznej Policji do Struktur Komendy Głównej Policji w formie dwóch Zarządów: *Bojowego i Wsparcia Bojowego Centralnego Biura Śledczego KGP*. Z uwagi na wysoki poziom wyszkolenia i wyposażenia pododdziału, przejmuje on zadania przeznaczone dla jednostki centralnej, obejmującej swym zasięgiem cały kraj i wykorzystywanej do sytuacji kryzysowych o szerokim zasięgu.

Sekcja minersko-pirotechniczna pozostaje w KSP, a pluton z lotniska Okęcie przekazano z powrotem do Komisariatu Policji Warszawa – Okęcie.

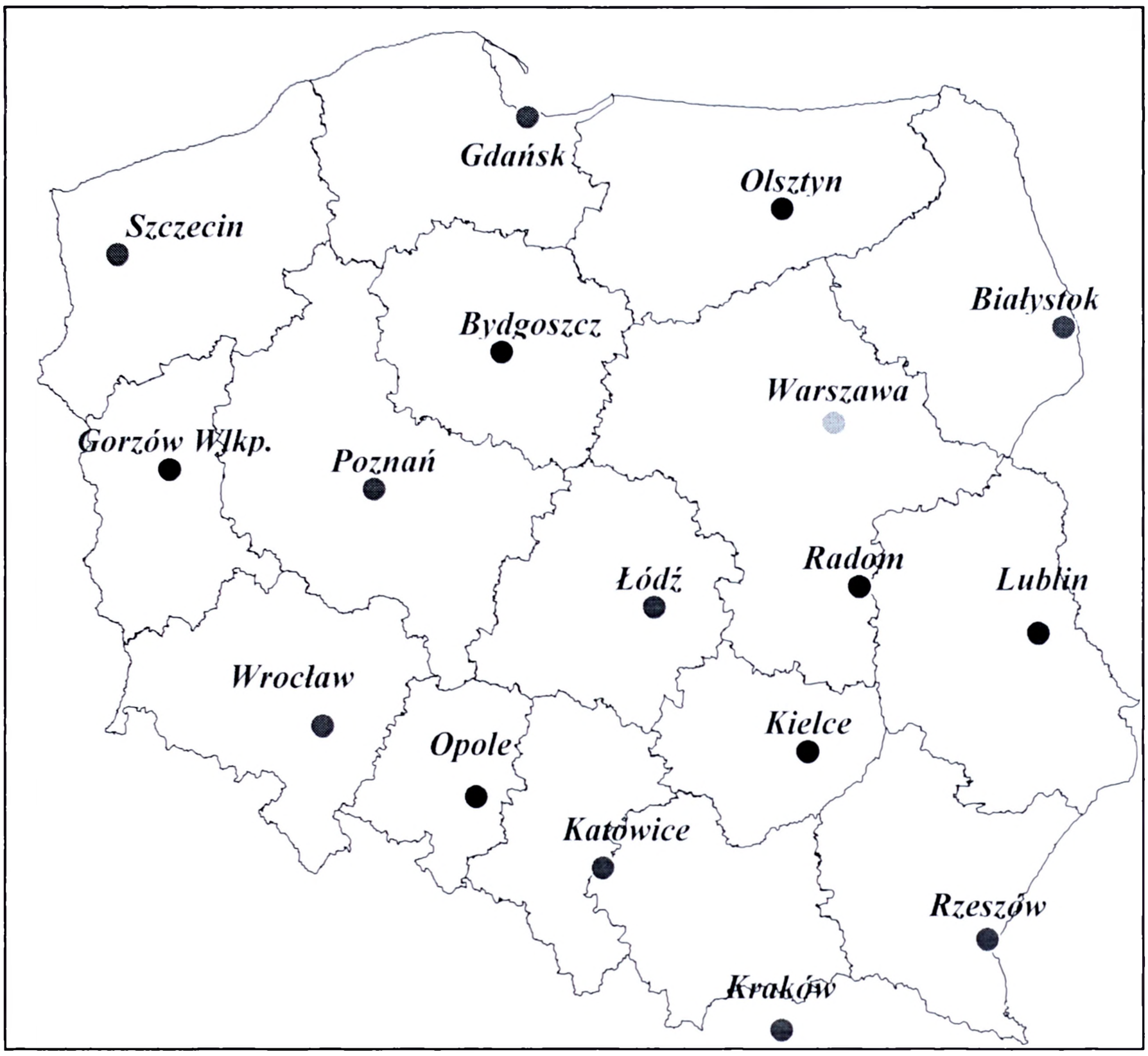
W czerwcu 2003 roku powstaje *Biuro Operacji Antyterrorystycznych Komendy Głównej Policji* (BOA KGP), jednostka podlegała bezpośrednio Komendantowi Głównemu Policji, przejęła obowiązki Zarządów Bojowego i Wsparcia Bojowego CBŚ KGP, a ponadto, jako jednostka centralna otrzymała funkcję koordynacyjną i odpowiadała za poziom wyszkolenia pododdziałów antyterrorystycznych znajdujących się na terenie funkcjonowania 16 komend wojewódzkich. Rozmieszczenie pododdziałów w kraju (rys. 3) daje jedynie ogólny pogląd na stan zabezpieczenia antyterrorystycznego w kraju.

---

[42] K. Jałoszyński, op. cit., s. 170.

[43] Niewątpliwym impulsem do podjęcia intensywnych działań w celu utworzenia centralnej jednostki antyterrorystycznej w Polsce, były wydarzenia z 11 września 2001 r. w USA.

[44] K. Jałoszyński, op. cit., s 170.



Rys. 3. Rozmieszczenie jednostek antyterrorystycznych Policji *(Na podstawie http://www.policja.pl/portal/pol/39/749/Jednostki_Policji.html)*

Kolor niebieski - Sekcje Antyterrorystyczne Policji

Kolor czerwony - Samodzielne Pododdziały Antyterrorystyczne Policji

Kolor zielony - Centralna jednostka antyterrorystyczna Policji

W wyniku kolejnych zmian organizacyjnych KGP, Biuro Operacji Antyterrorystycznych KGP w czerwcu 2004 roku przestaje istnieć. W jej miejsce powstał *Zarząd Operacji Antyterrorystycznych* i został umiejscowiony w strukturze Głównego Sztaby Policji KGP (ZOA GSP KGP). Do zadań ZOA, zgodnie z Decyzją Dyrektora Głównego Sztabu Policji należy[45]:

[45] Decyzja Nr 5/04 Dyrektora Głównego Sztabu Policji z dnia 29 czerwca 2004 r.

- realizacja zadań bojowych, analiza zagrożeń będących w zakresie właściwości pododdziałów antyterrorystycznych oraz przygotowanie związanych z tym informacji dla kierownictwa;
- analizowanie wydarzeń, w których prowadzone były działania antyterrorystyczne w celu doskonalenia form i metod ich działania, a także wypracowania projektów rozwiązań standaryzujących;
- analizowanie zdarzeń, mających miejsce na obszarze kraju i poza nim, =w których użyto urządzeń i materiałów wybuchowych do działań przestępczych oraz w działaniach bojowych pododdziałów antyterrorystycznych;
- - analizowanie zdarzeń, mających miejsce na obszarze kraju i poza nim, w których prowadzone były negocjacje w działaniach policyjnych;
- - koordynowanie współpracy pododdziałów antyterrorystycznych z podmiotami pozapolicyjnymi w zakresie działań antyterrorystycznych oraz koordynowanie współpracy komórek, właściwych w sprawach miniersko-pirotechnicznych z tymi podmiotami, w zakresie użycia materiałów i urządzeń wybuchowych do działań przestępczych.

W maju 2008 ponownie reaktywowano Biuro Operacji Antyterrorystycznych Komendy Głównej Policji jako centralnej jednostki AT w Polsce. Struktura BOA uległa zmianie.

Zadaniem Biura Operacji Antyterrorystycznych KGP jest fizyczne zwalczanie terroryzmu, prowadzenie działań bojowych, koordynowanie i nadzorowanie działań samodzielnych pododdziałów antyterrorystycznych Policji, w tym:

- nadzorowanie przygotowań do działań samodzielnych pododdziałów antyterrorystycznych Policji, zespołów minersko-pirotechnicznych oraz negocjatorów;
- prowadzenie działań bojowych, polegających na rozpoznawaniu i likwidowaniu zamachów terrorystycznych, a także przeciwdziałaniu zdarzeniom o tym charakterze;
- prowadzenie negocjacji policyjnych w ramach operacji i akcji antyterrorystycznych;
- zapewnienie, przez realizację programu szkolenia, stałej gotowości do prowadzenia działań bojowych, polegających na rozpoznawaniu, likwidowaniu zamachów terrorystycznych oraz innych działań, wymagających użycia specjalistycznych sił oraz środków, a także specjalnej taktyki działania;

- określanie potrzeb szkoleniowych, inicjowanie oraz uczestniczenie w organizowaniu szkoleń i doskonalenia zawodowego policjantów w komórkach antyterrorystycznych, komórkach właściwych w sprawach minersko-pirotechnicznych i w sprawach negocjacji policyjnych jednostek organizacyjnych Policji;
- współdziałanie z krajowymi i zagranicznymi podmiotami właściwymi w sprawach zwalczania aktów terroru[46].

W skład BOA wchodzi:

1) kierownictwo:

a) dyrektor biura,

b) zastępca dyrektora biura;

2) Wydział Bojowy I;

3) Wydział Bojowy II;

4) Wydział Bojowy III;

5) Wydział Bojowy IV;

6) Wydział Snajpersko-Rozpoznawczy;

7) Wydział Koordynacji i Szkolenia;

8) Wydział Wsparcia Technicznego;

9) Sekcja Negocjacji;

10) Sekcja Ogólna.

Zakres obowiązków, wykonywane i przewidywane sposoby działania wymagają od policjantów pododdziałów specjalnych szczególnych predyspozycji psychofizycznych, wyrażających się w: odwadze, ofiarności, opanowaniu, odporności na stres w trudnych warunkach i bardzo wysokiej sprawności fizycznej[47], dlatego też w procesie szkolenia jednostek antyterrorystycznych występuje wiele złożonych problemów organizacyjnych oraz konieczność uwzględnienia wpływu na wyniku szkolenia pewnej liczby zmiennych, nieodzowne staje się systemowe podejście oraz uwzględnienie czynników mających wpływ na efektywność procesu szkolenia, do których należą[48]:

- prognozowanie rozwoju i zakresu terroryzmu;

---

[46] http://www.policja.pl/portal/pol/560/Biuro_Operacji_Antyterrorystycznych.html

[47] M. Żywczyk, Szkolenie funkcjonariuszy pododdziałów specjalnych MO przeznaczonych do fizycznego zwalczania terroryzmu, „Zeszyty Naukowe" WSO Szczytno 1988, Nr 1/60, s. 141.

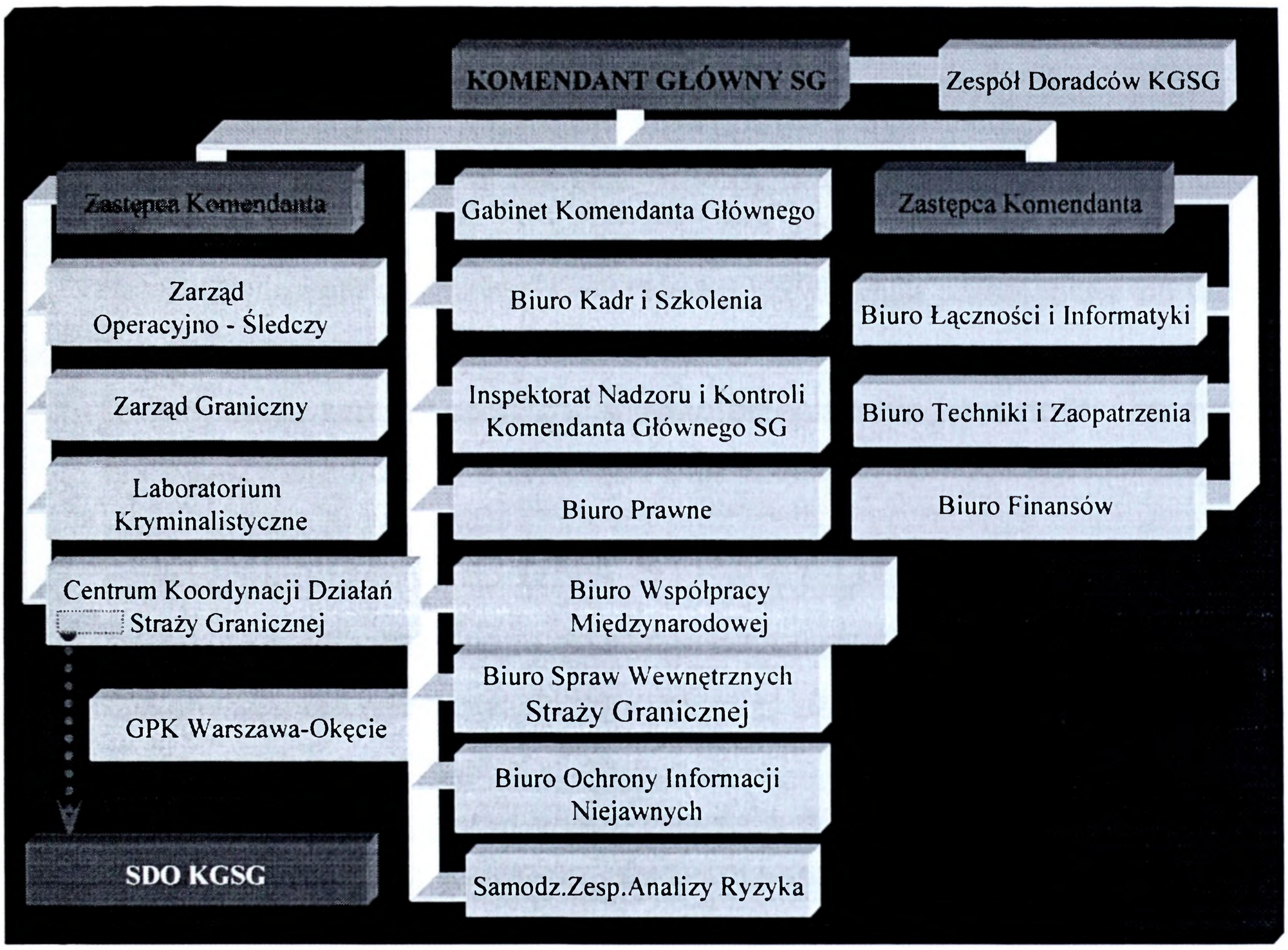
[48] A. Skuza, Teoretyczne założenia systemu szkolenia pododdziałów specjalnych, „Zeszyty Naukowe" WSO Szczytno 1988, Nr 1/60, s. 152.

- tworzenie teoretycznego modelu poziomu wyszkolenia i pożądanych cech psychofizycznych u policjantów pododdziałów specjalnych;
- dobór kandydatów w czasie procesu szkolenia;
- materialne warunki procesu szkolenia;
- poziom przygotowania zawodowego i specjalistycznego kadry dowódczej oraz instruktorskiej;
- organizacja i kierowanie systemem szkolenia.

2.2.3. Straż Graniczna

Straż Graniczna – (SG) funkcjonuje na podstawie Ustawy o Straży Granicznej z dnia 12 października 1990 r. (Dz. U. Nr 78 z 1990 r., poz. 462 z późn. zm.). Zadanie SG zgodnie z systemem zwalczania terroryzmu polega na zapobieganiu przedostawania się na teren Polski jednostek podejrzanych o terrorystyczną działalność, jak również: przechwytywaniu transportów szkodliwych substancji chemicznych, broni, amunicji i materiałów wybuchowych, jądrowych i promieniotwórczych"[49].

[49] Współczesny wymiar terroryzmu przeciwdziałanie zjawisku, red. nauk. Gryz J., Kwećka R., Wyd. AON. 2007r., s. 181.



Rys. 4. Struktura organizacyjna Komendy Głównej Straży Granicznej *(Na podstawie prezentacji Straż Graniczna w zakresie rozpoznania oraz przeciwdziałania terroryzmowi Kętrzyn 2008).*

W ramach swoich ustawowych zadań Straż Graniczna podejmuje działania takie jak:

1. Gromadzenie i analizowanie informacji dotyczących obywateli państw tzw. podwyższonego ryzyka przekraczających granicę w przejściach granicznych usiłujących przekroczyć ją nielegalnie poza przejściami;
2. Wydawanie opinii w sprawie udzielania wiz przez urzędy konsularne RP, dla obywateli z krajów tzw. podwyższonego ryzyka;
3. Monitorowanie środowisk pochodzących z państw tzw. podwyższonego ryzyka;
4. Kontrolowanie skali przewozów dużych sum pieniędzy przez granicę państwową;

5. Prowadzenie wymiany informacji z Policją, ABW, AW, SW, SKW oraz z organami państw sąsiednich w zakresie przeciwdziałania zagrożeniom terrorystycznym;
6. Analizowanie zagrożeń bezpieczeństwa granicy państwowej;
7. Kierowanie działaniami w zakresie ochrony granicy państwowej oraz kontroli ruchu granicznego;

Natomiast w celu wykluczenia możliwości popełnienia przestępstw lub wykroczeń, funkcjonariusze SG maja prawo m.in. do:

1. Dokonywania kontroli osobistej, a także przeglądania zawartości i sprawdzania bagaży w portach, na dworcach oraz środkach komunikacji lotniczej, drogowej, kolejowej i morskiej;
2. Legitymowania lub ustalania w inny sposób tożsamości osób;
3. Przeszukiwania osób, rzeczy, pomieszczeń i środków transportu;
4. Obserwowania i rejestrowania zdarzeń, przy użyciu środków technicznych do rejestracji obrazu i dźwięku.

Z całego zakresu działań wykonywanych przez Straż Graniczną dla zapobieżenia działaniom terrorystycznym szczególna uwagę przywiązuje się do działań:

1. Pozostających w związku z przekraczaniem granicy państwowej;
2. Niedopuszczeniem do wwozu i wywozu środków pieniężnych niewiadomego pochodzenia;
3. Związanych z przemieszczaniem przez granicę państwową towarów oraz przedmiotów określonych przepisami o broni, amunicji i materiałach wybuchowych;
4. Zapewniających bezpieczeństwo w międzynarodowej komunikacji lotniczej przez kontrolę bezpieczeństwa m.in. w ramach wykrywania przemieszczania materiałów promieniotwórczych, niebezpiecznych środków chemicznych, środków podwójnego zastosowania – stosując przy tym również dodatkowe formy i metody wtórnej kontroli bezpieczeństwa:
   - pasażerów i ich bagaży,
   - przesyłek pocztowych i towarów,
   - statków powietrznych przed odlotem.

Przejścia graniczne są infrastrukturą będącą w zarządzaniu innych podmiotów administracji rządowej, jednak Straż Graniczna jako ich użytkownik odpowiada za ich ochronę oraz organizację a w szczególności:

1. Ochronę obiektów będących we właściwości Straży Granicznej, przed atakami terrorystycznymi,
2. Zapobieganiu przekraczania granicy przez osoby niepożądane w RP poprzez ominięcie kontroli granicznej,
3. Zatrzymywanie osób poszukiwanych przez organa ścigania.

Wszystkie te działania mają zapobiec aktom terrorystycznym na terenie naszego kraju oraz zminimalizować swobodę poruszania się osób podejrzanych o taką działalność. Dodatkowo od 2003 roku jest prowadzona zaostrzona kontrola na granicy w przejściach granicznych oraz na granicy „zielonej". Prowadzone jest także intensywne rozpoznanie środowisk obcokrajowców pochodzących z krajów tzw. podwyższonego ryzyka. Szczególną uwagę przywiązuje się do ochrony portów lotniczych i morskich jako potencjalnych celów ataku, a także miejsc gdzie można wychwycić osoby podejrzane o działalność terrorystyczną.

Przedstawiciele Straży Granicznej od samego początku byli aktywnymi uczestnikami międzyresortowych zespołów, których zadaniem jest koordynacja przedsięwzięć mających na celu przeciwdziałanie zagrożeniom terrorystycznym. Poczynając od Zespołu do Spraw Kryzysowych powołanego przez Prezesa Rady Ministrów w 2002r. poprzez kolejne zespoły zadaniowe aż do Stałej Grupy Eksperckiej przy Międzyresortowym Zespole ds. Zagrożeń Terroryzmem MSWiA . Jednocześnie Komendant Główny Straży Granicznej powołał Zespół ds. Terroryzmu, mający za zadanie zbieranie informacji, koordynowanie działań w Straży Granicznej, a także zapewnienie współdziałania z innymi służbami w zakresie rozpoznawania, przeciwdziałania i zwalczania aktów terroru[50].

Do zakresu działania Zespołu należy w szczególności:

1. Bieżąca analiza sytuacji i informacji operacyjnych oraz innych uzyskanych podczas pełnienia służby granicznej dotyczących zagrożeń aktami terrorystycznymi, a także monitorowanie narażonych na te zagrożenia obszarów działania Straży Granicznej;

---

[50] Tamże, s. 186.

2. Inicjowanie prac legislacyjnych, których celem jest usprawnienie metod i form rozpoznania, zwalczania i przeciwdziałania zagrożeniom terrorystycznym, oraz opracowywanie projektów decyzji (zarządzeń) Komendanta Głównego Straży Granicznej w tym zakresie;
3. Koordynowanie działań antyterrorystycznych podejmowanych przez jednostki organizacyjne Straży Granicznej oraz prowadzonych w ramach współdziałania z innymi służbami;
4. Sporządzanie dokumentacji analitycznej i planistycznej[51].

Z uwagi na zagrożenia przemytu środków promieniotwórczych oraz broni chemicznej i biologicznej, wszystkie przejścia graniczne zostały wyposażone w urządzenia do kontroli radiometrycznej w celu zapobieżenia wwozowi do Polski materiałów i substancji promieniotwórczych oraz materiałów jądrowych[52].

Do kontroli materiałów promieniotwórczych w przejściach granicznych wykorzystuje się m.in. urządzenia typu:

1. UKO-1M – stacjonarne urządzenie do kontroli radiometrycznej osób;
2. UK-1M – stacjonarne urządzenie do kontroli radiometrycznej pojazdów;
3. PM 5000 – stacjonarne urządzenie do kontroli radiometrycznej osób i pojazdów, wykrywa także promieniowanie neutronowe;

Ponadto poza stacjonarnymi urządzeniami służącymi do kontroli radiometrycznej w Straży Granicznej wykorzystywane są samochody specjalne 101 X Ray z urządzeniami do prześwietlania.

W przypadku wystąpienia nietypowych lub wątpliwych zdarzeń w związku z ochroną radiometryczną zapewniona jest całodobowa konsultacja z dyżurnym specjalistą Centralnego Laboratorium Ochrony Radiologicznej. Jednocześnie w sytuacjach kiedy zaistnieją trudności w interpretacji wyników pomiarów dozymetrycznych lub pojawi się konieczność, w której należy określić rodzaj ładunku, wówczas dyżurny laboratorium zobowiązany jest do poinformowania funkcjonariuszy SG o sposobie reakcji lub wysłania na miejsce zdarzenia inspektorów ochrony radiologicznej[53].

W przypadku zaistnienia groźby użycia broni biologicznej lub chemicznej placówki Straży Granicznej zobowiązane są do podjęcia następujących działań:

---

[51] Tamże, s. 186.
[52] Hadyś T., Rola i zadania Straży Granicznej w przeciwdziałaniu zagrożeniom terrorystycznym. Wyd. Zeszyty Naukowe AON, 2003r., nr 1 (50)A s. 226.
[53] Tamże, s. 226.

1. Wzmożenie kontroli granicznej w przejściach granicznych i ścisłego przestrzegania zasad określonych w zarządzeniach Komendanta Głównego SG w sprawie kontroli przewozu przez granicę odpadów i szkodliwych substancji chemicznych, materiałów jądrowych, środków odurzających i substancji psychotropowych oraz broni, amunicji i materiałów wybuchowych;
2. Meldowanie w systemie służb dyżurnych operacyjnych o wszystkich przypadkach wystąpienia zagrożenia;
3. Wprowadzenia wcześniej opracowanych procedur:
   - zagrożeń niebezpieczną chorobą i bioterroryzmem,
   - zasad postępowania w przypadku otrzymania przesyłki niewiadomego pochodzenia,
   - zasad postępowania w sytuacjach stanowiących epidemiologiczne oznaki ataku bioterrorystycznego,
   - zasad postępowania z kombinezonami ochronnymi w przypadku zagrożenia zakażeniem laseczkami wąglika,
   - zasad użycia wybranych preparatów dezynfekcyjnych,
   - zasad postępowania na wypadek uzyskania sygnałów zagrożenia oraz podstawowych objawów klinicznych zarażenia laseczką wąglika, bakteriami jadu kiełbasianego lub wirusem ospy.
4. Utrzymywanie w gotowości do działania funkcjonariuszy ds. kontroli chemiczno-radiometrycznej oraz przeszkolenia pozostałych funkcjonariuszy w tym zakresie,
5. Utrzymywanie w gotowości do działania personelu służby zdrowia Straży Granicznej;
6. Utrzymywanie stałego kontaktu z osobami funkcyjnymi służby zdrowia Straży Granicznej w celu monitorowania zagrożeń;
7. Utrzymywanie stałego kontaktu z inspektorami sanitarnymi MSWiA, inspektorami wojewódzkimi i powiatowymi;
8. Utrzymywanie stałej łączności z wojewódzkimi stacjami sanitarno-epidemiologicznymi i personelem kierowniczym[54].

Ochrona w portach lotniczych.

Ciągłe zainteresowanie terrorystów lotnictwem może wynikać z kilku powodów:

---

[54] Rola i zadania ....., wyd. cyt., s. 228.

1. Lotnictwo jest w tej chwili najszybszym środkiem transportu potrafiącym transportować znaczne ilości ludzi na tak duże odległości. Jednocześnie ciągle trwa proces budowy jeszcze większych samolotów. Właśnie wszedł do eksploatacji Airbus – A380-800 mogący zabierać na pokład ponad 800 pasażerów co prowadzi do organizacyjnych komplikacjami, z punktu widzenia ochrony lotniska;
2. Presja właścicieli oraz akcjonariuszy na utrzymanie nieprzerwanej pracy, stale rosnąca dynamika oraz dochodowość a także bardzo wysoka wartość samolotów i infrastruktury portowej są czynnikami zwiększającymi zainteresowanie ze strony grup ekstremistycznych;
3. Wysoki stopień koncentracji ludzi w portach lotniczych, osób odprowadzających oraz innych zwiedzających jest dodatkowym czynnikiem mogącym zwiększyć efektywność ewentualnego zamachu. Porty lotnicze to miejsca, gdzie znaczna część osób to zdenerwowani, wyglądający nietypowo ludzie z bagażami wśród których łatwo można ukryć broń lub inne środki niezbędne do przeprowadzenia zamachu;
4. Mobilność i szybkość statków powietrznych oraz dotarcie w dowolny region świata może dawać iluzoryczną nadzieje terrorystom na uniknięcie odpowiedzialności za czyny i potęgować korzyści propagandowe z porwania;
5. Trudność w wyławianiu spośród podróżnych, podejrzanych osób, skutkuje możliwością maskowania przygotowań terrorystów do zamachu;
6. Wysokie prawdopodobieństwo, że zdeterminowani, odpowiednio wyszkoleni i wyposażeni terroryści przełamią potencjalny opór pasażerów, którzy są nieprzygotowani do walki i nieuzbrojeni;
7. Po przeprowadzeniu zamachów z 2001 roku w Nowym Jorku wzrosła możliwość użycia cywilnego statku powietrznego do przeprowadzenia skutecznego ataku.

Rozporządzeniem szefa MSWiA Ludwika Dorna z 19 grudnia 2005 r., opublikowanego w Dzienniku Ustaw nr 266 z 30 grudnia, Straż Graniczna została zobowiązana do zorganizowania, wyznaczenia i wyszkolenia grupy funkcjonariuszy jako „sky marshall” .

Do "wart ochronnych" na pokładach samolotów wyznacza się funkcjonariuszy:

1. Odpowiednio przeszkolonych, z zakresu specyfiki działań na pokładzie samolotu; dotyczy to takich kwestii jak: znajomość pokładów statków powietrznych, procedur obowiązujących na pokładach samolotów, skutków użycia broni palnej, sposobów unieszkodliwiania osoby niebezpiecznej bez użycia broni;

2. Znających język angielski;
3. Którzy ukończyli szkolenie specjalistyczne w zakresie udzielania pierwszej pomocy przedmedycznej;
4. Posiadających odpowiednie predyspozycje psychofizyczne do pełnienia takiej służby;
5. Mających nieposzlakowaną opinię funkcjonariuszy Straży Granicznej.[55]

Skład warty wyznacza Komendant Główny SG - po otrzymaniu decyzji prezesa Urzędu Lotnictwa Cywilnego o wprowadzeniu warty na pokład określonego samolotu. Już wcześniej informowano, że warty takie będą tylko w niektórych samolotach, np. latających do USA - czego zażyczyły sobie władze tego kraju po zamachach z 11 września 2001 r. W skład warty wchodzi nie mniej niż dwóch funkcjonariuszy. Ich liczbę określa się w zależności od typu samolotu i przewidywanego poziomu zagrożenia aktem bezprawnej ingerencji podczas lotu. Według rozporządzenia, funkcjonariusze pełnią wartę w sposób niejawny, a ich ujawnienie się wobec pasażerów może nastąpić tylko wtedy, gdy jest to niezbędne dla zapewnienia bezpieczeństwa na pokładzie. Dlatego funkcjonariusze, którzy występują w cywilu, są zobowiązani nosić broń palną, kajdanki, paralizatory, kamizelki kuloodporne i inne elementy wyposażenia w sposób nie zwracający uwagi pasażerów i uniemożliwiający nieuzasadnione ujawnienie funkcjonariuszy. Zadaniem warty jest:

1. Ujawnienie potencjalnych zagrożeń dla bezpieczeństwa samolotu;
2. Przeciwdziałanie aktom przemocy i próbom zawładnięcia maszyną;
3. Rozpoznanie i zabezpieczenie urządzeń i substancji zagrażających bezpieczeństwu oraz - w miarę możliwości - ich neutralizacja;
4. Przeciwdziałanie aktom niszczenia samolotu;
5. Podejmowanie niezbędnych działań wobec pasażera, którego zachowanie stwarza bezpośrednie niebezpieczeństwo dla uczestników lotu lub w inny sposób zagraża porządkowi.

---

[55] Rozporządzenie szefa MSWiA z dnia 19 grudnia 2005r.,Dz.U. Nr 266 poz. 2243.

2.2.4. Państwowa Straż Pożarna

Państwowa Straż Pożarna (PSP) to zawodowa, umundurowana formacja wyposażona w specjalistyczny sprzęt do walki z pożarami, klęskami żywiołowymi i innymi miejscowymi zagrożeniami. Do jej statutowych zadań należy:

- monitorowanie i zwalczanie zagrożeń pożarowych;
- organizowanie działań ratowniczych w czasie pożarów, klęsk żywiołowych i innych miejscowych zagrożeń;
- kształcenie kadr dla potrzeb Państwowej Straży Pożarnej, jednostek ochrony przeciwpożarowej i innych elementów systemu ochrony ludności;
- prowadzenie prac naukowo-badawczych w zakresie ochrony przeciwpożarowej oraz ochrony ludności;
- współpraca międzynarodowa z podobnymi służbami innych państw, na zasadach określonych odrębnymi przepisami[56].

PSP to formacja niezależna od innych jednostek, posiadająca własne siły, środki i bazę logistyczną co korzystnie wpływa na sprawność działania tej formacji czyniąc z niej trzon do integracji działań ratowniczych[57].

W strukturze PSP możemy wyróżnić następujące jednostki organizacyjne:

- Komendę Główną;
- 16 komend wojewódzkich;
- 335 komend powiatowych (miejskich). W ramach komend powiatowych działa 507 jednostek ratowniczo – gaśniczych (JRG);
- szkoły pożarnicze;
- ośrodki badawcze – Centrum Naukowo Badawcze Ochrony Przeciwpożarowej;
- Centralne Muzeum Pożarnictwa[58].

Na czele struktury organizacyjnej PSP stoi Komendant Główny. Jest on centralnym organem administracji państwowej w sprawach dotyczących ochrony przeciwpożarowej i Krajowego Systemu Ratowniczo – Gaśniczego. Do jego zadań należy:

---

[56]Ustawa z dnia 24 sierpnia 1991 r. *o Państwowej Straży Pożarnej*, Dz. U. z 2009, Nr 12 poz. 68

[57]D. Wróblewski, *Model współdziałania jednostek Państwowej Straży Pożarnej z jednostkami Obrony Cywilnej w zakresie działań ratowniczych,* rozprawa doktorska, AON 2001, Warszawa, s. 53.

[58]R. Kardaś, *Krajowy system ratowniczo – gaśniczy w systemie bezpieczeństwa RP,* praca studyjna AON, Warszawa 2004, s. 47.

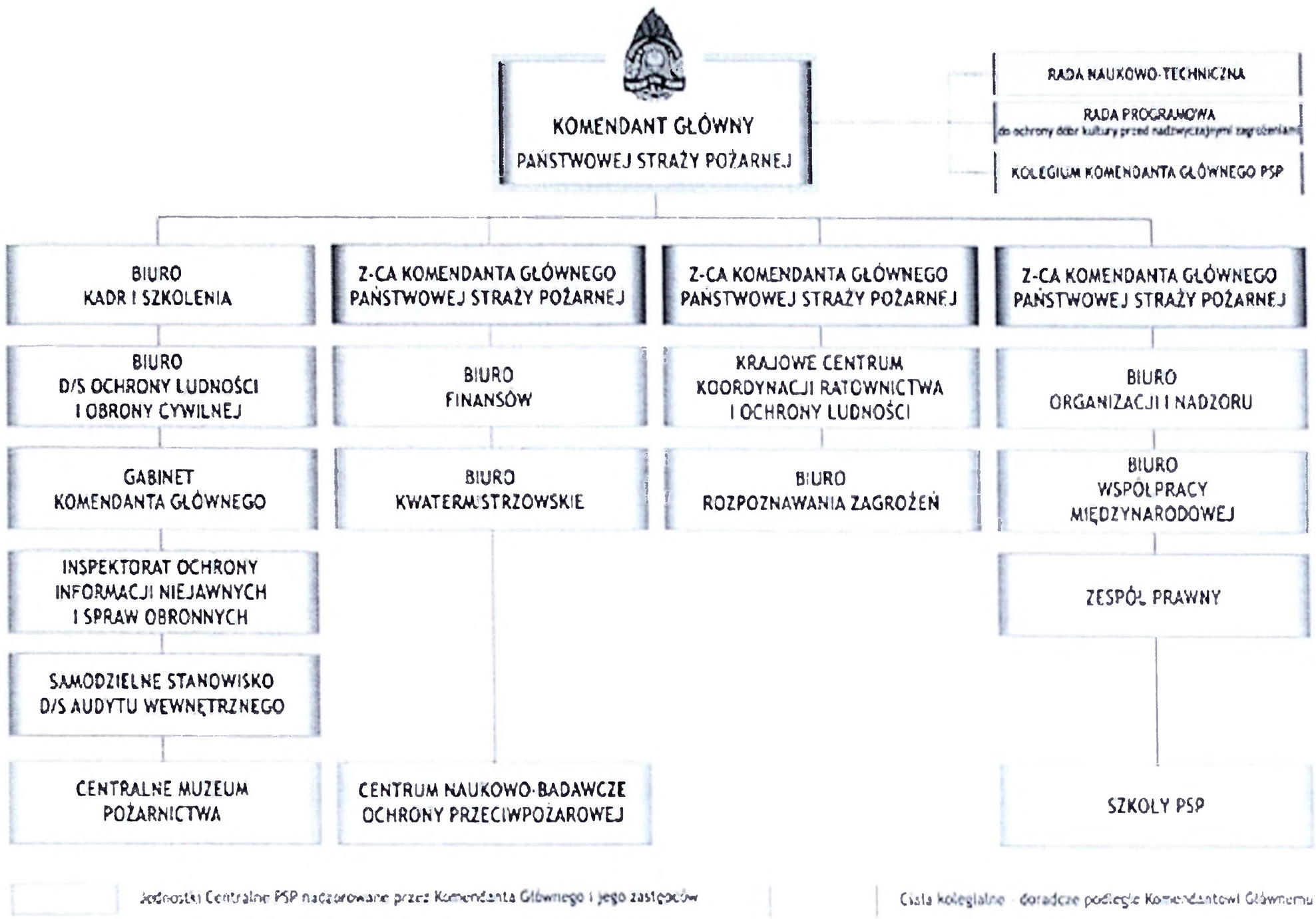
- dysponowanie siłami i środkami KSRG na obszarze kraju;
- ustalanie planu sieci podmiotów należących do systemu;
- ustalanie planu rozmieszczania sprzętu specjalistycznego;
- dysponowanie odwodami operacyjnymi KSRG;
- dowodzenie działaniami ratowniczymi prowadzonymi siłami szczebla krajowego;
- analizowanie zagrożeń pożarowych i innych na terytorium kraju;
- inicjowanie prac naukowo-badawczych w zakresie ochrony przeciwpożarowej i ratownictwa;
- inicjowanie oraz przygotowywanie projektów aktów normatywnych dotyczących ochrony przeciwpożarowej i ratownictwa;
- koordynacja współpracy międzynarodowej[59].

Komendant Główny wykonuje swoje zadania przy pomocy Komendy Głównej PSP i innych podległych mu jednostek organizacyjnych. Komenda funkcjonuje w oparciu o 10 biur, z pośród których najważniejsze to: Krajowe Centrum Koordynacji Ratownictwa i Ochrony Ludności, Biuro Rozpoznawania Zagrożeń, Biuro Kadr i Szkolenia i Biuro Współpracy Międzynarodowej. Poza biurami w strukturze Komendy Głównej funkcjonują: gabinet komendanta głównego i inne wyspecjalizowane komórki zaprezentowane na rysunku 5[60].

---

[59] M. Schroeder, M. Płotica, J. Żuber, *Krajowy System Ratowniczo – Gaśniczy w systemie bezpieczeństwa państwa. Czy jesteśmy bezpieczni?*, KG PSP KCKR, Warszawa 1994., s. 104.

[60] http://www.kgpsp.gov.pl



Rys. 5. Struktura organizacyjna Komendy Głównej PSP *(Źródło: http://kgpsp.gov.pl)*

Przepisy ustawy o Państwowej Straży Pożarnej stanowią, iż Komendant Główny PSP jest odpowiedzialny za kierowanie systemem ratownictwa na obszarze całego kraju, a kolejno komendanci wojewódzcy i powiatowi kierują systemem na terenie swojej jurysdykcji.

Akcje ratownicze organizuje i kieruje nimi jednostka PSP. Ustawa o PSP nadaje strażakom biorącym udział w akcji szereg uprawnień mających usprawnić prowadzenie działań. W katalogu kompetencji znalazły się między innymi uprawnienia do zarządzenia ewakuacji zagrożonej ludności, wstrzymania komunikacji w ruchu lądowym czy też żądania udostępnienia pojazdów[61].

W hierarchii działań ratowniczych najwyższy szczebel zajmują dowódcy z jednostek PSP. Mają oni obowiązek przejąć dowodzenie nad akcja od jednostek OSP czy zakładowych straży pożarnych. Pod kierownictwem dowódcy jednostki PSP wszystkie podmioty biorące udział w akcji zobowiązane są do podporządkowania

---

[61] Art. 21 ustawy z dnia 24 sierpnia 1991 r. *o Państwowej Straży Pożarnej*, Dz. U. z 2009, Nr 12 poz. 68

jego rozkazom i koordynacji działań według jego zaleceń[62]. Szczegółowo zakres kompetencji i uprawnień kierującego akcja określa rozporządzenie Rady Ministrów z dnia 4 lipca 1992 r. *w sprawie zakresu i trybu korzystania z praw przez kierującego działaniami ratowniczymi* (Dz. U. z 1992 nr 54 poz. 259).

Jednostki PSP pełnią również funkcje rozpoznawczo – kontrolną w obszarze bezpieczeństwa pożarowego i zapobiegania innym miejscowym zagrożeniom w tym terrorystycznym. Występujące w strukturze PSP stanowiska kierowania zapewniają przepływ informacji pomiędzy elementami systemu ratowniczo - gaśniczego, a także stanowią źródło sygnałów alarmowych dla podmiotów ratowniczych[63].

Jednostka ratowniczo - gaśnicza to podstawowa jednostka operacyjna w strukturze PSP. Te jednostki organizacyjne, za utworzenie, których odpowiadają komendanci powiatowi PSP jako jedyne posiadają potencjał umożliwiający samodzielne prowadzenie działań ratowniczych.

Oprócz prowadzenia indywidualnych działań JRG są przygotowane do współdziałania z innymi podmiotami w ramach akcji ratowniczych na wypadek klęsk żywiołowych bądź innych zagrożeń[64].

Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 września 2000 roku *w sprawie szczegółowych zasad wyposażenia jednostek organizacyjnych Państwowej Straży Pożarnej*[65] określa, w sposób ogólny, rodzaj i ilości sprzętu jaki powinien być na wyposażeniu JRG i innych jednostek organizacyjnych PSP. Jakość i ilość posiadanego przez JRG sprzętu determinuje szybkość i efektywność akcji ratunkowych prowadzonych przez jednostkę.

W strukturze PSP działają również jednostki odpowiedzialne za ratownictwo specjalistyczne. Funkcjonują one w ramach pododdziałów w odwodach operacyjnych, te zaś wchodzą w skład wojewódzkich brygad odwodowych. W roku 2004 funkcjonowały następujące grupy ratownictwa:

---

[62] Praca zbiorowa *Zintegrowany system ratowniczy w czasie pokoju. Państwowa Straż Pożarna jako główna siła w Krajowym Systemie Ratowniczo – Gaśniczym*, WKO AON, Warszawa 1996, s.23.

[63] Rozporządzenie Rady Ministrów z dnia 31 lipca 2001 *w sprawie szczegółowych zasad kierowania i współdziałania jednostek ochrony przeciwpożarowej biorących udział w działaniu ratowniczym*, Dz. U. z 2001 nr 82 poz. 895.

[64] Op. cit., *Zintegrowany system ratowniczy w czasie…*, s.35.

[65] Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 września 2000 roku *w sprawie szczegółowych zasad wyposażenia jednostek organizacyjnych Państwowej Straży Pożarnej* Dz. U. z 2000 r., nr 93 poz. 1035.

- 19 grup ratownictwa wysokościowego;
- 44 grup ratownictwa chemicznego;
- 6 grup ratownictwa;
- 53 grupy ratownictwa wodno – nurkowego;
- 2 grupy ratownictwa medycznego;
- 4 grupy poszukiwawczo – ratunkowe;
- 1 grupa ratownictwa radiacyjnego[66].

Ilość grup ratownictwa specjalistycznego w połączeniu z siłami i środkami jednostek ratowniczo – gaśniczych wskazuje na znaczny potencjał PSP w zakresie ochrony życia i zdrowia obywateli przed wszelkiego rodzaju zagrożeniami.

Bazy sprzętu specjalistycznego

W sytuacji gdy akcja wymaga użycia specjalistycznego sprzętu ze względu na jej rozmiar i stopień komplikacji jednostki PSP mogą korzystać z zasobów baz sprzętu specjalistycznego[67].

Koncepcja utworzenia baz zakładała ich rozmieszczenie w 14 najbardziej newralgicznych punktach kraju. Po analizie zagrożeń występujących w rejonach zdecydowano umieścić bazy w Warszawie, Szczecinie, Olsztynie, Gdańsku, Krakowie, Rzeszowie, Bydgoszczy, Białymstoku, Łodzi, Poznaniu, Kielcach, Wrocławiu, Lublinie i Katowicach. Każda baza miała działać na obszarze o promieniu do 150 km, a odległość ta systematycznie zmniejsza się, adekwatnie do stanu wyposażenia jednostek PSP.

Bazy sprzętu specjalistycznego na swoim wyposażeniu posiadają głównie ciężki sprzęt ratowniczy taki jak np. dźwigi, wozy ratownictwa chemicznego, wozy ratownictwa ekologicznego, śmigłowce, sprzęt do robót ziemnych etc[68].

Dla zapewnienia bezpieczeństwa obywateli największe znaczenie maja te podmioty, które posiadają pełną gotowość do podjęcia natychmiastowego działania na wypadek zagrożeń. Warunek ten definitywnie spełnia PSP, która posiada liczne i dobrze wyposażone jednostki, a także wykwalifikowaną kadrę[69]. Wykorzystując swoje siły i środki PSP determinuje jakość działania KSRG. Poza działaniami stricte ratowniczymi, PSP kształtuje siatkę systemu poprzez nawiązywanie porozumień z podmiotami zajmującymi się ratownictwem, a także wpływa na jakość działania podmiotów

---

[66] Op. cit., R. Kardaś, *Krajowy system ratowniczo – gaśniczy*..., s. 48.
[67] Op. cit., *Zintegrowany system ratowniczy w czasie*..., s.39.
[68] Tamże, s. 40.
[69] Op. Cit., R. Kardaś, *Krajowy system ratowniczo – gaśniczy*..., s. 46

już działających w systemie między innymi poprzez liczne szkolenia, standaryzację i normatywizację.

2.3. Podmioty podległe MON

2.3.1. Służba Wywiadu Wojskowego

Służbę Wywiadu Wojskowego utworzono z dniem 1 października 2006 r. na podstawie ustawy z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz o Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 i Nr 218, poz. 1592) jako służbę specjalną, właściwą w sprawach ochrony przed zagrożeniami zewnętrznymi dla obronności Państwa, bezpieczeństwa i zdolności bojowej SZ RP oraz innych jednostek organizacyjnych podległych lub nadzorowanych przez Ministra Obrony Narodowej.

Szef SWW podlega Ministrowi Obrony Narodowej z zastrzeżeniem ustawowych uprawnień Prezesa Rady Ministrów lub Ministra Koordynatora do Spraw Służb Specjalnych.

Do **ustawowych zadań SWW** należy:

1. *„uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć istotne znaczenie dla:*

a) bezpieczeństwa potencjału obronnego RP,

b) bezpieczeństwa i zdolności bojowej SZ RP;

c) warunków realizacji, przez SZ RP, zadań poza granicami państwa;

2. *rozpoznawanie i przeciwdziałanie:*

a) militarnym zagrożeniom zewnętrznym godzącym w obronność RP,

b) zagrożeniom międzynarodowym terroryzmem;

3. *rozpoznawanie międzynarodowego obrotu bronią, amunicją i materiałami wybuchowymi oraz towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także rozpoznawanie międzynarodowego obrotu bronią masowej zagłady i zagrożeń związanych z rozprzestrzenianiem tej broni oraz środków jej przenoszenia;*
4. *rozpoznawanie i analizowanie zagrożeń występujących w rejonach napięć, konfliktów i kryzysów międzynarodowych, mających wpływ na obronność państwa oraz zdolność bojową SZ RP, a także podejmowanie działań mających na celu eliminowanie tych zagrożeń;*

5. *prowadzenie wywiadu elektronicznego na rzecz SZ RP oraz przedsięwzięć z zakresu kryptoanalizy i kryptografii;*
6. *współdziałanie w organizowaniu polskich przedstawicielstw wojskowych za granicą;*
7. *uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia;*
8. *podejmowanie innych działań przewidzianych dla SWW w odrębnych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana"*[70].

Powyższe zadania są realizowane poza granicami Rzeczypospolitej Polskiej. Działalność SWW na terytorium Rzeczypospolitej Polskiej może być prowadzona wyłącznie w związku z jej działalnością poza granicami państwa.

W granicach ustawowych zadań, funkcjonariusze SWW wykonują czynności:

Operacyjno-rozpoznawcze

Funkcjonariusze SWW wykonując czynności operacyjno-rozpoznawcze mają prawo:

- *„żądania niezbędnej pomocy od instytucji państwowych, organów administracji rządowej i samorządu terytorialnego oraz przedsiębiorców prowadzących działalność w zakresie użyteczności publicznej; wymienione instytucje, organy i przedsiębiorcy są obowiązani, w zakresie swojego działania, do udzielania nieodpłatnie tej pomocy, w ramach obowiązujących przepisów prawa;*
- *zwracania się o niezbędną pomoc do innych przedsiębiorców, jednostek organizacyjnych i organizacji społecznych , jak również zwracania się w nagłych wypadkach do każdej osoby o udzielenie doraźnej pomocy w ramach obowiązujących przepisów prawa;*
- *posługiwania się dokumentami, które uniemożliwiają ustalenie danych identyfikujących funkcjonariusza oraz środków, którymi się posługuje przy wykonywaniu zadań służbowych;*
- *korzystania z pomocy osób nie będących funkcjonariuszami;*

---

[70] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz o Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 i Nr 218, poz. 1592).

- *zbierania, także niejawnie, wszelkich danych osobowych , jeżeli jest to uzasadnione charakterem realizowanych zadań, oraz przetwarzania ich bez wiedzy i zgody osoby, której te dane dotyczą".*

Ponadto funkcjonariusze realizują zadania **analityczno-informacyjne**.

2.3.2. Służba Kontrwywiadu Wojskowego

Podstawowe zadania SKW zostały określone w art. 5 ustawy o SKW i SWW[71].

Należą do nich:

1. *„rozpoznawanie, zapobieganie oraz wykrywanie popełnianych przez żołnierzy pełniących czynną służbę wojskową, funkcjonariuszy SKW i SWW oraz pracowników SZ RP i innych jednostek organizacyjnych MON, przestępstw:*
   a. *przeciwko pokojowi, ludzkości oraz przestępstw wojennych określonych w rozdziale XVI ustawy z dnia 6 czerwca 1997 r. - Kodeks karny (Dz. U. Nr 88, poz. 553, z późn. zm.), a także innych ustawach i umowach międzynarodowych,*
   b. *przeciwko Rzeczypospolitej Polskiej określonych w rozdziale XVII ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, oraz takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność,*
   c. *określonych w art. 140 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny,*
   d. *określonych w art. 228-230 ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON,*
   e. *przeciwko ochronie informacji określonych w rozdziale XXXIII ustawy z dnia 6 czerwca 1997 r. - Kodeks karny, jeżeli mogą one zagrażać bezpieczeństwu lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON, a także takich czynów skierowanych przeciwko państwom obcym, które zapewniają wzajemność,*
   f. *określonych w art. 33 ustawy z dnia 29 listopada 2000 r. o obrocie z zagranicą towarami, technologiami i usługami o znaczeniu strategicznym dla bezpieczeństwa państwa, a także dla utrzymania międzynarodowego pokoju i bezpieczeństwa (Dz. U. z 2004 r. Nr 229, poz. 2315),*

---

[71] Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego Dz.U. z 2006r. Nr 104, poz. 709,

g. związanych z działalnością terrorystyczną oraz innych niż wymienione w lit. a-f, godzących w bezpieczeństwo potencjału obronnego państwa, SZ RP oraz jednostek organizacyjnych MON, a także państw, które zapewniają wzajemność;

2. *współdziałanie z Żandarmerią Wojskową i innymi organami uprawnionymi do ścigania przestępstw wymienionych w pkt 1;*
3. *realizowanie, w granicach swojej właściwości, zadań służby ochrony państwa określonych w ustawie z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych (Dz. U. z 2005 r. Nr 196, poz. 1631 oraz z 2006 r. Nr 104, poz. 708);*
4. *uzyskiwanie, gromadzenie, analizowanie, przetwarzanie i przekazywanie właściwym organom informacji mogących mieć znaczenie dla obronności państwa, bezpieczeństwa lub zdolności bojowej SZ RP lub innych jednostek organizacyjnych MON, w zakresie określonym w pkt 1, oraz podejmowanie działań w celu eliminowania ustalonych zagrożeń;*
5. *prowadzenie kontrwywiadu radioelektronicznego oraz przedsięwzięć z zakresu ochrony kryptograficznej i kryptoanalizy;*
6. *uczestniczenie w planowaniu i przeprowadzaniu kontroli realizacji umów międzynarodowych dotyczących rozbrojenia;*
7. *ochrona bezpieczeństwa jednostek wojskowych, innych jednostek organizacyjnych MON oraz żołnierzy wykonujących zadania służbowe poza granicami państwa;*
8. *ochrona bezpieczeństwa badań naukowych i prac rozwojowych zleconych przez SZ RP i inne jednostki organizacyjne MON oraz produkcji i obrotu towarami, technologiami i usługami o przeznaczeniu wojskowym zamówionymi przez SZ RP i inne jednostki organizacyjne MON, w zakresie określonym w pkt 1;*
9. *podejmowanie działań, przewidzianych dla SKW, w innych ustawach, a także umowach międzynarodowych, którymi Rzeczpospolita Polska jest związana".*

Zadania SKW obejmują również rozpoznawanie oraz wykrywanie przestępstw, popełnionych we współdziałaniu z żołnierzami pełniącymi czynną służbę wojskową, funkcjonariuszami SKW i SWW lub pracownikami SZ RP i innych jednostek organizacyjnych MON. Działalność SKW poza granicami Rzeczypospolitej Polskiej może być prowadzona w związku z jej działalnością na terytorium państwa wyłącznie w zakresie realizacji zadań określonych w ustawie.

Służba Kontrwywiadu Wojskowego przy realizacji swoich działań współdziała[72]:

1. *„ze Sztabem Generalnym Wojska Polskiego i innymi komórkami organizacyjnymi Ministerstwa Obrony Narodowej oraz dowódcami rodzajów SZ RP, okręgów wojskowych, garnizonów wojskowych i jednostek wojskowych;*
2. *odpowiednimi organami, służbami i instytucjami podległymi ministrowi właściwemu do spraw wewnętrznych;*
3. *odpowiednimi organami i jednostkami organizacyjnymi podległymi ministrowi właściwemu do spraw finansów publicznych;*
4. *odpowiednimi organami, służbami i instytucjami podległymi ministrowi właściwemu do spraw zagranicznych;*
5. *innymi organami, służbami i instytucjami uprawnionymi do wykonywania czynności operacyjno-rozpoznawczych".*

2.3.3. Wojska Specjalne

Wojska specjalne będące dziś elitą każdych sił zbrojnych, nie zawsze były właściwie postrzegane. Z reguły rozwijane w okresach wojen i konfliktów, tuż po nich zakończeniu były w większości likwidowane, przez wiele lat były typowym przejawem działań wywołanych „chorobą zwycięstwa" opisywanych przez Jamesa F. Dunningana i Raymonda Macedonia.[73] Obecna sytuacja międzynarodowa wykazała w sposób niezbity, iż jedynie wszechstronne wykorzystanie wojsk specjalnych może okazać się w niedalekiej przyszłości jedynym, skutecznym antidotum na wyzwania XXI wieku. Państwa Sojuszu Północnoatlantyckiego zdecydowanie rozwijają wojska specjalne i tworzą prawne podstawy ich działań zarówno w granicach własnego państwa jak i poza jego granicami. Podstawą rozwoju jest obawa przed lawinowo narastającym zagrożeniem ze strony ugrupowań terrorystycznych oraz przestępczości zorganizowanej, których wzajemne powiązania (podziemia narkotykowego, przestępczości międzynarodowej i ugrupowań terrorystycznych) są dla każdego badacza problemu rzeczą oczywistą. Wzrastająca możliwość proliferacji broni masowego rażenia stanowi kolejne ogniwo łańcucha łączącego bezpieczeństwo państwa z koniecznością

---

[72] Tamże.

[73] Za C. Weinberger, P. Schweizer, Następna wojna światowa, ALBATROS, Warszawa 1998r., s. 17 „[...] Wojna w Zatoce tylko wzmocniła poczucie, że Ameryka nie potrzebuje tak dużej armii. [...]podczas uroczystości dla uczczenia zwycięstwa wiwatujące tłumy nie mogły powstrzymać myśli >>teraz, gdy wybuchnął pokój, nie potrzebujemy aż tylu tych naprawdę bombowych żołnierzy<<"

rozwoju sił specjalnych. Uwarunkowania prawne regulujące zasady użycia wojsk specjalnych w warunkach państwa demokratycznego stanowią niewątpliwie spore wyzwanie dla polityków tych państw, które nie mają doświadczenia w zwalczaniu zagrożeń tego typu.

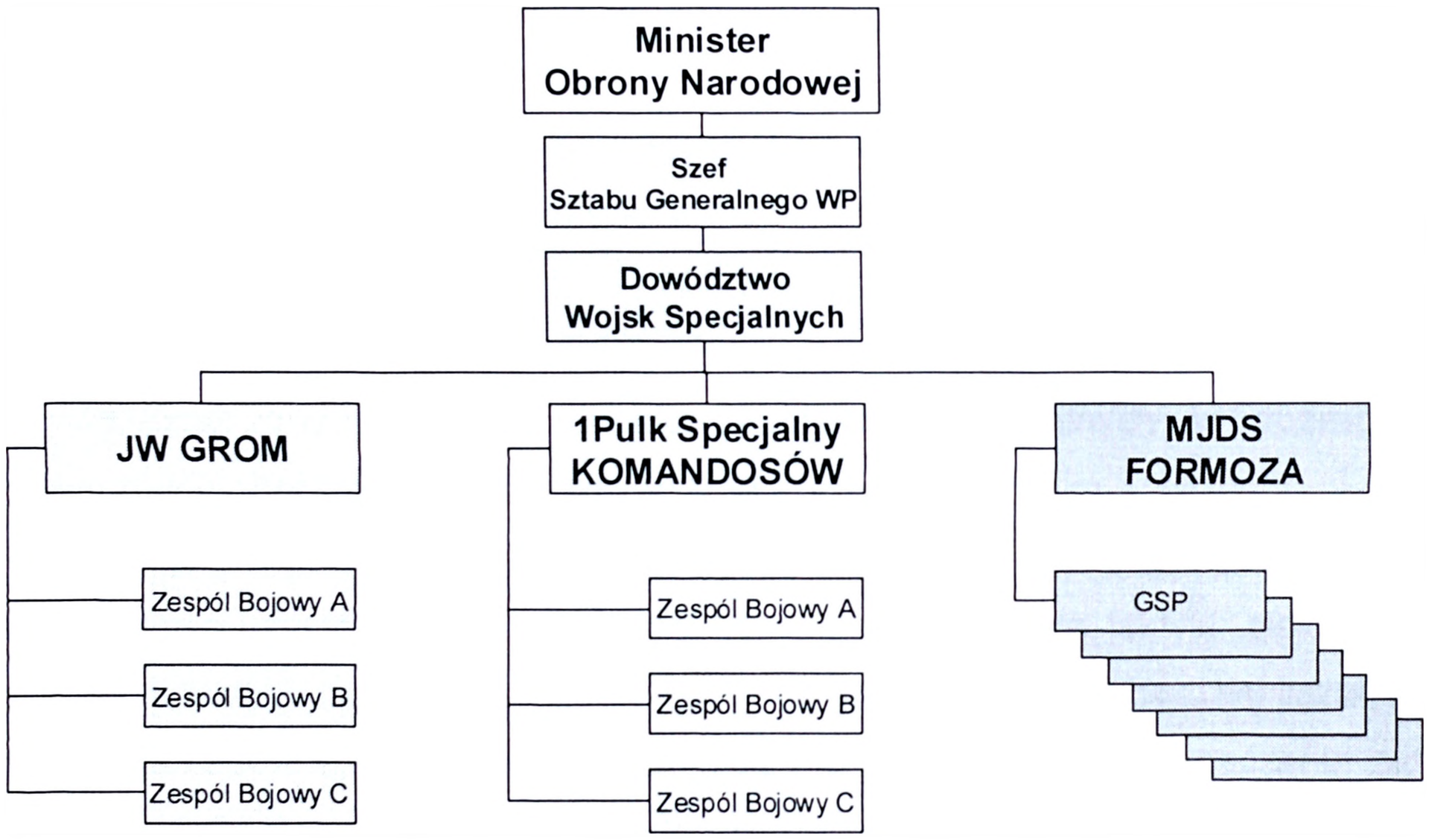
Nowa koncepcja strategiczna NATO oraz strategie bezpieczeństwa i obronności państwa, zakładają wykrywanie i zwalczanie zagrożeń, a zwłaszcza zagrożeń terrorystycznych, przez poszukiwanie i likwidowanie źródeł ich zaistnienia. W koncepcjach tych siły zbrojne będą uczestniczyć w misjach pokojowych, akcjach humanitarnych i poszukiwawczo-ratowniczych oraz zwalczaniu międzynarodowego terroryzmu. Wojska specjalne są pewnym powszechnie stosowanym „lekiem" i skutecznym środkiem w działaniach tego typu. Polska od dłuższego czasu sukcesywnie przebudowuje swoje Wojska Specjalne z zamiarem dostosowania ich struktur i zdolności do światowych standardów. Tym samym Wojska specjalne systematycznie osiągają zdolności niezbędne w działaniach antyterrorystycznych realizowanych na obszarze kraju i w rejonach odpowiedzialności Sojuszy oraz Unii Europejskiej. Stają się istotnym elementem systemu walki z terroryzmem mogącym działać w pełni samodzielnie lub współdziałać z pozostałymi narzędziami podmiotu wchodzącymi w skład tego systemu.

W roku 1994 na podstawie zarządzenia Szefa Sztabu Generalnego WP zlikwidowano pododdziały działań specjalnych na szczeblu operacyjnym i taktycznym (tzw. okręgowe kompanie specjalne oraz kompanie specjalne wchodzące w skład dywizyjnych batalionów rozpoznawczych).

Jednocześnie na bazie 1. Batalionu Szturmowego utworzono 1. Pułk Specjalny i podporządkowano go bezpośrednio Szefowi Zarządu Rozpoznawczego Sztabu Generalnego. Jednocześnie utrzymano kompanię specjalną płetwonurków Marynarki Wojennej. W roku 1999 w skład jednostek specjalnych podległych Ministerstwu Obrony Narodowej włączono "GROM" jednostkę podległą dotąd Ministerstwu Spraw Wewnętrznych. Tym samym siły specjalne MON zyskały jednostkę doskonale przygotowaną do działań antyterrorystycznych (jednakże w początkowym okresie bez stosownych uprawnień legislacyjnych do działań na obszarze kraju).

2.3.3.1. Dowództwo Wojsk Specjalnych

Na podstawie decyzji Ministra Obrony Narodowej z października 2006 roku sformowano z dniem 1 stycznia 2007 Dowództwo Wojsk Specjalnych, będące organem dowodzenia szczebla operacyjnego, zabezpieczającym od strony wykonawczej sprawowanie przez Dowódcę Wojsk Specjalnych funkcji dowodzenia i zarządzania podległymi jednostkami organizacyjnymi Wojsk Specjalnych w procesie ich wszechstronnego przygotowania do realizacji zadań w czasie zagrożenia bezpieczeństwa państwa i wojny. Docelowa struktura Wojsk Specjalnych wraz z ich podległością przedstawiona została na rys. 6.



Rys. 6. Docelowa struktura Wojsk Specjalnych wraz z ich podległością *(Opracowanie własne)*

Dowództwo Wojsk Specjalnych realizuje zadania związane z opracowaniem koncepcji rozwoju i użycia wojsk przeznaczonych do prowadzenia działań specjalnych oraz nadzór nad procesem szkolenia żołnierzy z jednostek specjalnych. Do jego zadań należy również realizacja i koordynacja przedsięwzięć związanych z użyciem jednostek specjalnych poza granicami kraju i na jego terenie, w tym przygotowaniem do działań w ramach Wielonarodowych Połączonych Sił Operacji Specjalnych NATO i Unii Europejskiej. Istotnym z punktu widzenia przyszłości Wojsk specjalnych zadaniem jest nadzorowanie poziomu zdolności bojowej sił i środków prze-

znaczonych do działań specjalnych oraz określanie potrzeb w zakresie uzbrojenia, wyposażenia, szkolenia i prowadzenia ćwiczeń, jak również opracowanie zasad rekrutacji do jednostek specjalnych i określenie kierunków kształcenia (doskonalenia) kadry tych jednostek.

Zadania te wynikają pośrednio również z nowelizacji ustawy o powszechnym obowiązku obrony Rzeczpospolitej Polskiej, która nakłada na Dowódcę Wojsk Specjalnych cztery główne zadania:

- dowodzenie związkami organizacyjnymi i jednostkami wojskowymi Wojsk Specjalnych;
- planowanie i realizację operacyjnego rozwinięcia oraz użycia Wojsk Specjalnych;
- szkolenie podległych związków organizacyjnych i jednostek wojskowych;
- przygotowanie sił i środków Wojsk Specjalnych do działań bojowych w sytuacjach przewidzianych w ustawach i ratyfikowanych umowach międzynarodowych.

1. Pułk Specjalny KOMANDOSÓW

Przeznaczony jest do prowadzenia działań specjalnych w operacyjno-strategicznych obszarach zainteresowania Sił Zbrojnych RP.

Pułk jest w pełni profesjonalnie przygotowaną i wyszkoloną jednostką o wysokim priorytecie użycia, realizującą zadania głównie w obszarze taktyki „zielonej[74]" z elementami taktyki „czarnej" i „niebieskiej[75]". Pułk ma stanowić najbardziej liczną jednostkę organizacyjną, co będzie odzwierciedlać jej podstawowe przeznaczenie jakim będzie zdolność do prowadzenia zakrojonych na szeroką skalę operacji specjalnych na lądzie i wodach śródlądowych samodzielnie lub we współdziałaniu z innymi jednostkami specjalnymi w warunkach gdy użycie sił konwencjonalnych będzie niemożliwe lub niewskazane. Do zasadniczych zadań jednostki należą:

- rozpoznanie specjalne;
- wsparcie militarne;
- akcje bezpośrednie;

---

[74] **Taktyka zielona** – działania bojowe prowadzone wg zasad obowiązujących w Wojskach Specjalnych na potrzeby zakrojonych na szeroką skalę (w sensie obszaru i zaangażowanych sił) operacji specjalnych przeciwko obiektom infrastruktury krytycznej lub instalacjom (organizacjom) wojskowym, powstańczym lub terrorystycznym.

[75] **Taktyka niebieska** – działania bojowe prowadzone wg zasad obowiązujących w Wojskach Specjalnych na potrzeby operacji prowadzonych na obiekty stałe infrastruktury morskiej takie jak platformy, porty, wojskowe instalacje nabrzeżne oraz obiekty ruchome takie jak statki, okręty itp. rozmieszczone w środowisku wodnym (morskim) lub pasie wybrzeżach.

- **operacje przeciwterrorystyczne i przeciwpowstańcze;**
- uwalnianie zakładników – tylko w podstawowym zakresie, gdy z uwagi na deficyt czasu lub sytuację operacyjną nie będzie możliwe użycie Jednostki Wojskowej GROM.

Ponadto 1. PSK będzie mógł być użyty do wsparcia operacji Jednostki Wojskowej GROM w środowisku lądowym.

Jednostka Wojskowa GROM

Jednostka Wojskowa „GROM" im. Cichociemnych Spadochroniarzy Armii Krajowej – sformowana 13 lipca 1990. Skrót GROM oznacza: Grupa Reagowania Operacyjno-Manewrowego. Koncepcję powołania do życia specjalnej jednostki wojskowej, zdolnej do ratowania polskich obywateli, w kwietniu 1990 r., przedstawił ówczesnemu wiceministrowi spraw wewnętrznych, Krzysztofowi Kozłowskiemu podpułkownik Sławomir Petelicki[76]. Do głównych powodów powstania tej jednostki należy zaliczyć:

- zagrożenie wynikające z demokratyzacji życia oraz otwarcie granic;
- problemy w trakcie realizacji operacji „Most"[77];
- zamach na polskich dyplomatów w Bejrucie.

Istotną sprawą była również ówczesna sytuacja wewnętrzna w Polsce, nastąpił bowiem gwałtowny wzrost agresji ze strony przestępczości zorganizowanej, zaczęto używać broni palnej. Szczególnym szokiem dla polityków była akcja w podwarszawskim Nadarzynie, gdzie doszło do starcia między policją a bandytami, która jednoznacznie uświadomiła, że nie mamy odpowiednich sił do walki ze zorganizowaną przestępczością[78]. Była to jednocześnie pierwsza polska jednostka, która zorganizowana została według najlepszych wzorców brytyjskich i amerykańskich.

Przez dziesięć lat formacja GROM funkcjonowała w strukturach resortu spraw wewnętrznych, od 1999 roku podporządkowano ją MON, gdzie została odpowiednio

---

[76] H. Królikowski, *Wojskowa Formacja Specjalna GROM im. Cichociemnych Spadochroniarzy Armii Krajowej: 1990–2000*, Gdańsk 2001, s. 29–32.

[77] Tamże, s. 30. Operacja „Most" jest to tajna, masowa akcja przesiedlania rosyjskich Żydów, emigrujących przez Polskę do Izraela 1990 r. Zagrożenie terrorystyczne, które stało się realne dla Polski od momentu, kiedy premier Tadeusz Mazowiecki na spotkaniu z przedstawicielami Amerykańskiego Kongresu Żydów powiedział, że Polska udzieli pomocy Żydom emigrującym ze Związku Radzieckiego i zapewni im tranzyt.

[78] J. Rybak, *Grom.pl: Tajne operacje w Afganistanie, Zatoce Perskiej i Iraku*, „Jeden Świat", Warszawa 2005, s. 17–18.

doposażona do nowych zadań oraz rozszerzono jej zakres szkolenia[79].

Jednostka specjalna „GROM" przeznaczona jest do zwalczania międzynarodowego terroryzmu, skierowanego na obywateli i obiekty RP, na obszarze kraju i za granicą. Jest w pełni zawodową jednostką wojskową, samodzielna budżetowo i logistycznie. Przerzut powietrzny jednostki zabezpieczają załogi i śmigłowce Dowództwa Wojsk Lotniczych i Wojsk Lądowych. Zasadnicze zadania bojowe jednostki specjalnej „GROM" obejmują:

Działania antyterrorystyczne na ladzie i morzu taktyka „czarna"":

- uwalnianie zakładników z różnych środków transportowych i budynków;
- statyczną i dynamiczną ochronę, szczególnie zagrożonych osób i obiektów;
- zwalczanie terroryzmu na statkach, promach i platformach wiertniczych.

Działania specjalne – taktyka „zielona":

- prowadzenie rozpoznania specjalnego, akcji bezpośrednich, wsparcia militarnego i działań towarzyszących;
- ratowanie załóg polskich samolotów, które znalazły się na terenie przeciwnika.

Działania antyterrorystyczne jednostki na obszarach kontrolowanych przez przeciwnika będą osłaniane i wspomagane przez 1. Pułk Specjalny. W ramach taktyki „zielonej", w okresie konfliktu i wojny jednostka może w ograniczonym wymiarze podjąć działania specjalne skierowane głównie na rozpoznanie i niszczenie wybranych obiektów wojskowych. Nabór do „GROM" dokonywany jest głównie spośród kandydatów wywodzących się z jednostek specjalnych Sił Zbrojnych RP oraz wyjątkowo z ochotników zgłaszających się z innych formacji. GROM od początku istnienia jest formacją w pełni zawodową, co jednoznacznie zapewnia najwyższy możliwy w Siłach Zbrojnych stopień wyszkolenia i przygotowania do zróżnicowanych zadań w kraju i poza jego granicami.

GROM jako najlepiej przygotowana i wyszkolona jednostka o najwyższym priorytecie użycia, realizuje operacje wyłącznie o znaczeniu strategicznym oraz o wysokim stopniu ryzyka i trudności, mieszczące się głównie w obszarze taktyki „czarnej".

---

[79] Tamże, s. 79.

Morska Jednostka Działań Specjalnych – „FORMOZA”

Jednostka powstała na bazie utworzonego w 1974 roku, Zespołu Badawczego ds. Płetwonurków Morskich, którego zadaniem było opracowanie koncepcji dla potrzeb sformowania specjalnego dywizjonu płetwonurków morskich. Już rok później, w listopadzie 1975 roku sformowano samodzielną jednostkę. Jej pierwszym dowódcą został kmdr Józef REMBISZ. We wrześniu 1987 roku, jednostka zmieniła nazwę na Wydział Działań Specjalnych, a w roku 1990 powstały Grupy Specjalne Płetwonurków, które następnie przemianowano na Sekcje Działań Specjalnych Marynarki Wojennej. W 2006 roku, jednostka powróciła do pierwotnie stosowanej nazwy Grupy Specjalnej Płetwonurków. Po przejściu w październiku 2007 roku z Marynarki Wojennej w struktury Wojsk Specjalnych, jednostka zmieniła nazwę na Morską Jednostkę Działań Specjalnych (MJDS). Ze względu na wyszkolenie, wyposażenie i tryb działania członkowie jednostki nazywani są często "Polskimi Fokami" i porównywani do Navy Seals, jednostka jest w 100% zawodowa.

Morska Jednostka Działań Specjalnych podobnie jak inne formacje specjalne przygotowana jest do prowadzenia działań w każdym okresie funkcjonowania podmiotu, tzn., w okresie pokoju, kryzysu i wojny. Ze względu na swą specyfikę może być wykorzystana zarówno w operacjach o charakterze wodnym, jak i wodno-lądowym, należy podkreślić , że żołnierze jednostki wyposażeni są w uzbrojenie typowe dla wiodących jednostek specjalnych w świecie. Żołnierze MJDS brali do tej pory udział w akcjach związanych z ochroną polskich statków uczestniczących w operacji irackiej. Najczęściej współdziałają i współpracują z oddziałem morskim jednostki GROM, żołnierzami 1. PSK i podobnymi jednostkami armii państw NATO.

MJDS jest w pełni profesjonalną jednostką sił specjalnych, przygotowaną do prowadzenia działań specjalnych z zakresu taktyki „niebieskiej” z elementami taktyki „czarnej” i „zielonej”.

Do zasadniczych zadań jednostki należy realizacja przedsięwzięć z zakresu operacji specjalnych w środowisku morskim oraz w pasie wybrzeża, w tym specjalnych operacji podwodnych, operacji specjalnych na obiekty pływające, obiekty morskiej infrastruktury technicznej oraz obiekty położone w pasie wybrzeża.

W obszarze zainteresowania jednostki znajdować się będą cele o znaczeniu strategiczno – operacyjnym. Jednocześnie będzie zachowywała podstawowe zdolności do prowadzenia operacji uwalniania zakładników w swoim obszarze odpowie-

działności gdy z uwagi na deficyt czasu lub sytuację operacyjną nie będzie możliwe użycie Jednostki Wojskowej GROM.

Przewiduje się, również użycie elementów jednostki do wsparcia Jednostki Wojskowej GROM w środowisku morskim. Dodatkowo jednostka realizować może specjalistyczne przedsięwzięcia polegające na:

- zabezpieczeniu antyterrorystycznym okrętów wykonujących zadania poza granicami kraju;
- udziale w międzynarodowych morskich operacjach blokadowych;
- współdziałaniu ze Strażą Graniczną w zakresie ochrony morskiej granicy państwa;
- kontroli ruchu na morzu w obszarze zainteresowania.

Jednostka Wsparcia Dowodzenia i Zabezpieczenia Wojsk Specjalnych[80]

Jednostka przeznaczona do realizacji zadań wsparcia informacyjnego, dowodzenia i zabezpieczenia logistycznego operacji specjalnych prowadzonych przez Wojska Specjalne w kraju oraz poza jego granicami, zarówno w układzie narodowym jak i sojuszniczym. Formowanie jednostki rozpoczęto w styczniu 2009 r. Zakłada się, iż pełną zdolność operacyjną jednostka osiągnie w 2015 roku. W połowie 2009 roku jednostka powinna osiągnąć zdolność do prowadzenia gospodarki zgodnie z ustawą o finansach publicznych. W przyszłości pełnić będzie funkcję Wojskowego Oddziału Gospodarczego dla Wojsk Specjalnych.

2.3.4. Żandarmeria Wojskowa

Żandarmeria wojskowa[81] stanowi istotny element systemu antyterrorystycznego istniejącego w Polsce. Formacja ta działa na podstawie ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. nr 123 z 2001 r., poz. 1353 z późn. zm.). Zgodnie z art. 4 ust. 1 ustawy o ŻW ma ona za zadanie pilnować porządku publicznego na terenie obiektów wojskowych oraz w miejscach publicznych, a przy tym ochraniać życie i zdrowie ludzi oraz mienie wojskowe przed zamachami zakłócającymi te dobra. Po szeregu restrukturyzacji i prze-

---

[80] Decyzja Nr Pf 74/Org./SSG/ZOiU-P1 Ministra Obrony Narodowej z dnia 2.12.2008r. w sprawie sformowania Jednostki Wsparcia Dowodzenia i Zabezpieczenia Wojsk Specjalnych.

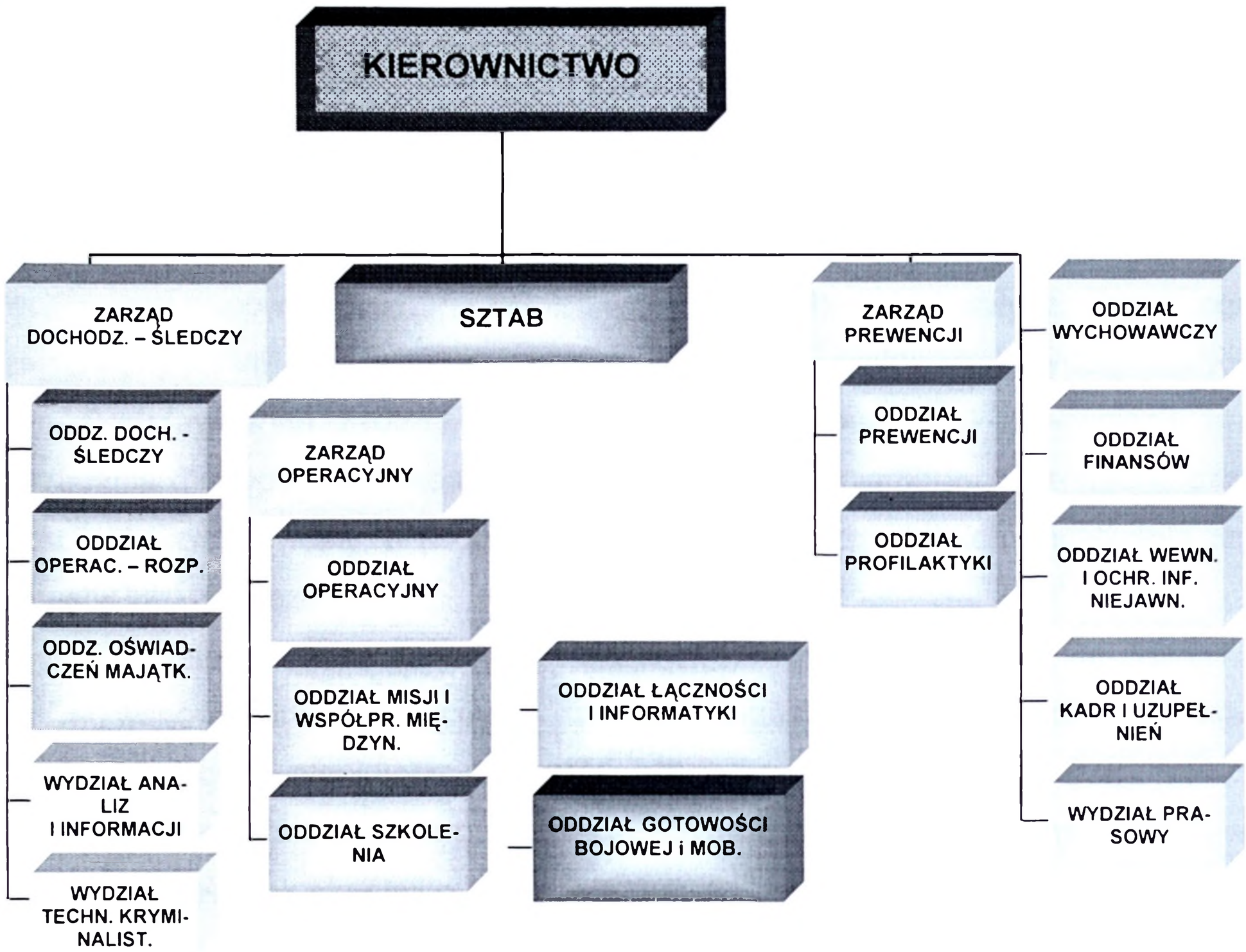
[81] Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. nr 123 z 2001 r., poz. 1353 z późn. zm.)

kształceń Żandarmeria Wojskowa stała się formacją samodzielną. Przez to również zmienił się jej charakter działań. Żandarmeria wykonuje szereg zadań na w zakresie przeciwdziałania terroryzmowi na terenie kraju ale również poza jego granicami. Powstały wyspecjalizowane odłamy tej formacji, które wykonują zadania typowo antyterrorystyczne. Widoczny jest dwupłaszczyznowy podział Żandarmerii. Pierwszy to faktyczne siły i środki działające na terenie terytorium Polski, drugi natomiast to wszelkie siły i środki wydzielane do międzynarodowych oraz wielonarodowych pododdziałów policji

W celu skutecznego zwalczania zjawiska jakim jest terroryzm, ŻW współdziała na podstawie porozumień międzyresortowych z takimi formacjami jak Policja, Straż Graniczna, SOK, Straż Pożarna itp. Ścisła współpraca zapewnia wczesne wykrycie zdarzenia o podłożu terrorystycznym i ewentualne zapobiegnięcie jego rozprzestrzenieniu się.

Żandarmeria Wojskowa jest zorganizowana w określoną strukturę, którą tworzą Komenda Główna oraz terenowe i specjalistyczne jednostki organizacyjne. Ich bieżące funkcjonowanie oraz ewentualne działania w okresie kryzysu i wojny zamierza się realizować się w trzech pionach funkcjonalnych: „dochodzeniowo-śledczym, prewencyjnym i administracyjno – logistyczno – technicznym”[82], zapewniając sprawne kierowanie i dowodzenie, użycie operacyjne oraz zabezpieczenie logistyczne.

[82] Ibid., Art. 8.



Rys. 7. Struktura organizacyjna Żandarmerii Wojskowej. (Źródło na podstawie materiałów z Komendy Głównej Żandarmerii Wojskowej w Warszawie)

Żandarmeria Wojskowa wykonuje zadania przede wszystkim na obszarze kraju, jednak może realizować je poza granicami państwa w stosunku do żołnierzy oraz pracowników polskich, zatrudnionych za granicą w polskich jednostkach i przedstawicielstwach wojskowych. Współdziała z dowódcami rodzajów sił zbrojnych i wszystkich jednostek wojskowych oraz z większością instytucji zajmujących się bezpieczeństwem państwa, (w tym z MSWiA) przestrzeganiem prawa i porządku, a także bezpieczeństwem i ochroną ludności. Rangę i znaczenie tych działań oraz nadanie określonych uprawnień żandarmom kierowanym do pomocy Policji, określono między innymi w „ustawie o Policji art.18 i 18a”[83].

Pion **dochodzeniowo-śledczy** w Żandarmerii Wojskowej jest właściwym w zakresie działalności dochodzeniowej, śledczej i operacyjno – rozpoznawczej, a także ujawniania przestępstw i wykroczeń oraz ścigania ich sprawców (sprawców podlega-

[83] Ustawa o policji wyd. cyt.

jących orzecznictwu sądów wojskowych). Realizuje także przedsięwzięcia profilaktyczne oraz rozpoznanie przesłanek i zagrożeń przestępczością ukrytą o charakterze kryminalnym i zorganizowanym.

Pion **Prewencji** jest właściwym w zakresie: szeroko rozumianej działalności prewencyjnej i profilaktycznej, w tym czynności patrolowych, asystencyjnych, konwojowych i kontroli ruchu drogowego, a także koordynowania zabezpieczeń uroczystości z udziałem wojska, przegrupowań, ćwiczeń i szkoleń wojsk własnych i sojuszniczych, wizyt delegacji zagranicznych i VIP oraz wydawania pozwoleń na broń prywatną żołnierzy zawodowych.

Podstawowym zadaniem Żandarmerii Wojskowej jest zapewnienie przestrzegania dyscypliny wojskowej, bezpieczeństwa i porządku publicznego w czasie pokoju, kryzysu i wojny, a także interweniowania w przypadkach popełniania przestępstw lub wykroczeń[84].

Do kolejnych zadań Żandarmerii Wojskowej należą:

- wspomaganie dowódców w dziedzinie przestrzegania dyscypliny wojskowej i przeciwdziałaniu przestępczości, w tym przestępczości skarbowej;
- ochranianie porządku publicznego zarówno w jednostkach i instytucjach wojskowych jak również w miejscach publicznych;
- udział w tworzeniu – szeroko rozumianych – warunków do realizacji zadań bojowych;
- **udział w zwalczaniu sytuacji kryzysowych wynikłych z zagrożeń niemilitarnych.**

Żandarmeria Wojskowa jest formacją, która cały czas się rozwija nie tylko pod względem militarnym ale również w kierunku działalności niemilitarnej, która polega na ścisłej współpracy z innymi organami państwowymi uczestniczącymi w NSPK. Świadczy o tym fakt, że bierze ona udział szeregu ćwiczeń jakie są organizowane na szczeblu krajowym w ramach Systemu Reagowania Kryzysowego.

Udział jednostek ŻW w zapobieganiu i eliminowaniu sytuacji kryzysowych, w tym zagrożeniach terrorystycznych

Udział jednostek ŻW, oraz zakres ich działania wynika z zadań antykryzysowych jakie są realizowane przez tą formację SZ RP w przypadku zaistnienia sytuacji kryzysowej. Do głównych zadań należą[85]:

---

[84] Ustawa z dnia 24. 08. 2001r. o Żandarmerii Wojskowej i wojskowych organach porządkowych.

[85] „Plan użycia ŻW w przypadku wystąpienia sytuacji kryzysowych".

1) **współdziałanie z RSZ, DO, IWSZ, SG, Policją oraz innymi militarnymi i niemilitarnymi podmiotami bezpieczeństwa państwa, w zakresie przeciwdziałaniu zagrożeniom terrorystycznym, w tym również typu „RENEGADE", osłonie i izolacji obiektów szczególnie ważnych dla bezpieczeństwa i obronności państwa, zabezpieczeniu usuwania skutków sytuacji kryzysowych;**
2) wsparcie specjalistycznymi siłami i środkami podmiotów biorących udział w realizacji zadań zapobiegania, zwalczania, likwidacji skutków tych sytuacji kryzysowych;
3) zabezpieczenie pod względem prewencyjnym i dochodzeniowo – śledczym działania wojsk (w tym wojsk sojuszniczych NATO) realizujących zadania w związku z zaistniałą sytuacją kryzysową;
4) zapewnienie przestrzegania prawa i porządku publicznego w rejonie wystąpienia sytuacji kryzysowej;
5) udział w akacjach i działaniach:
   - poszukiwawczo ratowniczych;
   - ratowniczo - gaśniczych i usuwania skutków pożarów przestrzennych;
   - przeciwepidemicznych;
   - likwidacji skutków awarii technicznych i wypadków radiacyjnych;
   - odśnieżania;
   - zwalczania powodzi zjawisk lodowych.

Powyższe zadania ŻW realizuje w trzech fazach[86] :

- faza I – monitorowanie sytuacji w ramach działalności bieżącej;
- faza II – aktywacja sił i środków, reagowanie;
- faza III – usuwanie skutków.

W fazie I Żandarmeria Wojskowa[87]:

1) uświadamia stanom osobowym, poprzez szereg spotkań, wykładów i pokazów w jednostkach organizacyjnych SZ RP, możliwe rodzaje zagrożeń, ich źródła i przewidywane skutki, a także kształtuje pożądane zachowania i reakcje na mogące powstać zagrożenia;

---

[86] Ibid.
[87] Opracowano na podstawie materiałów dostępnych z KGŻW.

2) prowadzi, we współdziałaniu z wyspecjalizowanymi instytucjami, pracę operacyjno - rozpoznawczą nakierowaną na zdobywanie informacji o potencjalnych i realnych zagrożeniach;
3) utrzymuje w aktualności dokumentacje planistyczną dotyczącą udziału w zapobieganiu, zwalczaniu, likwidacji skutków sytuacji kryzysowych;
4) przygotowuje wydzielone siły do podjęcia natychmiastowych działań ochronno-obronnych, ratowniczych i wspierających;
5) monitoruje i na bieżąco ocenia sytuację na świecie, w Europie, w RP oraz SZ RP;
6) prowadzi wymianę informacji z militarnymi i niemilitarnymi podmiotami bezpieczeństwa państwa w zakresie możliwości wystąpienia potencjalnych i realnych zagrożeń;
7) utrzymuje, w stałej gotowości, system ostrzegania i alarmowania stanów osobowych podległych jednostek organizacyjnych;
8) aktywuje, w zależności od potrzeb, system zarządzania kryzysowego;
9) realizuje szkolenie, wydzielonych do realizacji zadań antykryzysowych określonych sił .

W fazie II kontynuowana jest realizacja zadań fazy I, a ponadto[88]:

1) ostrzegane i alarmowane są stany osobowe własnych jednostek oraz jednostek i instytucji zarówno MON jak i podsystemu niemilitarnego;
2) przygotowuje się do użycia niezbędne siły i środki;
3) przystępuje do przeciwdziałania sytuacjom kryzysowym we współdziałaniu z siłami innych podmiotów bezpieczeństwa i porządku publicznego państwa w zakresie:
   - zapewnienia przestrzegania prawa i porządku publicznego w rejonie wystąpienia sytuacji kryzysowej,
   - zabezpieczenia pod względem prewencyjnym i dochodzeniowo – śledczym działania wojsk realizujących zadania w związku z zaistniałą sytuacją kryzysową,
   - wzmocnienia systemu ochrony kluczowych osób i obiektów pozostających w jurysdykcji resortu ON;
4) planowana jest realizacja zadań w ramach wsparcia państwa-gospodarza (HNS);

---

[88] Ibid.

5) prowadzone są (wg potrzeb) poszukiwania sprawców przestępstw oraz zaginionych żołnierzy, biorących udział w akcji antykryzysowej a także utraconej broni, amunicji, materiałów wybuchowych i innego mienia wojskowego;
6) przygotowuje się i kieruje do działań kolejne, niezbędne siły i środki oraz dokonuje ich rotacji, tym również siły do przekazania w podporządkowanie Dowódcy Operacyjnemu;
7) wysyła się do SzK MON oraz do Wojewódzkich Zespołów Zarządzania Kryzysowego (WZZK), oficerów łącznikowych ŻW;
8) realizuje się przedsięwzięcia zapewniające zwiększenie bezpieczeństwa własnym stanom osobowym i obiektom;
9) monitorowane są zagrożenia w dyscyplinie wojskowej oraz przestępczością w rejonach objętych kryzysem.

W fazie III Żandarmeria Wojskowa realizuje zadania fazy II oraz[89]:

1) aktywuje, w zależności od potrzeb, do udziału w likwidacji skutków sytuacji kryzysowych, inne siły nie ujęte w żadnych planach reagowania kryzysowego zachowując ciągłość realizacji innych zadań nie związanych z likwidacją skutków sytuacji kryzysowej;
2) po zakończeniu realizacji zadań ,we współdziałaniu z Policją, zabezpiecza pod względem prewencyjnym przegrupowanie użytych pododdziałów SZ RP do macierzystych garnizonów;
3) odtwarza zdolność bojową sił, zaangażowanych w działania antykryzysowe, oraz dokonuje rozliczeń finansowych z właściwymi władzami, na wniosek których użyto siły ŻW;
4) opracowuje i przedstawia do zapoznania właściwym przełożonym szczegółowe sprawozdania z realizacji zadań.

Ponadto Żandarmeria wojskowa w ramach funkcjonowania w NSPK jako jeden z Elementów Reagowania Kryzysowego, realizuje szereg przedsięwzięć, które są przewidziane dla poszczególnych stopni alarmowych: ALFA, BRAVO, CHARLIE, DELTA.

---

[89] Ibid.

1) Pierwszy stopień alarmowy „ALFA”[90]

Jego wprowadzenie ma charakter ogólnego ostrzeżenia przed możliwymi działaniami terrorystycznymi, których rodzaj i zasięg są nieprzewidywalne, a okoliczności nie usprawiedliwiają pełnego wprowadzenia przedsięwzięć zawartych w wyższych stopniach alarmowych. Łącznie z tym stopniem alarmowym mogą zostać wprowadzone określone przewidziane dla wyższych stopni alarmowych.

Realizuje się w nim następujące przedsięwzięcia:

- żołnierze oraz pracownicy wojska są informowani o konieczności zachowania wzmożonej czujności w stosunku do osób obcych, posiadających (wnoszących) podejrzane przedmioty,
- informuje się odpowiednie służby SKW, Policję, w przypadku zauważenia: nieznanych pojazdów na terenie jednostek organizacyjnych ŻW lub innych ważnych obiektów o porzuceniu na ich terenie paczek i bagaży lub gdy zaobserwuje się jakichkolwiek inne oznaki nietypowej działalności,
- kluczowe osoby funkcyjne w jednostkach organizacyjnych ŻW, niezbędne do wprowadzenia w życie planów ochrony bezpieczeństwa zachowują gotowość do stawiennictwa w miejscu pracy i podjęcia działań „uchwytni telefonicznie o każdej porze dnia i nocy”,
- budynki, pokoje, sejfy, szafy i innego rodzaju schowki, które nie są regularnie użytkowane, zostają zamknięte i zabezpieczone,
- przeprowadzane są wzmożone kontrole pojazdów oraz osób wchodzących na teren jednostek ŻW oraz ogranicza się ruch pojazdów i osób do niezbędnego minimum,
- obiekty (budynki, pomieszczenia) będące w stałym użyciu są regularnie sprawdzane na zewnątrz i od wewnątrz pod względem podejrzanej działalności osób postronnych oraz w poszukiwaniu podejrzanych przedmiotów ponadto sprawdzane są wszelkiego rodzaju dostawy zaopatrzenia do klubów, stołówek żołnierskich oraz innych obiektów zajmujących się działalnością usługową na rzecz ŻW,
- w miarę dostępności środków powadzona jest wzmożona kontrola miejsc dużych skupisk ludzkich, obiektów użyteczności publicznej, ważnych obiektów cywilnych i wojskowych oraz innych potencjalnych pozamilitarnych

---

[90] Ibid.

obiektów ataku, w celu wzmocnienia środków zapobiegania, ochrony i zwiększenia zaufania wśród żołnierzy i pracowników wojska ŻW i ich rodzin,

- dokonuje się przeglądu wszystkich dokumentów planistycznych, rozkazodawczych dotyczących podwyższania gotowości do podjęcia działań antykryzysowych.

2) Drugi stopień alarmowy „BRAVO”[91]

Stopień ten jest wprowadzany w przypadku zaistnienia zwiększonego i „bardziej przewidywalnego” zagrożenia działalnością terrorystyczną lub aktem sabotażu, jednakże konkretny cel ataku nie został zidentyfikowany. Łącznie z drugim stopniem alarmowym mogą być zadeklarowane przedsięwzięcia reagowania kryzysowego stopni alarmowych: CHARLIE, DELTA. Przedsięwzięcia przewidziane do realizacji obejmują swoim zakresem stopień alarmowy „ALFA” a ponadto:

- żołnierzy i pracowników wojska ostrzega się o możliwych formach i metodach ataku, których potencjalnie mogą zastosować terroryści i sabotażyści;
- odsuwa się na co najmniej kilkadziesiąt metrów, samochody oraz takie obiekty jak: kontenery, pojemniki na śmieci itp., od budynków, a zwłaszcza od budynków o szczególnie wrażliwym lub prestiżowym charakterze. Ponadto wprowadza się, w zależności od możliwości, system scentralizowanego parkowania pojazdów służbowych,
- poddaje się wzmożonej kontroli wszystkie przesyłki pocztowe. W ramach tego przedsięwzięcia prowadzi się szkolenia dla kadry i pracowników wojska, podczas których przypomina się, aby również członkowie ich rodzin dokonywali sprawdzenia wszelkich dostaw do miejsca zamieszkania,
- informuje się żołnierzy i pracowników wojska ŻW oraz ich rodziny o ogólnej sytuacji, tak aby nie dopuścić do powstawania plotek oraz zapobiec panice,
- niezwłocznie powiadamia się lokalne organy bezpieczeństwa i porządku publicznego, z zachowaniem zasad ochrony informacji niejawnych, o wszelkich podjętych działaniach (wprowadzonych ograniczeniach i podjętych środkach ostrożności)i ich przyczynach ich wprowadzenia,

---

[91] Opracowano na podstawie materiałów dostępnych z KGŻW.

- w miarę posiadanych sił środków, wprowadza się nieregularne patrole, odpowiednio przygotowane, wyszkolone i wyposażone do kontrolowania pojazdów, ludzi oraz budynków,
- poucza się kierowców o konieczności zamykania na zaparkowanych pojazdów oraz o przeprowadzaniu kontroli pojazdu przed wejściem do samochodu i jego uruchomieniem.

3) Trzeci stopień alarmowy „CHARLIE”[92]

Stopień alarmowy CHARLIE ma zastosowanie w przypadku konkretnego zdarzenia lub, kiedy informacje służb wywiadu wskazują na istnienie bezpośredniego zagrożenia jakąś formą ataku terrorystycznego lub akcji sabotażowej. Wszystkie przedsięwzięcia stopnia alarmowych: ALFA i BRAVO są kontynuowane natomiast te, które dotąd nie były wprowadzone, wprowadza się niezwłocznie a ponadto:

- wszystkie osoby funkcyjne odpowiedzialne za wprowadzanie planów działań na wypadek aktów terroru lub sabotażu pełnią dyżur na wyznaczonych stanowiskach w miejscu pracy,
- ogranicza się, do absolutnego minimum, liczbę miejsc wstępu do określonych rejonów (obszarów) będących w jurysdykcji ŻW,
- przy wejściu na teren obiektów ZW się ścisłe kontrole oraz wyrywkowe kontrole samochodów,
- wzmacnia się system ochrony jednostek organizacyjnych ŻW m.in. poprzez zwiększenie częstotliwości patrolowania obiektów oraz wydania obsadom służb dyżurnych dodatkowych środków przymusu bezpośredniego i środków ochrony osobistej,
- miejsca podlegające szczególnej ochronie, nadzoruje się w trybie całodobowym oraz nieustannie monitorowane są miejsca znajdujące się poza obiektami znajdujące się w ich najbliższym otoczeniu,
- minimalizuje się obecność, w miejscu pracy pracowników wojska.

4) Czwarty stopień alarmowy „DELTA”[93]

---

[92] Ibid.

Najwyższy stopień alarmowy ma zastosowanie bezpośrednio na obszarze, na którym miał miejsce atak terrorystyczny lub akt sabotażu lub, jeżeli informacje wywiadowcze stwierdzają wysokie prawdopodobieństwo ataku w konkretnym miejscu.

W tym stopniu wprowadzone lub kontynuowane są wszystkie przedsięwzięcia dla pierwszego, drugiego i trzeciego stopnia alarmowego, a ponadto:

- przeprowadza się identyfikację wszystkich pojazdów znajdujących się już na terenie pozostającym w jurysdykcji ŻW, przeszukuje się wszystkie pojazdy wjeżdżające na ich teren, w tym również szczegółowej kontroli poddany zostaje ich ładunek oraz wprowadza pełną kontrolę dostępu do tych obiektów,
- ogranicza się do niezbędnego minimum wszelkie służbowe podróże i wizyty żołnierzy i pracowników wojska ŻW,
- przeprowadza się konsultacje z lokalnymi władzami państwowymi i samorządowymi w sprawie możliwości zamknięcia dróg publicznych oraz rejonów (obszarów) szczególnie wrażliwych na atak terrorystyczny lub akt sabotażu, zwłaszcza tych, które znajdują się w bezpośredniej styczności z obiektami ŻW.

Wszystkie zadania jakie realizuje Żandarmeria Wojskowa w poszczególnych stopniach alarmowych muszą być prowadzone na najwyższym poziomie profesjonalizmu, ponieważ dotyczą przede wszystkim działań o charakterze sabotażowym i terrorystycznym. Działania terrorystyczne mają charakter trudno przewidywalny (pełzający). Aby można było im skutecznie przeciwdziałać Żandarmeria Wojskowa musi ściśle współpracować z innymi jednostkami Wojsk Lądowych, Marynarki Wojennej oraz Sił Powietrznych. W ŻW na zwalczanie aktów terroru i sabotażu kładzie się duży nacisk. Świadczy o tym fakt, że funkcjonowanie Oddziałów Specjalnych ŻW (OSŻW) opiera się głównie na działaniach antyterrorystycznych.

Wobec nowo powstałych zagrożeń zaistniała koncepcja transformacji Sił Zbrojnych RP, a co za tym idzie przygotowania wojsk (w tym również ŻW) do realizacji nowych zadań. W związku z tym w 2002 roku pojawiła się myśl utworzenia Oddziałów Specjalnych Żandarmerii Wojskowej (OSŻW), jako wysoce wyspecjalizowanej formacji.

Podstawowym złożeniem koncepcji utworzenia OSŻW była konieczność sformowania mobilnych, wyposażonych i wyszkolonych zgodnie ze standardami NATO

---

[93] Ibid.

jednostek ŻW, które skutecznie mogą działać także jako element wsparcia policyjnego jednostek operacyjnych SZ RP na terenie kraju jak również poza jego granicami. Oddziały Specjalne miały by wspierać również działania Policji w sytuacjach kryzysowych.

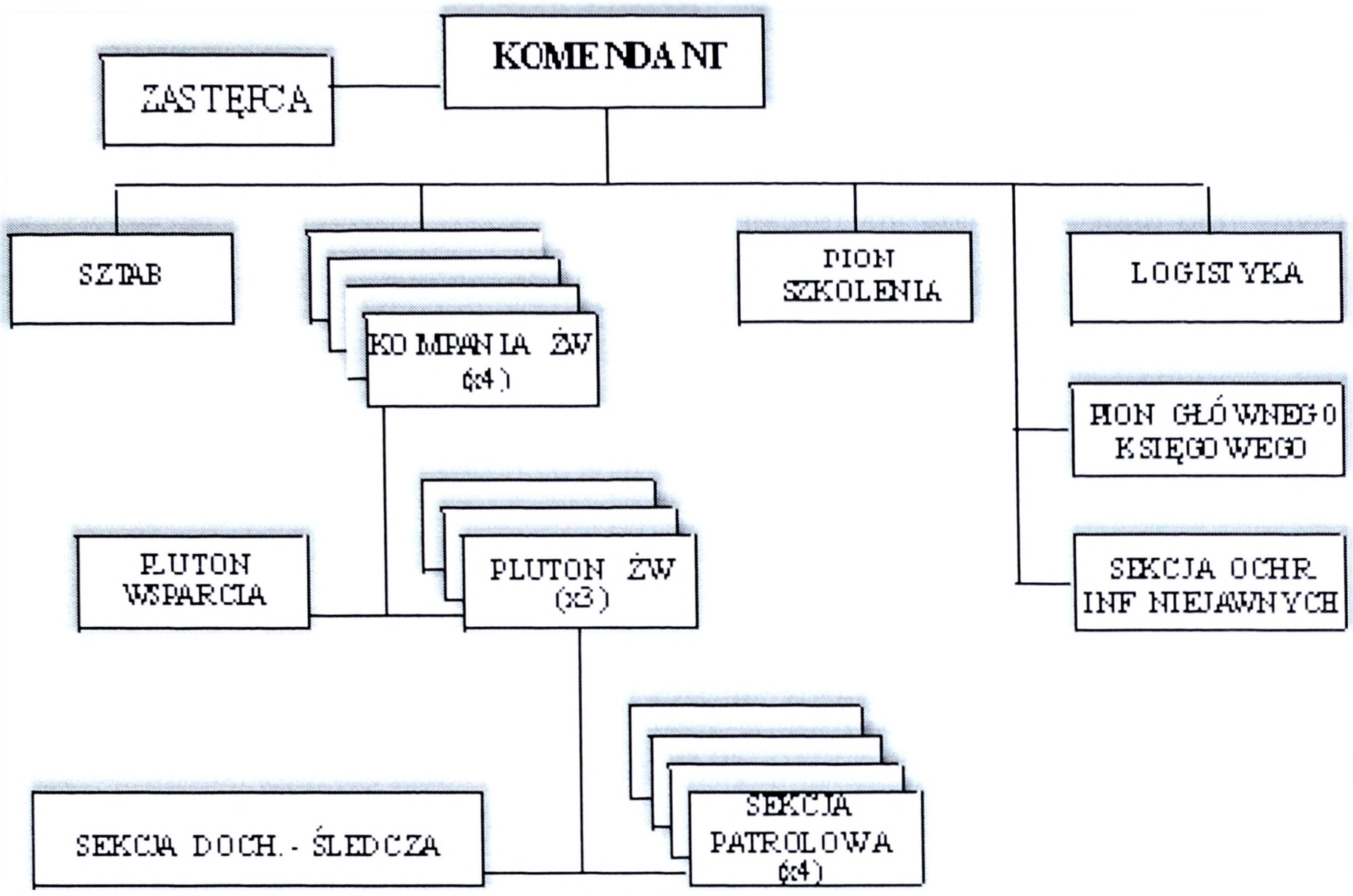
„Na podstawie zarządzenia Ministra Obrony Narodowej z dnia 28.10.2004 r. utworzono trzy Oddziały Specjalne ŻW stacjonujące w Mińsku Mazowieckim, Gliwicach i w Warszawie. Jednostki te są szkolone i wyposażone zgodnie z wymaganiami określonymi dla sił policji wojskowych wykorzystywanych w połączonych operacjach NATO. Oddziały specjalne liczą ok. 1500 żołnierzy zawodowych, co stanowi prawie 40% całego potencjału osobowego Żandarmerii Wojskowej. Operacyjne użycie tych jednostek, w zależności od mandatu misji, zadań oraz warunków lokalnych, może odbywać się całością sił lub częściami (samodzielnymi modułami)"[94].

Przy tworzeniu OS ŻW kierowano się następującymi przesłankami:

- *„relatywnie małym kosztem ich utworzenia;*
- *pełną profesjonalizacją;*
- *stosownym do przewidywanych zadań wyszkoleniem, uzbrojeniem i wyposażeniem;*
- *dużą mobilnością i zdolnością do natychmiastowego przerzutu w rejon operacji;*
- *posiadaniem ustawowych uprawnień policyjnych;*
- *modułową strukturą organizacyjną, umożliwiającą tworzenie pododdziałów odpowiednio do potrzeb misji czy operacji (podstawowym modułem będzie pluton ŻW w składzie czterech sześcioosobowych sekcji patrolowych i jednej sekcji dochodzeniowo-śledczej)"*[95].

---

[94] Na podstawie materiałów udostępnionych przez Komendę Główną Żandarmerii Wojskowej.
[95] Ibid.



Rys. 8. Struktura organizacyjna Oddziału Specjalnego ŻW. (Źródło na podstawie materiałów z Komendy Głównej Żandarmerii Wojskowej w Warszawie).

Oddziały Specjalne Żandarmerii Wojskowej wykonują zadania w obszarach, które są określone art. 3 i 4 ustawy z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych, jak również realizują szereg zadań dodatkowych:

- *realizowanie zadań wsparcia oddziałów Sił Zbrojnych RP i sił MSWiA dotyczących działań przeciwko terroryzmowi, a także związanych z ochroną obiektów i instalacji ważnych dla bezpieczeństwa Państwa oraz zapobieganiem klęskom żywiołowym i likwidacją ich skutków w przypadku wystąpienia sytuacji kryzysowych;*
- *zapewnienie w ramach HNS wsparcia policyjnego wojsk sojuszniczym na terytorium RP;*
- *realizacja zadań wynikających z „Celów Sił Zbrojnych NATO" i „Wymagań Długoterminowych dla RP";*
- *prowadzenie szkoleń i kursów specjalistycznych na potrzeby ŻW"*[96].

[96] Art.3 i 4 ustawy z dnia 24 sierpnia 2001r.o ŻW i wojskowych organach porządkowych.

Podstawę i zakres użycia oddziałów specjalnych ŻW na terenie kraju określa ustawa o żandarmerii wojskowej oraz znowelizowana ustawa o policji, która w art. 18a.1 stanowi, że „w razie zagrożenia bezpieczeństwa i porządku publicznego, gdy siły Policji są niewystarczające do wykonania ich zadań w zakresie ochrony bezpieczeństwa i porządku publicznego, Prezes Rady Ministrów, na wniosek ministra właściwego do spraw wewnętrznych uzgodniony z Ministrem Obrony Narodowej, może zarządzić użycie żołnierzy Żandarmerii Wojskowej do udzielenia pomocy Policji"[97].

Z kolei w art.18.1 ustawy o Policji wyszczególniono sytuacje, w których do pomocy policji mogą zostać użyci żołnierze ŻW.

Są to sytuacje mogące stanowić:

- *„zagrożenie bezpieczeństwa powszechnego dla życia, zdrowia lub wolności obywateli;*
- *bezpośrednie zagrożenia dla mienia w znacznych rozmiarach;*
- *bezpośrednie zagrożenie obiektów i instalacji mających szczególne znaczenie dla obronności lub bezpieczeństwa państwa;*
- *zagrożenie przestępstwem o charakterze terrorystycznym bądź jego dokonanie"*[98].

[97] Art. 18a.1 ustawy o policji.
[98] Art.18.1 ustawy o policji.

3. ANALIZA I OCENA ORAZ ZARZĄDZANIE RYZYKIEM W SYSTEMIE CYWILNO – WOJSKOWEJ OCHRONY MIAST POLSKICH W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH

3.1. Analizy podatności na zagrożenia terrorystyczne w miastach polskich

W wielu krajach po 11 września 2001 r. zintensyfikowano prace nad podniesieniem poziomów bezpieczeństwa w miastach, a przede wszystkim ważnych obiektów infrastruktury krytycznej w odniesieniu do potencjalnych aktów terrorystycznych i sabotażu.

W wyniku wzrastającego zagrożenia związanego z aktami terroru i sabotażu zintensyfikowano działania na rzecz podwyższenia poziomu bezpieczeństwa w miastach w aspekcie ochrony przed działaniami niepożądanymi.

Głównym celem oceny ryzyka na potrzeby zarządzania w ochronie miast polskich przed zagrożeniami terrorystycznymi jest wyznaczenie najbardziej prawdopodobnych zdarzeń powodujących sytuację kryzysową.

Sposób zwiększenia bezpieczeństwa w kontekście zagrożeń terrorystycznych jest uwarunkowany wieloma czynnikami, główne z nich to:

rodzaj zagrożenia,

- stopień podatności różnych elementów na poszczególne działania niepożądane,
- możliwe skutki wypadków, awarii czy ataków,
- a także „atrakcyjność" niektórych elementów infrastruktury (najbardziej strategicznych) dla stron trzecich.

W przypadku zagrożenia terrorystycznego, punktami krytycznymi - najbardziej narażonymi na atak, są elementy strategiczne dla funkcjonowania miasta, a zwłaszcza takie, których awaria spowoduje zatrzymanie pracy znacznej części instalacji oraz elementy, których awaria spowoduje jak największe skutki dla środowiska i pobliskiej ludności. Kluczowym elementem systemu bezpieczeństwa w kontekście zagrożeń terrorystycznych jest przygotowanie i wdrożenie analiz podatności SVA (Security Vulnerability Analysis). Jest to proces analityczny, w którym wyznacza się typy i warunki dla potencjalnych zagrożeń terrorystycznych i sabotażowych, prawdopodobieństwa skutków oraz możliwe ich następstwa.

Wyznaczenie priorytetów i oszacowanie wrażliwości obiektów na oddziaływanie

terrorystów jest jednym z głównych zadań i problemów osób odpowiedzialnych za bezpieczeństwo w miastach.

W tym celu należy:

- przeprowadzić szereg działań, które pozwolą zidentyfikować potencjalne zagrożenia (włączając atak terrorystyczny), a następnie określić prawdopodobieństwa wystąpienia danego zdarzenia, środki zapobiegawcze oraz ewentualne skutki.
- wprowadzić w życie środki bezpieczeństwa współmierne z ryzykiem zidentyfikowanym w oszacowaniach;
- chronić informacje i dane (bezpieczeństwo w sieci); trenować, ćwiczyć, prowadzić szkolenia w zakresie bezpieczeństwa dla służb odpowiedzialnych za bezpieczeństwo by zwiększyć ich świadomość i zdolność do trzeźwego reagowania w sytuacjach kryzysowych;
- mieć łączność informacji, ciągły system wymiany danych; reagować i odpowiadać na potencjalne zagrożenia- informować o zagrożeniach personel i opinię publiczną;
- umożliwiać prowadzanie kontroli bezpieczeństwa przez zespoły ekspertów z zewnątrz.

Istnieje wiele materiałów wspomagających przeprowadzenie analiz podatności na zagrożenia terrorystyczne instalacji stacjonarnych, przesyłowych, systemów cyfrowych zabezpieczeń i komunikowania obsługujących takie instalacje.

Do takich materiałów należą przewodniki opracowane w: Center for Chemical Process Safety SVA, CCPS Eqiuvalent Methods (ExxonMobil Chemical, BASF, Air Products, Georgia Pacific), Sandia National Lab VAM-CF.

Wszystkie te metodologie zalecają przeprowadzanie analiz w następujących etapach:

- opracowanie planu projektu analiz podatności,
- scharakteryzowanie potencjalnych miejsc zagrożonych,
- zidentyfikowanie zagrożeń,
- przeprowadzenie analiz wrażliwości,
- określenie środków zaradczych.

W poniższej pracy przedstawiono metodę analizy i zarządzania bezpieczeństwem SVA opracowaną przez CCPS (Center for Chemical Process Safety) w USA.[99]

Podstawowe definicje stosowane w analizach SVA.

SVA (Security Vulnerability Analysis) jest procesem określającym prawdopodobieństwo wystąpienia niepożądanego zdarzenia, opartym na analizie wrażliwości oraz szacującym zasięg szkód. SVA wykorzystuje głównie analizy jakościowe w celu określenia stanu bezpieczeństwa systemu.

Wynikiem analiz jest uzyskanie listy rankingowej celów najbardziej zagrożonych atakiem ze strony terrorystów, na podstawie której podejmowane są decyzje o środkach zaradczych. Oszacowanie wrażliwości danego celu na atak jest zadaniem trudnym, gdyż jest to obiektywny proces oszacowywania subiektywnych osądów ekspertów.

Skutki (Consequences):

- rozpatrywane w SVA mogą różnić się wielkością, charakterem i zakresem od skutków rozważanych w standardowych analizach ryzyka;
- w analizach przyjmuje się z reguły, że terrorysta chce zmaksymalizować szkodę i zaatakować cel, który jest dość łatwo dostępny;
- skutki niepożądanego działania rozważa się w kilku kategoriach: wpływ na zdrowie ludzkie, straty finansowe czy negatywne oddziaływanie na środowisko zewnętrzne.

Zagrożenie (Threat):

- w ramach SVA zagrożenie jest definiowane jako okoliczność, mogąca spowodować utratę lub zniszczenie dóbr materialnych i/lub straty w ludziach i w środowisku. Może być zdefiniowane jako zamiar lub zdolność terrorysty do przedsięwzięcia działań powodujących szkody dla środowiska i zdrowia ludzkiego;
- źródłem zagrożenia może być: inny rząd, niezadowolony pracownik albo kontrahent, kryminalista, gwałtowny aktywista, terrorysta (polityczny, religijny, środowiskowy).

---

[99] Center for Chemical Process Safety SVA, CCPS Equivalent Methods (ExxonMobil Chemical, BASF, Air Products, Georgia Pacific), Sandia National Lab VAM-C F: Guidelines for analyzing and managing the security vulnerabilities of fixed chemical sites, New York, August 2002

Podatność (Vulnerability):

- jest zdefiniowana jako słabe rozwiązania organizacyjne, które mogą być wykorzystane przez strony nieupoważnione dla wyrządzenia szkód. Podatność na atak może wynikać z niewłaściwego zabezpieczenia obiektów czy też z innych czynników operacyjnych.

Atrakcyjność celu: może wynikać z wielkości i rodzaju szkody jaką może spowodować zaatakowanie danego celu.

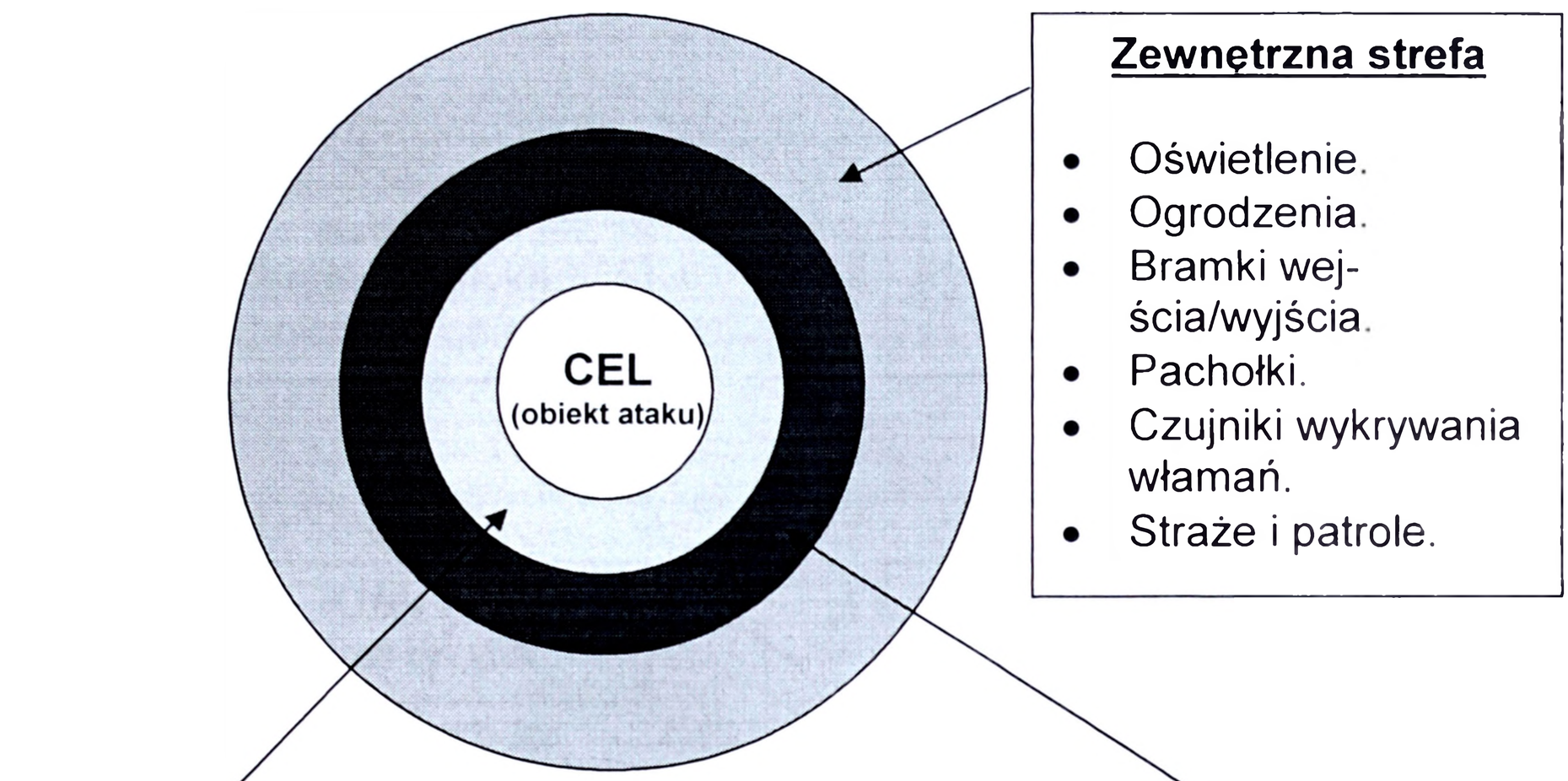
- Nie wszystkie cele są jednakowo atrakcyjne dla terrorysty, co ma znaczący wpływ na określenie prawdopodobieństwa ataku na dany element w mieście.

Środki zaradcze:

- są działaniami podjętymi w celu zmniejszenia albo wyeliminowania jednej/kilku słabych cech w infrastrukturze miasta. Środki zaradcze obejmują sprzęt komputerowy, systemy techniczne, oprogramowanie, procedury i kontrole. Podczas analiz SVA środki zaradcze wybiera się na podstawie oceny ich dostępności, efektywności działania, niezawodności;
- do środków zaradczych można zaliczyć: bezpieczeństwo fizyczne, kontrolę dostępu, zapobieganie stratom, zarządzanie w sytuacjach kryzysowych i awaryjnych, politykę bezpieczeństwa w tym procedury postępowania, bezpieczeństwo sieciowe i bezpieczeństwo danych.

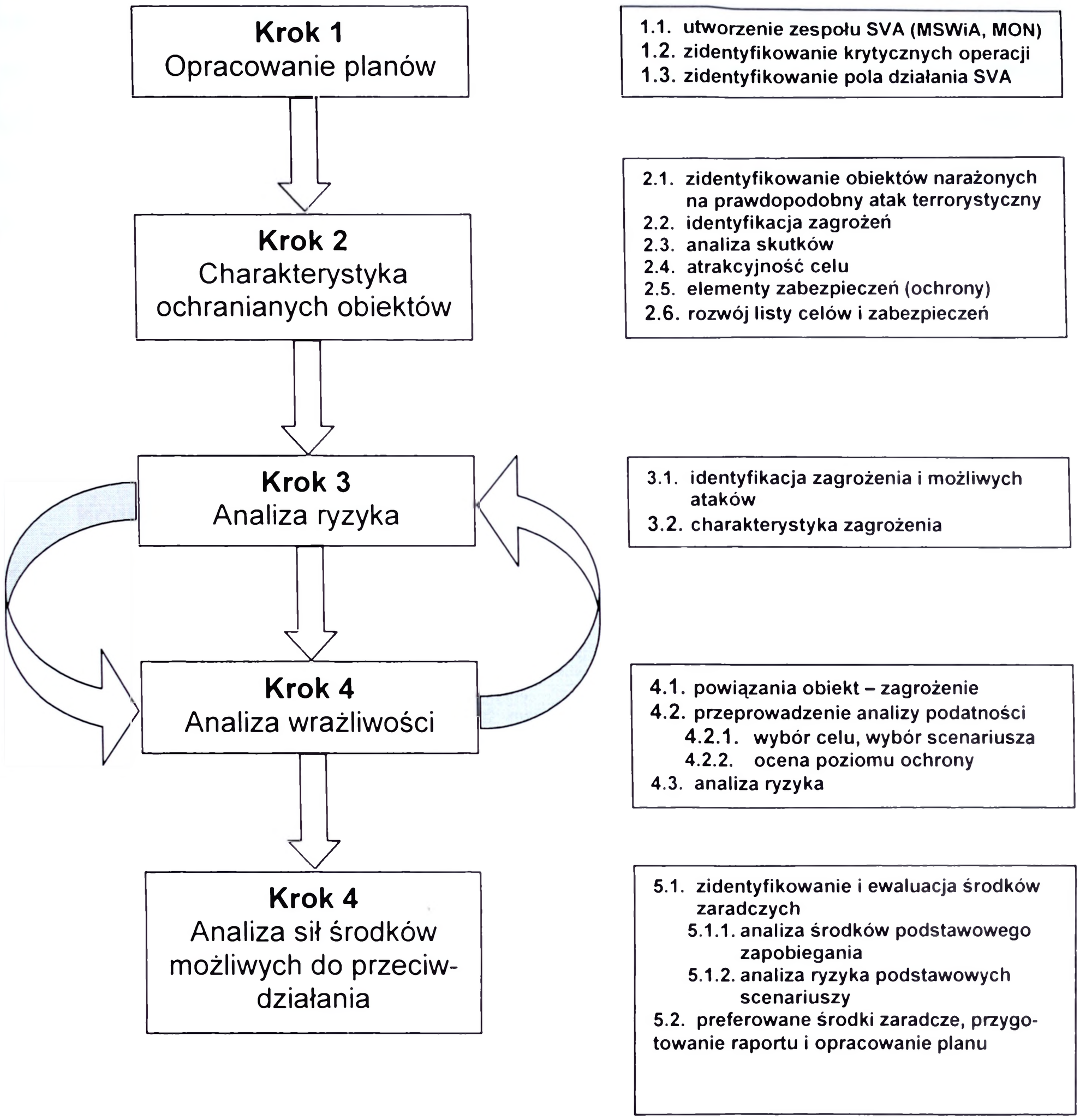
Redukcja ryzyka działań terrorystycznych może być prowadzona poprzez zapobieganie, detekcję i opóźnianie działań terrorysty (DDD - Deter, Detect and Delay), tworzenie fizycznych i cybernetycznych stref i pierścieni ochronnych, odpowiednią taktykę i procedury działania, czy też stosowanie systemów i technologii naturalnie bezpiecznych (rys. 9.) [100].

[100] Tamże



Rys. 9. Elementy zabezpieczeń przed nieupoważnionymi działaniami stron trzecich (Opracowanie na podstawie prezentacji M. Borysiewicz, I. Garanty, A. Kozubal, S.Potempski nt „Analizy podatności na zagrożenia dla instalacji stacjonarnych i rurociągów" Szkoła tematyczna „Zarządzanie Zagrożeniami dla Zdrowia i Środowiska" 26-30.09.2005)

WYMAGANE KROKI SVA[101]



Rys. 10. Wymagane kroki SVA podczas analizy sił i środków do przeciwdziałania zagrożeniom terrorystycznym miast polskich

Krok 1: Planowanie procesu SVA:

Planowanie SVA wymaga określenia celów i zakresu analiz. Najważniejsza w tym kroku jest identyfikacja krytycznych operacji i zakresu działań.
Ważny jest również wybór i utworzenie zespołu SVA.

---

[101] Center for Chemical Process Safety SVA.....Wyd. cyt.

Krok 2: Charakterystyka ochranianych obiektów.

Krok ten obejmuje charakterystykę elementów najbardziej potencjalnych ataków oraz listę celów i zabezpieczeń. Krok ten obejmuje również ocenę środków zaradczych podejmowanych w razie zaistnienia ataku terrorystycznego. Po zidentyfikowaniu zabezpieczeń i określeniu atrakcyjności celów ustala się harmonogram istniejących modyfikacji lub wprowadzenia dodatkowych środków prewencji i wspomagania reagowania w sytuacji ataku.

2.1 Identyfikowanie obiektów krytycznych.

W tym kroku zwraca się uwagę głównie na obiekty szczególnie ważne dla funkcjonowania miasta oraz na sposoby zabezpieczeń tych obiektów (systemy fizyczne i systemy automatyki zabezpieczeniowej) dla instalacji stacjonarnych.

Konkretne zabezpieczenia dotyczą m.in.: sposobu ochrony, podatności na oddziaływanie terrorystów oraz warunków ewakuacji w przypadku zagrożenia.

2.2 Identyfikacja zagrożeń.

Krok identyfikacji zagrożeń jest procesem identyfikowania i zrozumienia jak zabezpieczenia krytyczne wpływają na możliwe zajścia i wypadki, i jak wówczas zmienia się poziom zagrożenia.

2.3 Analiza skutków

Celem analizy skutków jest zrozumienie i oszacowanie potencjalnych strat, które mogą zaistnieć w przypadku udanego ataku terrorystycznego. Potencjalne skutki dotkną wówczas sąsiednie regiony, gdzie także trzeba będzie ocenić szkody i zniszczenia. W przypadku ataku cybernetycznego, może zostać stracona część danych oraz może nastąpić chaos podczas akcji ratunkowych.

Analiza skutków powinna zawierać rozległe informacje na temat możliwych scenariuszy działania terrorystów, jak i służb odpowiedzialnych za bezpieczeństwo. Dla każdego scenariusza, analiza powinna zawierać: oszacowanie potencjalnych skutków użycia różnego rodzaju broni (bomby, broi chemicznej, broni biologicznej) oraz oszacowanie jej wpływu na ochranianą ludność (obiekty).

Tabela 1. Typy i znaczenie potencjalnych zagrożeń

Numer zmiennej	Zmienna	Opcje
1.	**Rodzaj ataku terrorystycznego**	**1. Bezpośredni atak na:** • obiekty dyplomatyczne i rezydencje wszystkich krajów, w zależności od stopnia zagrożenia, oraz siedzib firm amerykańskich i zachodnich, z uwzględnieniem obiektów i terenów przylegających, • porty lotnicze z uwzględnieniem portów cargo oraz lotnisk lotnictwa cywilnego, • obiekty rządowe, • centra handlowe, multikina, duże dworce kolejowe i autobusowe, • ważne dla bezpieczeństwa społecznego obiekty i urządzenia (np. ujęcia wody pitnej, przepompownie, filtry, zapory, zbiorniki wody, duże mosty, anteny telekomunikacyjne), • zakłady produkujące materiały niebezpieczne lub firmy je dystrybuujące, • transporty z substancjami niebezpiecznymi, • świątynie, • obiekty sportowe w trakcie trwania imprez masowych (koncerty). 2. **Podłożenie ładunku wybuchowego.** 3. **Podłożenie ładunku wybuchowego z zastosowaniem materiału promieniotwórczego.** 4. Podłożenie ładunku wybuchowego z zastosowaniem środka mikrobiologicznego. 5. Podłożenie ładunku wybuchowego z zastosowaniem środka chemicznego. 6. Uprowadzenie środka transportu w komunikacji lotniczej. 7. Uprowadzenie środka transportu w komunikacji lądowej. 8. Uprowadzenie środka transportu w komunikacji wodnej. 9. Zajęcie obiektu, w tym również z przetrzymywaniem zakładników. 10. **Uprowadzenie zakładników.** 11. **Zagrożenie atakiem terrorystycznym z powietrza typu "Renegade":** • zidentyfikowanie cywilnego statku powietrznego, który zachowuje się w taki sposób, że powstaje podejrzenie, iż może być użyty do wykonania ataku terrorystycznego z powietrza (określany jako samolot typu "Renegade"),

		• lądowanie samolotu określanego jako samolot typu "Renegade" na lotnisku interwencyjnym, • lądowanie awaryjne samolotu określanego jako samolot typu "Renegade" poza lotniskiem interwencyjnym.
2.	**Zakres zamierzonego celu lub cel pośredni**	• Spowodowanie masowych strat materialnych (zniszczenia obiektów). • Zagrożenie życia i zdrowia ludzi na terenie objętym atakiem terrorystycznym. • Zakłócenie infrastruktury w sieciach (rtv, energia, łączność itp.). • Wymuszanie określonego działania, np. wypuszczenie więzionych terrorystów, wypłacenie okupu, poprzez wzięcie zakładników, podłożenie bomb. • Wzrost liczby przestępstw przeciwko życiu, zdrowiu i mieniu. • Zabójstwa osób objętych szczególną ochroną. • Podpalenia obiektów. • Zamachy przy użyciu materiałów wybuchowych. • Napady rabunkowe (zdobycie środków finansowych na działalność terrorystyczną). • Terror internetowy (cyberterror). • Porwania osób (kidnaping). • Porwania środków transportu (pociągi, autokary, samoloty itp.) wraz z pasażerami. • Atak z użyciem środków chemicznych, biologicznych i radiologicznych. • Zmniejszenie skuteczności organów ścigania. • Totalna negacja obowiązującego prawa spowodowana walką o przetrwanie. • Powodowanie katastrof drogowych, kolejowych, lotniczych, morskich, wodnych, których zadaniem jest spowodowanie totalnego paraliżu komunikacyjnego. • Nasilenie zgonów i zachorowań spowodowanych atakiem terrorystycznym. • Zmniejszenie skuteczności służb medyczno-ratowniczych z uwagi na wzrost liczby ofiar (brak miejsc w szpitalach, środków, leków). • Totalny chaos na miejscu zdarzenia.
3.	**Przedmiot zamierzonego celu**	• Życia ludzkie • Organy władzy • Ludność cywilna • Przerwanie ciągłości funkcjonowania infrastruktury krytycznej • Przechwycenie strategicznych informacji, baz danych • Wizerunek i reputacja władzy oraz systemu odpowiedzialnego za bezpieczeństwo wewnętrzne państwa
4.	**Wpływ strefy**	• Ludność cywilna • Zakłady przemysłowe • Własność publiczna • Ciągłość działania • Środowisko • Wizerunek i reputacja władzy oraz systemu odpowiedzialnego za bezpieczeństwo wewnętrzne państwa • Oddźwięk społeczny

5.	**Źródła zagrożeń**	• Zewnętrzny bezpośredni atak fizyczny - rozpoczęty od zewnętrznych barier kontroli z zamiarem spowodowania bezpośredniej szkody (rakieta; materiał wybuchowy; zastosowanie broni z terenów przyległych do obiektu ataku, eksplozja w obiekcie) • Zewnętrzny pośredni atak fizyczny - rozpoczęty od zewnętrznych barier kontroli z zamiarem spowodowania ogólnej szkody w obiekcie chronionym lub bezpośredniej szkody dla innych (zniszczenie obiektów sąsiadujących z obiektem ale będących łatwiejszym celem) • Zewnętrzny pośredni atak wpływający na dany obiekt - atak na główną infrastrukturę miejską wpływającą na funkcjonowanie miasta (zniszczenie strategicznych elektrowni w mieście; zablokowanie sieci internetowych; zablokowanie systemu bankowego; przerwanie transportu, itp) • Wewnętrzny atak fizyczny - rozpoczęty od wewnętrznych barier kontroli poprzez ich uszkodzenie (naruszenie barier bezpieczeństwa poprzez umieszczenie ładunku wybuchowego w sąsiedztwie danego obiektu) • Wewnętrzny atak fizyczny przez wewnętrzne źródło - rozpoczęty od wewnętrznych barier kontroli ze źródłem wewnątrz obiektu (sabotaż przez osoby, która znajdują się wewnątrz ochranianych obiektów)
6	**Motyw**	• Rząd przeprowadzający akcje militarne przeciwko terrorystom • Założenia organizacji terrorystycznych • Zbrodniczy zamiar (podpalenie; kradzież; morderstwo)
7	**Typ broni**	• Broń dużego zasięgu -materiały wybuchowe; rakiety, granaty; broń dużego kalibru • Broń masowego rażenia (broń jądrowa, biologiczna i chemiczna) • Broń ręczna - pistolet; broń automatyczna; strzelby; • Elektroniczne (cybertrrroryzm opanowanie lub uszkodzenie serwerów instytucji państwowych i odpowiedzialnych za bezpieczeństwo) • Działania fizyczne (np. uszkodzenie kabli komunikacyjnych) • Prywatny i publiczny transport – zniszczenie lub uszkodzenie autobusów, wagonów kolei, transportu lotniczego
8	**Wywołane skutki**	• Fizyczne • Wybuchy i eksplozje • Elektroniczne • Chemiczne substancje • Jądrowe • Biologiczne
9	**Mechanizm wpływu**	• Wpływ fizyczny • Eksplozja • Pożar • Uwolnienie toksyczne substancje • Wpływ elektroniczny • Wpływ na łączność

TYPY ZDARZEŃ NIEPOŻĄDANYCH

Istnieją różne typy zdarzeń i odpowiednio dla nich potencjalne cele.

- Śmierć i zranienia wśród ludzi, straty, szkody w mieniu: potencjalnymi celami są obiekty oraz ludzie znajdujący się w większych skupiskach.
- Kradzież: potencjalne cele to związki chemiczne i biologiczne w trakcie ich przetwarzania, magazynowania czy transportowania, systemy kontroli i strategiczne informacje w trakcie przekazywania ich drogą telekomunikacyjną lub internetową.
- Zanieczyszczenia: potencjalne cele to: obiekty produkujące i przechowujące surowce chemiczne i biologiczne, paliwa, produkty końcowe i pośrednie procesów, emitowane zarówno przy ataku zakłady, jak i na magazyny.

2.4. Atrakcyjność celu

Atrakcyjność celu dla terrorystów jest wskazówką dla osób odpowiedzialnych za ochronę w miastach, jak oceniać prawdopodobieństwo ataku.

2.5 Elementy zabezpieczeń (ochrony).

Zespół SVA określa i dokumentuje istniejący poziom bezpieczeństwa w aspekcie możliwych działań terrorystycznych i stosowane strefy bezpieczeństwa w celach ochronnych (przykład stref obrazuje rys.1)[102].

Może to oznaczać bezpieczeństwo fizyczne, cybernetyczne, kontrolę administracyjną i inne działania. Podczas tego kroku wszystkie działania, informacje i strategie powinno być realizowane i zbierane w specjalnej bazie informacyjnej.

Krok 3 Ocena źródeł zagrożeń terrorystycznych (threat assessment)

Istnieje wiele czynników determinujących oszacowywanie wrażliwości danego obiektu na zagrożenia zewnętrzne. Zagrożenie może wynikać z łatwego dostępu do poszczególnych segmentów danego obiektu, z dostępności sąsiedztwa poszczególnych obiektów oraz ze względu na znaczenie strategiczne danego obiektu. Do ataku może dojść w każdej chwili. Ataki terrorystyczne mogą mieć charakter ogólny jak i specyficzny i indywidualny.

---

[102] Tamże.

Krok 4: Analiza Podatności (vulnerability) - metoda wyboru celu lub scenariusza ataku

W trakcie tego kroku definiowane są podstawowe zagrożenia w mieście z uwzględnieniem prawdopodobieństwa ataku, a także ich „atrakcyjności" dla terrorystów. Jeżeli w trakcie analiz SVA jakieś zdarzenie zostanie określone jako dość prawdopodobne, należy dla niego określić także potencjalne scenariusze. Są dwie szkoły metodologii analiz: analizy oparte na scenariuszach i analizy oparte na obiektach „atrakcyjnych" dla terrorysty. Zarówno w podejściu do analiz opartym na scenariuszu jak i na aktywach ostatecznym zadaniem jest uszeregowanie potencjalnych celów pod względem ryzyka ich zaatakowania, tzn. jak bardzo prawdopodobny jest atak, uwzględniając wartość strategiczną celu, ale także dostępne środki zaradcze.

Wszystkie scenariusze opracowane w **Kroku 4** grupuje się w zestawy, a następnie szereguje (obiekt, którego uszkodzenie ma największe konsekwencje, znajduje się na czele listy). Zespół powinien opracować takie zestawy, w których aktywa są współzależne z zagrożeniami.

Krok 5: Analiza środków zaradczych

Podejście oparte na aktywach przedstawiało scenariusze ogólne z odgórnym założeniem określonych dostępnych środków zaradczych. W podejściu opartym na scenariuszu środki zaradcze są określane dla każdego scenariusza osobno. Niezależnie jednak od stosowanego przez zespół SVA podejścia, należy określić ilość i właściwości dostępnych środków zaradczych, aby móc stworzyć hierarchię zagrożeń.

Przeprowadzenie analizy środków zaradczych jest potrzebne, aby zespół SVA mógł określić różnicę pomiędzy istniejącymi a pożądanymi środkami bezpieczeństwa oraz zdefiniował gdzie istnieje potrzeba zwiększenia tychże środków.

Analizy SVA stanowią podstawę do opracowania planów bezpieczeństwa, obejmujących działania prewencyjne i zalecenia sposobu reagowania w przypadku wystąpienia ataku terrorystycznego.

Podsumowanie

Bezpieczeństwo i ochrona miast polskich powinno opierać się na szczegółowo opracowanym planie bezpieczeństwa, zawierającym wytyczne pozwalające zminimalizować m.in. zagrożenia terrorystyczne i sabotażowe oraz pomagające w efektywnym przydzielaniu środków zaradczych poprzez:

- identyfikowanie aktualnych i potencjalnych źródeł wypadków, zagrożeń aktami terroru i sabotażu, mogących powodować zagrożenie dla prawidłowego funkcjonowania miasta;
- identyfikowanie prawdopodobieństwa i konsekwencji potencjalnych wypadków z użyciem różnego rodzaju broni;
- prowadzenie wyczerpującej i zintegrowanej oceny, testującej i porównującej całe spektrum potencjalnych wypadków oraz nakreślającej możliwe sposoby zapobiegania i redukowania skutków ataku terrorystycznego;
- prowadzenie porównawczej oceny całego spektrum potencjalnych wypadków oraz określenia priorytetów możliwych sposobów zapobiegania i redukowania skutków ataku terrorystycznego;
- ustalenie i śledzenie rozwoju planu bezpieczeństwa zwłaszcza pod względem wdrażania głównych założonych celów.
- w zależności od rodzaju zagrożenia wydzielać odpowiednie siły i środki do przeciwdziałania.

Zespół opracowujący plan bezpieczeństwa powinien kierować się następującymi zasadami:

- plan ochrony miast polskich w warunkach zagrożeń terrorystycznych powinien być elastyczny;
- uzyskanie pełnej informacji jest naczelną zasadą pozwalającą stworzyć sprawnie funkcjonujący plan ochrony miast polskich w warunkach zagrożeń terrorystycznych;
- przeprowadzenie SVA jest kluczowym elementem budowy systemu ochrony miast polskich w warunkach zagrożeń terrorystycznych
- zarządzanie ryzykiem w ochronie miast polskich w warunkach zagrożeń terrorystycznych powinno polegać na monitorowaniu i obniżaniu ryzyka do poziomu akceptowalnego przez zespół odpowiedzialny za bezpieczeństwo.

3.2. Istota ryzyka w systemie cywilno – wojskowej ochrony miast polskich w warunkach zagrożeń terrorystycznych.

Zdefiniowanie ryzyka jest zadaniem dość trudnym, a podanie jednoznacznej, precyzyjnej definicji jest wręcz niemożliwe. Ryzyko jest definiowane na bazie różnych nauk i teorii, m.in. w ekonomii, naukach behawioralnych, naukach prawnych, psychologii, statystyki, ubezpieczeniach, teorii prawdopodobieństwa i innych.

Już od kilkudziesięciu lat próbuje się zdefiniować ryzyko i tak: w 1901 roku A.H. Willet twierdził, że ryzyko jest czymś obiektywnym, związanym z subiektywną niepewnością. Definicja ta jest jednak bardzo nieprecyzyjna ze względu na wieloznaczność pojęcia niepewności. W roku 1921 F.H. Knight opublikował swoją koncepcję niepewności mierzalnej i niemierzalnej gdzie pierwszą nazwał ryzykiem a drugą niepewnością sensu stricto.

Słowo **ryzyko** pochodzi od starowłoskiego risicare, które oznacza odważyć się. Zatem z semantyki wynika, że ryzyko jest raczej wyborem, a nie nieuchronnym przeznaczeniem. Wiążąc ryzyko z wyborem, potwierdzamy nierozerwalny związek ryzyka z czasem.[103]

Obecnie w języku potocznym za ryzyko przyjmuje się jakąś miarę lub ocenę zagrożenia wystąpienia jakiegoś niepożądanego zjawiska na skutek podjęcia przez nas jakiejś decyzji lub z prawdopodobnych zdarzeń od nas niezależnych. Potwierdzają to nowe rodzaje ryzyk związane ze współczesnymi zagrożeniami cywilizacyjnymi (terroryzm, awarie systemów informatycznych) ryzyko nierozerwalnie związane jest z niepewnością, jednak niepewności jako takiej nie da się oszacować.[104]

Ryzyko nierozerwalnie związane jest z niepewnością jako takiej nie da się oszacować. Ryzyko występuje jeżeli:

- można oszacować prawdopodobieństwo realizacji poszczególnych zdarzeń w przyszłości;
- można zidentyfikować skutki tych zdarzeń.

---

[103] http://mfiles.pl/pl/index.php/Ryzyko

[104] J.R. Rak Wybrane elementy zarządzania ryzykiem w przedsiębiorstwie wodociągowym. Ochrona środowiska Nr4 2007r.

Współcześnie ryzyko definiowane jest jako uporządkowany zbiór trójelementowy:

$$r=(S,P,C)$$

w którym:

S – negatywny scenariusz opisany jako ciąg następujących po sobie zdarzeń niepożądanych;

P – prawdopodobieństwo zajścia scenariusza S;

C – miara strat wywołanych przez scenariusz S[105].

Można postawić tezę, że ryzyko w miarę upływu czasu jest coraz większe, bowiem wraz z upływem czasu maleje wartość oczekiwana związana z podjęciem decyzji i rośnie możliwy rozrzut wokół wartości oczekiwanej.[106]

Ryzyko – w języku naturalnym oznacza jakąś miarę/ocenę zagrożenia czy niebezpieczeństwa wynikającego albo z prawdopodobnych zdarzeń od nas niezależnych, albo z możliwych konsekwencji podjęcia decyzji.[107]

Najogólniej, ryzyko jest wskaźnikiem stanu lub zdarzenia które może prowadzić do strat. Jest ono proporcjonalne do prawdopodobieństwa wystąpienia tego zdarzenia i do wielkości strat które może spowodować.[108]

Rozpatrując ryzyko z punktu widzenia możliwych skutków wyróżnia się:

- poniesienie straty, co wskazuje na negatywne skutki związane ze zdarzeniami niepożądanymi;
- działania powodujące skutek niezgodny z oczekiwaniami, które mogą być pozytywne lub negatywne.

Trzy koncepcje ryzyka[109]

Etapy rozwoju naukowej definicji ryzyka są w dużej mierze zgodne z ewoluowaniem rozróżnienia określeń ryzyko i niepewność z nim związana.

Pierwsza koncepcja ekonomicznej teorii ryzyka Willetta została ogłoszona w 1901 roku. Przyjął on założenie, że ryzyko jest terminem o różnych znaczeniach powszechnie używanych w życiu codziennym. Łącząc pojęcie ryzyka z niepewnością i wykorzystując determinizm filozoficzny, uznał on, że powinno się mówić jedynie o

---

[105] Tamże.

[106] J.Rak; B. Tchórzewska – Cieślak., Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005.

[107] http://pl.wikipedia.org/wiki/Ryzyko

[108] Tamże.

[109] http://pl.wikipedia.org/wiki/Zarządzanie_ryzykiem

wrażeniu lub złudzeniu przypadkowości, co jest efektem niedoskonałości wiedzy o prawach rządzących rzeczywistością. Willett uznawał ryzyko za stan otoczenia i twierdził, że ryzyko należy odnosić do stopnia niepewności, czy określony skutek w ogóle wystąpi, a nie do prawdopodobieństwa jego wystąpienia. Ryzyko rozumiane jako stan otoczenia jest obiektywne i skorelowane z subiektywną niepewnością.

Za drugą należy przyjąć koncepcję niepewności mierzalnej oraz niemierzalnej zaproponowaną w 1921 roku przez Knighta. Zasadniczym celem prac Knighta było sprecyzowanie, jakimi cechami powinna charakteryzować się niepewność, którą należy identyfikować z ryzykiem, w odniesieniu od niepewności sensu stricto. W tej koncepcji ryzyko jest niepewnością mierzalną. Niepewność która nie może być zmierzona, jest niepewnością sensu stricto, którą Knight nazwał niepewnością niemierzalną.

Trzecia zasadnicza koncepcja została opracowana przez Komisję do Spraw Terminologii Ubezpieczeniowej USA w 1996 roku. Efektem prac były dwie definicje ryzyka. Według pierwszej z nich ryzyko jest to niepewność co do określonego zdarzenia w warunkach dwóch lub więcej możliwości. W tym rozumieniu jest to mierzalna niepewność, czy zamierzony cel działania zostanie osiągnięty. Druga definicja koncentruje uwagę na zagadnieniach praktyki ubezpieczeniowej, stanowiąc, że ryzyko jest to ubezpieczona osoba lub ubezpieczony podmiot.

Dyskusje nad tymi definicjami doprowadziły do czterech zasadniczych wniosków dotyczących natury ryzyka:

1. Ryzyko nie jest czymś jednorodnym, a zatem nie jest możliwe podanie jednej uniwersalnej i jednoznacznej definicji tego pojęcia.
2. Ryzyko występuje w co najmniej dwóch aspektach:
    - obiektywnym
    - subiektywnym
3. Ryzyko może być badane w różnych kontekstach, na przykład jako:
    - niebezpieczeństwo
    - niepewność
    - prawdopodobieństwo.
4. Ryzyko jest czymś zmiennym i stadialnym, czyli jest raczej procesem niż stanem otoczenia.

Nauka o ryzyku jest praktycznie rozwijana w większości nauk i stosowana we wszystkich technologiach. Obecnie nie istnieje jeszcze jednolita teoria ryzyka, natomiast wyróżniane są następujące jej praktyczne działy, takie jak:

- **analiza ryzyka**
- szacowanie ryzyka
- percepcja ryzyka
- **zarządzanie ryzykiem**
- komunikacja ryzyka
- socjologia ryzyka
- ryzyko informatyczne

Celem **analizy ryzyka** jest określenie i oszacowanie prawdopodobieństwa oraz skutków wystąpienia danego (niepożądanego) zdarzenia. Analiza ryzyka to określone działania skierowane na obniżenie wpływu ryzyka na funkcjonowanie danego podmiotu i podejmowanie odpowiednich środków przeciwdziałania i minimalizacji ryzyka. Pozwala na określenie poziomu ryzyka w sposób jakościowy i ilościowy dzięki czemu mogą zostać przeprowadzane działania zapobiegawcze lub działania polegające na jego eliminacji.

Analiza ryzyka jest jednym z elementów procesu zarządzania ryzykiem. Wyróżnia się kilka rodzajów podejścia do analizy[110]:

1. Podejście podstawowego poziomu - zastosowanie standardowych zabezpieczeń.
2. Podejście nieformalne - oparte na wiedzy i doświadczeniu ekspertów,
3. Szczegółowa analiza ryzyka - z wykorzystaniem technik analizy ryzyka,
4. Podejście mieszane.

Analiza ryzyka jest narzędziem wykorzystywanym m.in. do:

- **przygotowania polityki bezpieczeństwa i systemów zarządzania bezpieczeństwem**,
- zarządzania projektem,
- zarządzania przedsiębiorstwem,
- różnego rodzaju analiz biznesowych.

Zarządzanie ryzykiem łączy funkcje zarządzania z monitorowaniem określonej dziedziny i zmniejszaniem możliwych w niej **zagrożeń** poprzez szacowanie lub

---

[110] Tamże.

estymacje wartości tzw. parametru ryzyka odnoszącego się do stanu zawartych w tej dziedzinie obiektów i zdarzeń/procesów.[111]

Zarządzanie ryzykiem w ochronie miast polskich to zarządzanie polegające na monitorowaniu i obniżaniu ryzyka do poziomu akceptowalnego przez odpowiedzialnego za bezpieczeństwo.

Proces zarządzania ryzykiem składa się z następujących etapów[112]:

1. Zrozumienie wykonywanej działalności
2. Identyfikacja ryzyka
3. Analiza ryzyka
4. Ocena punktowa ryzyka
5. Hierarchizacja ryzyka
6. Zarządzanie i kontrolowanie ryzyka

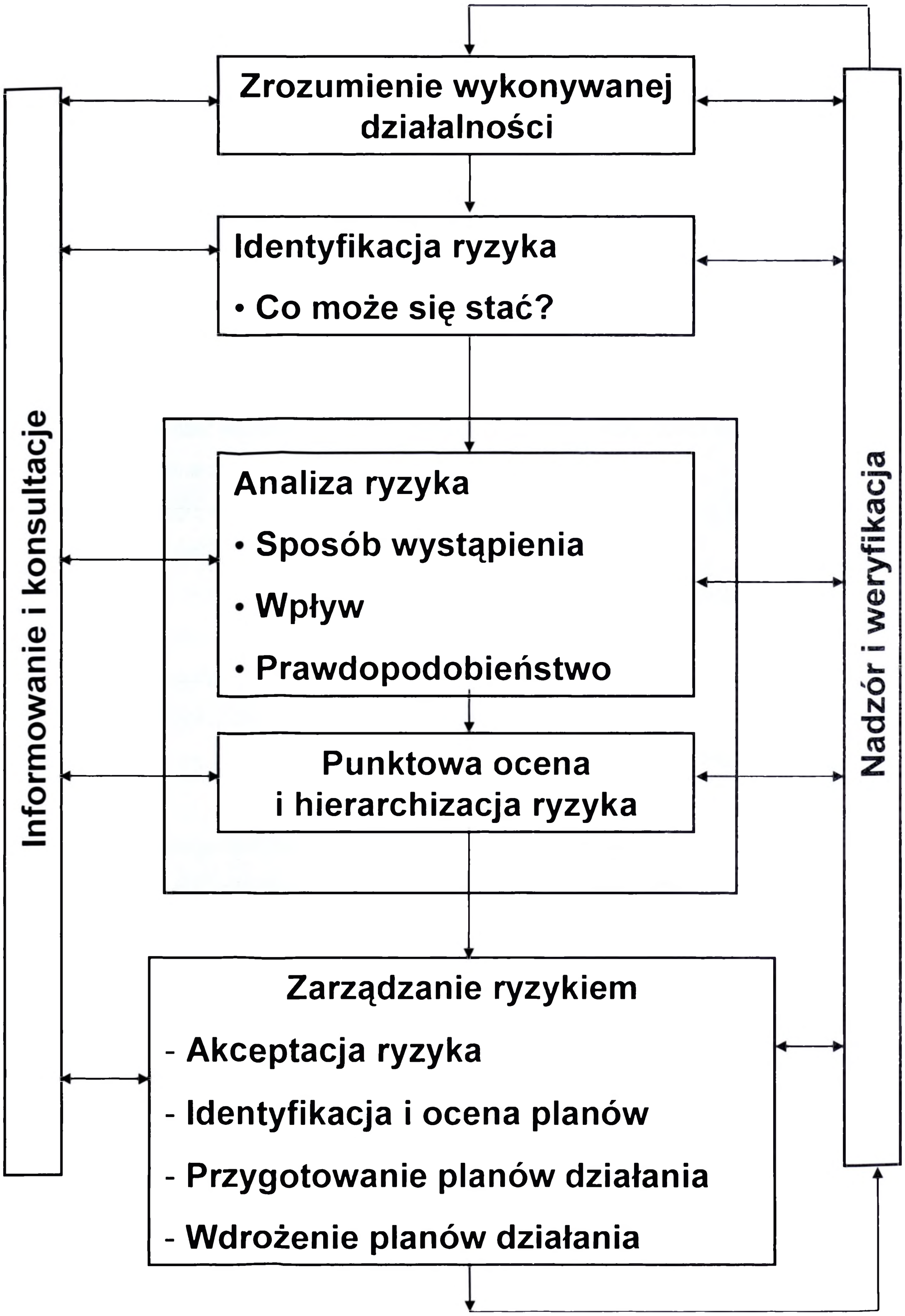
Zarządzania ryzykiem nie można traktować jako obciążenia dla organizacji, lecz jako sposób maksymalizacji dostępnych możliwości i zmniejszenia prawdopodobieństwa porażki. Identyfikacja i zarządzanie ryzykiem winno dotyczyć każdej osoby w organizacji i być realizowane przez kierownictwo organizacji. Powiązania pomiędzy etapami w procesie zarządzania ryzykiem[113] przedstawia rysunek 11.

---

[111] http://pl.wikipedia.org/wiki/Zarz%C4%85dzanie_ryzykiem

[112] Bentley Dennison, Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce. Wyd. Ministerstwo Finansów 2004r.

[113] Tamże.



Rys. 11. Powiązania pomiędzy etapami w procesie zarządzania ryzykiem [Opracowanie w *oparciu o przegląd procesu zarządzania ryzykiem (AS / NZS 4360:1999)*]

Zrozumienie wykonywanej działalności Jest to zbiór czynności, które mają na celu z jednej strony skłonienie szefa (odpowiedzialnego) projektu do przygotowania i zorganizowania procesu zarządzania ryzykiem, z drugiej zaś mają one doprowadzić do powstania infrastruktury organizacyjnej, której zadaniem będzie podjęcie działań zmierzających do: izolowania i zmniejszenia ryzyka, eliminowania ryzyka (jeśli jest to możliwe i uzasadnione), przygotowania alternatywnych sposobów działania. Materiały te powinny być wykorzystane podczas spotkań, których celem będzie stworzenie planu zarządzania ryzykiem. Plan taki powinien zawierać[114]:

- *„metodykę określającą sposoby, narzędzia i źródła danych, które należy wykorzystać w zarządzaniu ryzykiem,*
- *opis ról i obowiązków poszczególnych zespołów roboczych względem procesu zarządzania ryzykiem,*
- *listę terminów określających wszystkie działania związane z procesem zarządzania ryzykiem na wszystkich etapach projektu,*
- *system oceny i interpretacji zdarzeń mogących wywołać niepożądany przebieg projektu,*
- *progi akceptacji, czyli kryteria określające, kiedy powinny zostać podjęte działania będące odpowiedzią na zaistniałe ryzyko,*
- *sposoby tworzenia dokumentacji procesu zarządzania ryzykiem."*

Identyfikacja ryzyka Są to działania, których celem jest wykrycie źródeł ryzyka, a następnie ich usystematyzowanie według przyjętych kategorii. Identyfikacja ryzyka w metodyce PMBoK[115] jest procesem iteracyjnym, wykonuje się ją wielokrotnie zarówno podczas planowania, jak i w trakcie realizacji projektu. Materiałami wejściowymi do identyfikacji ryzyka są[116]:

- *„plan zarządzania ryzykiem będący efektem poprzedniego etapu,*
- *rezultaty procesów planowania projektu, do których należą: struktura podziału pracy, harmonogram i szacunki kosztów, plany użycia zasobów, listy zagrożeń i ograniczeń,*

---

[114] http://pl.wikipedia.org/wiki/Zarządzanie_ryzykiem_(projektowanie).

[115] **PMBoK** (ang. *Project Management Body of Knowledge*) jest zbiorem standardów i najlepszych rozwiązań w dziedzinie zarządzania projektami zebranych i opublikowanych przez członków PMI (*Project Management Institute*). Standard PMBoK jest to zbiór najlepszych, powszechnie uznanych praktyk znajdujących zastosowanie w zarządzaniu projektami.

[116] http://pl.wikipedia.org/wiki/ Zarządzanie _ryzykiem_(projektowanie).

- *zdefiniowane kategorie ryzyka. Są to nazwy grup, do jakich będzie można zakwalifikować wszystkie niekorzystne zdarzenia mogące pojawić się podczas planowania i realizacji przedsięwzięcia. Wprowadzenie kategorii (niekiedy nazywanych profilami) umożliwia systematyzację wszystkich ryzyk. Ważne jest, by przyjęte kategoria były prawidłowo dobrane w zależności od specyfiki projektu i tym samym odpowiadały typowym źródłom ryzyka dla ochrony miast przed zagrożeniami terrorystycznymi. Do często wyróżnianych kategorii ryzyka należą: ryzyko techniczne, ryzyko organizacyjne oraz ryzyko zewnętrzne,*
- *dane historyczne dotyczące wcześniejszych realizacji projektów".*

Proces identyfikacji ryzyka w metodyce PMBoK może być wspierany wieloma narzędziami i technikami. Wydaje się to oczywiste, gdyż przewidzenie, jakie zdarzenia mogą istotnie wpłynąć na niezrealizowanie planowanych zadań projektowych jest czynnością trudną i nie zawsze w pełni możliwą do wykonania. Do najważniejszych technik należą:

- przegląd dokumentacji. Jest to zwyczajowo pierwszy krok w procesie identyfikacji ryzyka,
- techniki gromadzenia informacji o źródłach zagrożeń, do których zalicza się: burzę mózgów, technikę delficką, ankiety oraz analizę mocnych stron, słabych stron, szans i zagrożeń (SWOT),
- listy kontrolne. Należą do narzędzi tworzonych na podstawie danych historycznych oraz wiedzy gromadzonej w podczas realizacji podobnych projektów w przeszłości. Są to proste i skuteczne narzędzia identyfikacji ryzyka. Główną wadą ich jest to, że nie można stworzyć ewidencji wszystkich potencjalnych zagrożeń projektowych,
- analiza założeń projektowych - ma na celu identyfikację ryzyka wynikającą z niedokładności, niespójności lub niekompletności założeń,
- techniki oparte na diagramach. Umożliwiają łatwą identyfikację symptomów ryzyka oraz przejrzyste ułożenie schematów przyczynowo skutkowych.[117]

W wyniku użycia jednej bądź wielu powyższych technik zespół zarządzający ryzykiem otrzymuje: listę zidentyfikowanych źródeł ryzyka usystematyzowaną według określonych kategorii oraz spis czynności wyzwalających (symptomów, sygnałów

---

[117] Tamże.

ostrzegawczych) wskazujących, że wkrótce może dojść lub że już doszło do wystąpienia niekorzystnego zdarzenia.

Analiza ryzyka Głównym zadaniem tej fazy procesu zarządzania ryzykiem jest oszacowanie wielkości prawdopodobieństwa i skutków zaistnienia zidentyfikowanych uprzednio ryzyk. Na tym etapie wykonuje się hierarchizację zidentyfikowanych niebezpieczeństw według ich potencjalnego wpływu na proces realizacji przedsięwzięcia. Uzyskane wyniki będą stanowiły podstawę do dalszego planowania reakcji na niekorzystne zjawiska. Analiza ryzyka wymaga zastosowania odpowiednich narzędzi np. technik macierzowych. Wielokrotne zastosowanie podczas realizacji przedsięwzięcia tych prostych narzędzi umożliwia zaobserwowanie trendów, które mogą stanowić podstawę do podjęcia uzasadnionych decyzji o intensyfikacji lub ograniczeniu działań związanych z zarządzaniem ryzykiem. Podstawowe narzędzia i techniki używane do jakościowej analizy ryzyka to: lista prawdopodobieństw i skutków ryzyka (korzysta się tu ze skal opisowych np. bardzo wysokie, umiarkowane, niskie i bardzo niskie), macierze ocen prawdopodobieństwa i skutków wystąpienia ryzyka (stosuje się w nich w zależności od potrzeb skale liniowe lub logarytmiczne), badanie złożoności projektu (ocenia się stabilność założeń projektowych oraz ewentualne skutki wpływu błędów popełnionych przy ich formułowaniu). Rezultatem analizy ryzyka jest: ogólny ranking projektu pod kątem ryzyka (pozwalający na porównanie poziomu ryzyka z ryzykami występującymi w innych projektach), lista hierarchii ryzyka (umożliwiająca wyszczególnienie źródeł ryzyka o bardzo dużym potencjalnie negatywnym wpływie na projekt, czy też prawdopodobnie nieistotnych dla projektu), trendy wynikające z rezultatów jakościowej analizy ryzyka przeprowadzonej wielokrotnie podczas realizacji projektu.

Punktowa ocena i hierarchizacja ryzyka. Proces ten ma na celu określenie wymiernych wartości wielkości prawdopodobieństwa oraz skutków wystąpienia zdarzeń niekorzystnych zarówno dla poszczególnych czynności projektu, jak i dla całego przedsięwzięcia. Pomiar taki pozwala ustalić w wielkościach wymiernych szansę osiągnięcia celów projektu, określić poziomy niezbędnych rezerw, przeprowadzić szczegółową analizę typu, „co-jeśli". Efektem przeprowadzenia punktowej oceny ryzyka dla danego projektu są: lista zmierzonych ilościowo ryzyk uszeregowanych według priorytetów, analiza probabilistyczna projektu (zawiera prognozy dotyczące kosztów i czasów realizacji zadań), wielkości prawdopodobieństwa osiągnięcia celów kosztowych i czasowych, trendy charakteryzujące wyniki ilościowej analizy ryzyka

(dane te są uzyskiwane na podstawie kilkukrotnego przeprowadzenia analizy ilościowej).

Zarządzanie i kontrolowanie ryzyka Jest to proces opracowywania wariantów postępowania dotyczących czynności zmniejszających zagrożenia i zwiększających potencjalne korzyści dla sformułowanych celów projektowych. Plan reakcji na ryzyko to kluczowy etap procesu zarządzania ryzykiem, gdyż opracowuje się w nim metody reagowania na zdarzenia korzystne i niekorzystne. Skuteczność planowania reakcji na ryzyka zadań zagrożonych ma bezpośredni wpływ na wzrost lub spadek ryzyka realizacji całego projektu. Planowane reakcje muszą być proporcjonalne do skutków wystąpienia niekorzystnych zjawisk, likwidować (lub niwelować) wpływy danego zagrożenia w sposób kosztowo efektywny oraz być realizowane terminowo. W procesie planowania reakcji na ryzyka powszechnie stosuje się kilka strategii. Do każdego z ryzyk należy tak dobrać plan postępowania, by podjęte działania były jak najbardziej skuteczne. Do najbardziej popularnych strategii zalicza się[118]:

- *„unikanie ryzyka - polega na takiej modyfikacji planów realizacji projektu, by zlikwidować dane ryzyko (niestety nie można w praktyce wyeliminować wszystkich zdarzeń, z którymi wiążą się niebezpieczeństwa) albo korzystnie zmienić uwarunkowania z nim związane,*
- *łagodzenie ryzyka - to najpowszechniejsza ze wszystkich strategii reagowania na ryzyko. Proces ten polega na podejmowaniu określonych działań prowadzących do zmniejszenia prawdopodobieństwa lub skutków ryzyka,*
- *akceptacja ryzyka - polega na przyjęciu i udźwignięciu wszelkich konsekwencji wynikających z ewentualnego wystąpienia niekorzystnego zjawiska. Jest to świadoma decyzja osób zarządzających ryzykiem, by nie wprowadzać żadnych zmian w planie projektu związanych z wystąpieniem danego niekorzystnego zjawiska. Istnieją dwa podstawowe typy akceptacji ryzyka: aktywna i pasywna. Pasywna akceptacja polega na przyjęciu ryzyka bez podejmowania jakichkolwiek działań w celu rozwiązania problemów jakie się z nim wiążą. Natomiast aktywna akceptacja polega na pogodzeniu się z ryzykiem, ale wymaga stworzenia specjalnego planu działania w razie wystąpienia niekorzystnego zdarzenia, a w niektórych przypadkach tzw. planu odwrotu,*

---

[118] Tamże.

- *plan awaryjny - buduje się tylko dla zidentyfikowanych ryzyk, które mogą pojawić się w trakcie realizacji projektu, wcześniejsze opracowanie planu awaryjnego może w sposób istotny obniżyć koszty działań podejmowanych w reakcji na wystąpienie danego niekorzystnego zjawiska".*

Kontrola ryzyka Jest to proces wdrożenia planu zarządzania ryzykiem, nieustannej obserwacji i nadzorowaniu zidentyfikowanych ryzyk, identyfikacji nowo powstałych zagrożeń oraz systematycznego oceniania skuteczności podejmowanych działań prewencyjnych. To właśnie kontrola ryzyka dostarcza informacji niezbędnych do podejmowania decyzji wyprzedzających pojawienie się niekorzystnych zdarzeń. Celem monitorowania ryzyka jest ustalenie czy[119]:

- wdrożono zgodnie z planem strategie reakcji na ryzyka,
- działanie podejmowane w ramach realizacji planów reakcji na ryzyko skutkują oczekiwanymi rezultatami,
- przyjęte założenia projektu są aktualne,
- podczas realizacji projektu nie doszło do zmian w szczególnym i ogólnym poziomie ryzyka (np. zgodnie z analizą trendów),
- wystąpiły czynniki wyzwalające zidentyfikowane ryzyka,
- wystąpiły nowe ryzyka nierozpoznane uprzednio.

O charakterze każdego rodzaju ryzyka decydują trzy podstawowe składniki: zdarzenie, prawdopodobieństwo oraz straty/dotkliwość. Niskie prawdopodobieństwo oraz niezbyt dotkliwe skutki oznaczają niskie ryzyko. Wysokie prawdopodobieństwo oraz bardzo dotkliwe skutki oznaczają wysokie ryzyko. Wysokie prawdopodobieństwo oraz niezbyt dotkliwe skutki oznaczają niskie ryzyko dla ostatecznego powodzenia projektu.

Zarządzanie ryzykiem jest bardzo dynamicznie rozwijającą się dziedziną. Z uwagi na powstanie wielu definicji i metod zarządzania ryzykiem, koniecznością stało się opracowanie standardów w tej dziedzinie. Przez niebezpieczeństwo rozumie się przyczynę lub źródło straty. Przez hazard rozumie się zespół warunków i okoliczności, w których realizuje się niebezpieczeństwo. Niebezpieczeństwo jest sekwencją czasową przebiegającą w następujących fazach:

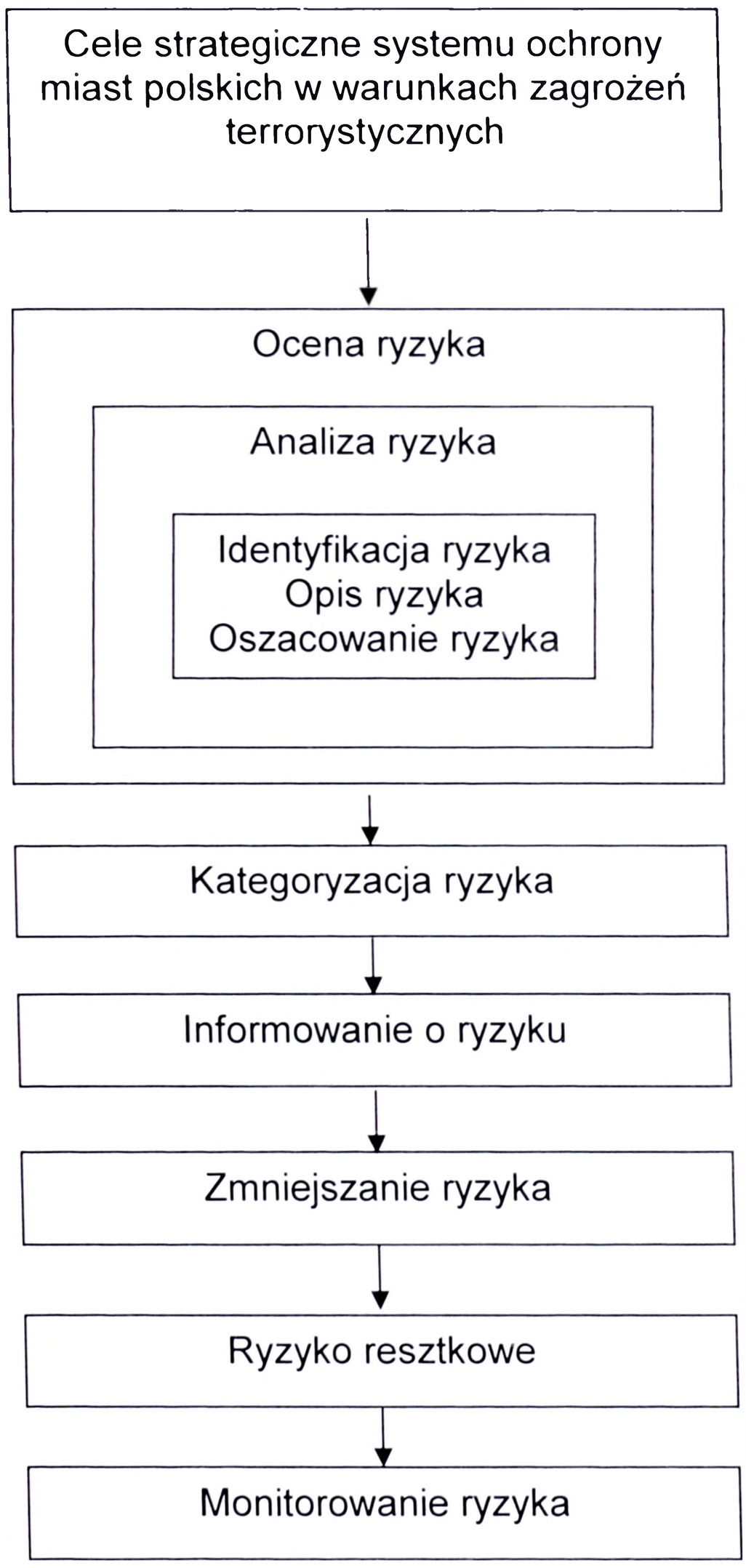
- zagrożenie, niebezpieczeństwo potencjalne;
- realizacja rzeczywista niebezpieczeństwa;

---

[119] Tamże.

- skutki realizacji niebezpieczeństwa.

Rysunek 12 przedstawia schemat procesu zarządzania ryzykiem w ochronie miast polskich przed zagrożeniami terrorystycznymi.



Rys. 12. Schemat zarządzania ryzykiem w ochronie miast polskich w warunkach zagrożeń terrorystycznych. (Opracowanie na podstawie J.R. Rak Wybrane elementy zarządzania ryzykiem w przedsiębiorstwie wodociągowym. Ochrona środowiska Nr 4 2007r.)

W tabeli 2 i 3 przedstawiono standardowe kategorie prawdopodobieństwa (P) wystąpienia zagrożeń terrorystycznych w miastach, tabela 3 przedstawia kategorie skutków (C) w odniesieniu zagrożeń. Tabela 4 zawiera standardową matrycę ryzyka

Tabela 2. Skala opisowa prawdopodobieństwa

Prawdopodobieństwo	**Zagrożenie**	**Waga punktowa**	**Szansa**	**Waga punktowa**
Wysokie – H (prawdopodobne)	P > 0,25	3	P > 0,75	1
Średnie – M (możliwe)	0,02 ≤ P ≤ 0,25	2	0,25 ≤ P ≤ 0,75	2
Niskie – L (mało prawdopodobne)	P < 0,02	1	P < 0,25	3

Tabela 3. Skala opisowa skutków

Skutek	**Opis skutku**	**Waga punktowa**
Duży – H (prawdopodobne)	Duże straty wśród ludności i mienia w mieście	3
Średnie – M (możliwe)	Ograniczone straty wśród ludności i mienia w mieście	2
Mały – L (mało prawdopodobne)	Małe straty wśród ludności i mienia w mieście	1

Tabela 4. Skala opisowa skutków w zależności od zdarzenia

Zdarzenie	Prawdo-podo-bieństwo	Opis skutku	Skutek	Waga punkto-wa
<u>Atak bezpośredni na:</u> • obiekty dyplomatyczne i rezydencje wszystkich krajów, w zależności od stopnia zagrożenia, oraz siedzib firm amerykańskich i zachodnich, z uwzględnieniem obiektów i terenów przylegających, • porty lotnicze z uwzględnieniem portów cargo oraz lotnisk lotnictwa cywilnego, • obiekty rządowe, • centra handlowe, multikina, duże dworce kolejowe i autobusowe, • ważne dla bezpieczeństwa społecznego obiekty i urządzenia (np. ujęcia wody pitnej, przepompownie, filtry, zapory, zbiorniki wody, duże mosty, anteny telekomunikacyjne), • zakłady produkujące materiały niebezpieczne lub firmy je dystrybuujące, • transporty z substancjami niebezpiecznymi, • świątynie, • obiekty sportowe w trakcie trwania imprez masowych (koncerty).	Wysokie – H	1. Spowodowanie masowych strat materialnych (zniszczenia obiektów). 2. Zagrożenie życia i zdrowia ludzi na terenie objętym atakiem terrorystycznym. 3. Zakłócenie infrastruktury w sieciach (rtv, energia, łączność itp.). 4. Wymuszanie określonego działania, np. wypuszczenie więzionych terrorystów, wypłacenie okupu, poprzez wzięcie zakładników, podłożenie bomb. 5. Wzrost liczby przestępstw przeciwko życiu, zdrowiu i mieniu. 6. Zabójstwa osób objętych szczególną ochroną. 7. Podpalenia obiektów. 8. Zamachy przy użyciu materiałów wybuchowych. 9. Napady rabunkowe (zdobycie środków finansowych na działalność terrorystyczną). 10. Terror internetowy (cyberterror). 11. Porwania osób (kidnaping). 12. Porwania środków transportu (pociągi, autokary, samoloty itp.) wraz z pasażerami. 13. Atak z użyciem środków chemicznych, biologicznych i radiologicznych. 14. Zmniejszenie skuteczności organów ścigania. 15. Totalna negacja obowiązującego prawa spowodowana walką o przetrwanie. 16. Powodowanie katastrof drogowych, kolejowych, lotniczych, morskich, wodnych, których zadaniem jest spowodowanie totalnego paraliżu komunikacyjnego. 17. Nasilenie zgonów i zachorowań spowodowanych atakiem terrorystycznym. 18. Zmniejszenie skuteczności służb medyczno-ratowniczych z uwagi na wzrost liczby ofiar (brak miejsc w szpitalach, środków, leków). 19. Totalny chaos na miejscu zdarzenia.	Duży – M (prawdopodobny)	3

<u>Podłożenie ładunku wybuchowego</u>	Wysokie – H	1. Zagrożenie życia i zdrowia obywateli objętych atakiem terrorystycznym z użyciem materiałów wybuchowych. 2. Spowodowanie znacznych strat materialnych w strefie zagrożenia. 3. Przerwanie szlaków komunikacyjnych drogowych, kolejowych, lotniczych. 4. Przerwanie dostaw energii elektrycznej, ciepłowniczej, a także ograniczenie bądź całkowita utrata łączności radiowej i telefonicznej. 5. Próba wymuszenia określonego działania na organach władzy państwowej i samorządowej. 6. Niechęć do opuszczenia miejsc zamieszkania czy też przebywania ludności w strefie zagrożonej i potrzeba podejmowania działań porządkowych przez Policję w celu wsparcia organu samorządowego. 7. Dewastacja i grabież mienia prywatnego i publicznego pozostawionego na czas ewakuacji ludności z terenu potencjalnie zagrożonego wybuchem (bomby). 8. Powstanie chaosu w miejscu prowadzonych działań ratowniczych oraz zakłócenie bezpieczeństwa i porządku publicznego w czasie prowadzonej akcji. 9. Wystąpienie zakłóceń na ciągach komunikacyjnych tras przewidzianych do ewakuacji ludności, dojazdów służb policyjno-ratowniczych przez gromadzących się tzw. gapiów i pozostawiane przez nich środki lokomocji. 10. Ograniczona możliwość działania służb medycznych związana z przepełnieniem szpitali, punktów medycznych i niewystarczającymi ilościami środków opatrunkowych i farmakologicznych.	Duży – H (prawdopodobne)	3
<u>Podłożenie ładunku wybuchowego z zastosowaniem:</u> - środka mikrobiologicznego	Średnie – M	1. Zagrożenie życia i zdrowia ludzi. 2. Wystąpienie objawów paniki wśród ludności, brak reakcji na wydawane polecenia, nieprzestrzeganie obowiązującego porządku prawnego. 3. Wzrost przestępczości o charakterze kryminalnym. Zwiększona liczba przestępstw i wykroczeń pospolitych (kradzieże z włamaniem, kradzieże, rozboje, niszczenie mienia). 4. Duże zainteresowanie osób postronnych i środków masowego przekazu.	Duży – H (prawdopodobne)	3

<u>Podłożenie ładunku wybuchowego z zastosowaniem:</u> - środka chemicznego	Średnie – M	1. Zagrożenie życia i zdrowia obywateli objętych atakiem i możliwość szybkiego rozprzestrzeniania się zagrożenia na tereny jeszcze niezagrożone. 2. Wzrost zachorowań i zgonów związanych z zatruciem i skażeniem chemicznym. 3. Konieczność hospitalizacji dużej liczby pacjentów w przypadku zatrucia środkiem chemicznym. 4. Powstanie katastrofy ekologicznej, budowlanej. 5. Niechęć do opuszczenia miejsc zamieszkania czy też przebywanie ludności w strefie zagrożonej. 6. Dewastacja i grabież mienia prywatnego i publicznego pozostawionego na czas ewakuacji ludności z terenu potencjalnie zagrożonego skażeniem chemicznym. 7. Wprowadzenie do sprzedaży skażonej żywności. 8. Powstanie chaosu w miejscu prowadzonych działań ratowniczych oraz zakłócenie bezpieczeństwa i porządku publicznego w czasie prowadzonej akcji ratowniczej. 9. Wystąpienie zakłóceń na ciągach komunikacyjnych tras przewidzianych do ewakuacji ludności, dojazdów służb policyjnych i ratowniczych przez pozostawiane środki lokomocji. 10. Możliwy wzrost zachorowań i zgonów wśród funkcjonariuszy Policji i innych osób biorących udział w działaniach ratowniczych. 11. Ograniczona możliwość działania służb medycznych, związana z przepełnieniem szpitali, punktów medycznych i niewystarczającymi ilościami środków opatrunkowych i farmakologicznych.	Duży – H (prawdopodobne)	3
<u>Uprowadzenie środka transportu w komunikacji lotniczej</u>	Wysokie – H	1. Poważne niebezpieczeństwo dla znajdujących się na pokładzie środka transportu pasażerów i załogi. 2. Możliwość ewentualnej katastrofy lotniczej jako: - zagrożenie życia dla pasażerów i załogi, - zagrożenie życia dla ludności znajdującej się na powierzchni ziemi, - zniszczenie różnego rodzaju obiektów znajdujących się na po-	Duży – H (prawdopodobne)	3

		wierzchni ziemi, - pożar. 3. Zagrożenie bezpieczeństwa innych środków transportu znajdujących się w tym samym czasie w przestrzeni powietrznej: - możliwość kolizji w powietrzu ze skutkami jak wyżej. 4. Wzięcie zakładników, w tym VIP-ów. 5. Nielegalne przekroczenie jednej lub kilku granic państwowych z pogwałceniem międzynarodowych przepisów prawnych.		
<u>Uprowadzenie środka transportu w komunikacji lądowej</u>	Wysokie – H	1. Zagrożenie życia oraz zdrowia osób (obsługi, pasażerów) przemieszczających się środkami komunikacji lądowej (pociąg, autobus, metro, inne). 2. Zagrożenie życia i zdrowia innych uczestników ruchu drogowego i pasażerów linii kolejowych. 3. Zagrożenie życia, zdrowia i mienia osób mieszkających przy trasach komunikacyjnych. 4. Żądania wobec rządów obcych państw. 5. Uprowadzenie VIP-ów. 6. Wzięcie zakładników. 7. Zniszczenie mienia państwowego lub prywatnego znacznej wartości. 8. Skażenie środowiska środkami chemicznymi. 9. Spowodowanie pożaru lub wybuchu. 10. Zablokowanie szlaków komunikacyjnych. 11. Wystąpienie nielegalnych zgromadzeń publicznych popierających lub przeciwstawiających się aktowi terroru.	Średni – M (możliwe)	2
<u>Uprowadzenie środka transportu w komunikacji wodnej</u>	Średnie – M	1. Zagrożenie dla życia i zdrowia pasażerów (w tym VIP-ów) i członków załogi. 2. Zagrożenie dla życia i zdrowia innych użytkowników jednostek pływających oraz mieszkańców stref przybrzeżnych. 3. Zagrożenie skażeniem środowiska. 4. Możliwość wystosowania żądań w stosunku do rządów państw, których obywatele zostali zakładnikami. 5. Zatopienie statku na torze wodnym. 6. Zagrożenie dla infrastruktury portów i komunikacji drogowej (mosty).	Średni – M (możliwe)	2

		7. Możliwość nielegalnego przekroczenia granicy.		
Zajęcie obiektu, w tym również z przetrzymywaniem zakładników	Wysokie – H	1. Zagrożenie życia i zdrowia osób znajdujących się w opanowanym przez terrorystów obiekcie. 2. Zagrożenie życia i zdrowia osób znajdujących się w bezpośrednim sąsiedztwie opanowanego obiektu (sąsiednie budynki). 3. Wysunięcie żądań w stosunku do państw obcych, których obywatele zostali zatrzymani w charakterze zakładników przez grupę przestępczą. Skierowanie żądań do właściciela (użytkownika) obiektu - np. w przypadku opanowania budynków konsularnych, ambasad lub szkół dla dzieci personelu dyplomatycznego. 4. Uwolnienie znajdujących się w obiekcie niebezpiecznych substancji chemicznych lub biologicznych, np. poprzez: skażenie ujęć wody pitnej, wprowadzenie do systemów wentylacyjnych środków chemicznych. 5. Nielegalne zgromadzenie przeciwników zaistniałego aktu terroru. 6. Wystąpienie blokady komunikacyjnej uniemożliwiającej przeprowadzenie siłowego przejęcia obiektu. 7. Wysunięcie przez porywaczy nierealnych żądań (politycznych, gospodarczych, osobistych), co może skutkować uszkodzeniem ciała lub fizyczną likwidacją przetrzymywanych osób. 8. Zagrożenie zniszczenia mienia prywatnego lub publicznego, wystąpienie konkretnych strat materialnych, np. w przypadku opanowania pomieszczeń bankowych. 9. Uzyskanie od uprowadzonej osoby (osób) informacji, które mogą służyć do popełnienia innych przestępstw. 10. Zagrożenie dla użytkowników ciągów komunikacyjnych w trakcie trwania pościgu za grupą przestępczą - po opuszczeniu obiektu. 11. Przemieszczanie się grupy przestępczej wraz z uprowadzoną osobą (osobami) w kierunku granicy RP celem jej przekroczenia i opuszczenia terytorium RP. 12. Celowe spowodowanie katastrofy budowlanej przy użyciu materiałów wybuchowych.	Duży – H (prawdopodobne)	3

<u>Uprowadzenie zakładników</u>	Średnie – M	1. Zagrożenie życia i zdrowia uprowadzonej osoby (osób). 2. Zagrożenie życia i zdrowia osoby (osób) mającej styczność z grupą przestępczą lub osoby prowadzącej pertraktacje z porywaczami bez wiedzy organów ścigania. 3. Wystąpienie z żądaniami w stosunku do państw obcych, których obywatele zostali uprowadzeni przez grupę przestępczą. 4. Zagrożenie nielegalnymi zgromadzeniami przeciwstawiających się zaistniałemu aktowi terroru. 5. Wysuniecie przez porywaczy nierealnych żądań (politycznych, gospodarczych, osobistych), co może skutkować uszkodzeniem ciała lub fizyczną likwidacją uprowadzonej osoby (osób). 6. Wystąpienie blokady komunikacyjnej w miejscu zlokalizowania grupy przestępczej wraz z uprowadzoną osobą (osobami). 7. Zagrożenie zniszczenia mienia prywatnego lub publicznego. 8. Uzyskanie od uprowadzonej osoby (osób) informacji, które mogą służyć do popełnienia innych przestępstw. 9. Zagrożenie dla użytkowników ciągów komunikacyjnych w trakcie trwania pościgu za grupą przestępczą (przemieszczającą się z uprowadzoną osobą). 10. Przemieszczanie się grupy przestępczej wraz z uprowadzoną osobą (osobami) w kierunku granicy RP celem jej przekroczenia i opuszczenia terytorium RP.	Średni – M (możliwe)	2
<u>Zagrożenie atakiem terrorystycznym z powietrza typu "Renegade"</u> • zidentyfikowanie cywilnego statku powietrznego, który zachowuje się w taki sposób, że powstaje podejrzenie, iż może być użyty do wykonania ataku terrorystycznego z powietrza (określany jako samolot typu "Renegade"), • lądowanie samolotu określanego jako	Wysokie – H	1. Zagrożenie życia oraz zdrowia osób przemieszczających się samolotem określanym jako samolot typu "Renegade". 2. Możliwość staranowania przez uprowadzony środek transportu komunikacji lotniczej (z użyciem materiałów wybuchowych lub posiadanego zapasu paliwa) ważnego obiektu gospodarczego lub obiektu użyteczności publicznej. 3. Zagrożenie życia i zdrowia współuczestników przemieszczających się innymi środkami komunikacji lotniczej. 4. Żądania wobec rządów obcych państw, których obywatele są pasażerami środków transportu w komunikacji lotniczej.	Duży – H (prawdopodobne)	3

samolot typu "Renegade" na lotnisku interwencyjnym, • lądowanie awaryjne samolotu określanego jako samolot typu "Renegade" poza lotniskiem interwencyjnym.		5. Zagrożenie życia, zdrowia i mienia osób mieszkających na trasie przelotu samolotu określanego jako samolot typu "Renegade" oraz w pobliżu lotniska interwencyjnego. 6. Blokada lotniska poprzez unieruchomienie środka transportu komunikacji lotniczej. 7. Występowanie nielegalnych zgromadzeń publicznych popierających (lub się przeciwstawiających) zaistniałemu aktowi terroru. 8. Możliwość uwolnienia przewożonych niebezpiecznych substancji (środków toksycznych, promieniotwórczych, paliw płynnych). 9. Uprowadzenie środka komunikacji lotniczej poza granice RP.		

Tabela 5. Skala punktowa standardowej matrycy ryzyka

Prawdopodobieństwo	**Skutek**		
	H=3	M=2	L=1
H=3	9	6	3
M=2	6	4	2
L=1	3	2	1

Tabela 6. Skala punktowa dla zdarzeń zawartych w tabeli 3

Zdarzenie	**Prawdopodobieństwo**	**Skutek**		
		H=3	**M=2**	**L=1**
Atak bezpośredni na obiekt	Wysokie – H **3**	Duży – M **9**		
Podłożenie ładunku wybuchowego	Wysokie – H **3**	Duży – H **9**		
Podłożenie ładunku wybuchowego z zastosowaniem: - środka mikrobiologicznego	Średnie – M **2**	Duży – H **6**		
Podłożenie ładunku wybuchowego z zastosowaniem: - środka chemicznego	Średnie – M **2**	Duży – H **6**		

Uprowadzenie środka transportu w komunikacji lotniczej	Wysokie – H **3**	Duży – H **9**		
Uprowadzenie środka transportu w komunikacji lądowej	Wysokie – H **3**		Średni – M **6**	
Uprowadzenie środka transportu w komunikacji wodnej	Średnie – M **2**		Średni – M **4**	
Zajęcie obiektu, w tym również z przetrzymywaniem zakładników	Wysokie – H **3**	Duży – H **9**		
Uprowadzenie zakładników	Średnie – M **2**		Średni – M **4**	
Zagrożenie atakiem terrorystycznym z powietrza typu "Renegade"	Wysokie – H **3**	Duży – H **9**		

Poszczególne kategorie ryzyka przedstawiają się następująco:

- ryzyko tolerowane, r = 1÷2;
- ryzyko kontrolowane, r = 3÷4;
- ryzyko nieakceptowane, r = 6÷9.

Kompensacja ryzyka związanego z ochroną miast polskich w warunkach zagrożeń terrorystycznych ma miejsce w sytuacji, gdy istnieje możliwość współdziałania cywilnych i wojskowych sił odpowiedzialnych za bezpieczeństwo. Określenie ścisłych ram współdziałania podmiotów odpowiedzialnych za bezpieczeństwo miast polskich oznacza szansę na bezpośrednią kompensację ryzyka.

Złożoność prezentowanych szczegółowych zagrożeń atakiem terrorystycznym stanowi o treści wspólnych połączonych policyjno – wojskowych działań w ochronie miast polskich, których celem może być:

- zniechęcenie (odstraszanie) potencjalnych sprawców ataków terrorystycznych;
- właściwie zorganizowana cywilno – wojskowa ochrona miast przed zagrożeniami terrorystycznymi;
- minimalizacja skutków zagrożeń atakami terrorystycznymi w miastach;
- ochrona życia i zdrowia obywateli przed bezprawnymi zamachami;
- zapewnienie ochrony i nienaruszalności obiektów infrastruktury krytycznej;

- zapewnienie ciągłości funkcjonowania organów władzy i administracji oraz służb państwowych.

W świetle aktualnych zagrożeń terrorystycznych uzasadniających potrzeby udziału różnych sił, celowe jest aby połączone działania zapewniały:

- możliwie szybkie, elastyczne i efektywne rozwijanie sił i środków oraz odpowiednio wczesne reagowanie na zagrożenia;
- skuteczność w działaniu i niezakłócone przechodzenie od jednego rodzaju działań w następne zarówno w przypadku eskalacji jak i deeskalacji działań;
- możliwość zachowania zdolności i gotowości Sił Zbrojnych RP do realizacji głównej funkcji – ochrony i obrony terytorium państwa i realizacji zobowiązań sojuszniczych;
- możliwość zachowania zdolności i gotowości do działań sił policyjnych i innych podmiotów odpowiedzialnych za bezpieczeństwo wewnętrzne;
- połączoność działań wszystkich sił i środków zaangażowanych w ochronę miast przed zagrożeniami terrorystycznymi oraz jednolite kierowanie działaniami.

Wymaga to w szczególności podjęcia zawczasu odpowiednich przygotowań organizacyjnych (instytucjonalizacji) oraz osiągnięcia gotowości koordynowania połączonych działań. Konieczna jest organizacja odpowiadająca istocie połączonych działań – umożliwiająca tworzenie połączonych sztabów / zespołów kierowania na stanowiskach kierowania, koncentrację niezbędnych sił wszystkich podmiotów odpowiedzialnych za bezpieczeństwo wewnętrzne oraz wspólnych procedur regulujących wzajemne relacje zapewniające uzyskanie efektu synergii.

Połączone sztaby / kierownictwa powinny uzyskiwać kompetencje niezbędne do utrzymania stanu pogotowia i gotowości podporządkowanych (przydzielonych) sił, planowania oraz prowadzenia działań przeciwterrorystycznych.

Złożony charakter występujących zagrożeń w ochronie miast i duża liczba podmiotów uczestniczących w przeciwdziałaniu wymaga:

- celowości łączenia konkretnych działań wytypowanych sił;
- jedności dowodzenia sprowadzającej się do podporządkowania sił jednej osobie oraz uzgadniania zadań i określenia kompetencji koordynacji na zasadzie współpracy;
- zapewnienia dużej swobody działania wynikającej z uzyskania uprawnień, ale też i obowiązku podejmowania koniecznej inicjatywy;

- szacowania ryzyka podejmowanych działań i zapewnienie maksymalnego bezpieczeństwa uczestniczących w nim sił;
- adekwatności użycia sił w konkretnej sytuacji;
- racjonalności dysponowania siłami i środkami odpowiednio do otrzymanych zadań (sytuacji);
- koncentracji połączonych wysiłków w czasie i przestrzeni;
- pozyskiwania akceptacji społecznej i poparcia dla legalnego (zgodnego z prawem) i uzasadnionego oraz powściągliwego (odpowiednio do sytuacji) użycia sił i środków;
- integracji wojskowych i cywilnych systemów łączności;
- monitorowania rozwoju sytuacji;
- stałej współpracy ze środkami masowego przekazu i zachowania określonej polityki informacyjnej

3.3. Cechy i zdolności sił przeznaczonych do zwalczania zjawiska terroryzmu w aglomeracjach miejskich

Jest rzeczą powszechnie wiadomą, że zmiana charakteru **wyzwań**[120] powoduje zmianę sposobów reakcji na ich zaistnienie. Na przełomie wieków wyzwania czysto militarne, ustępują miejsca zupełnie innym wyzwaniom. Przestępczość zorganizowana, terroryzm, konflikty na tle politycznym, społecznym, ekonomicznym, narodowościowym i religijnym, oraz różne formy skrajnego nacjonalizmu, niekontrolowany przemyt narkotyków, broni, destrukcyjne działania służb specjalnych i rozpad struktur państwa to **zagrożenia i szanse o stosunkowo dużym stopniu ryzyka**, z którymi musimy się zmierzyć. Dla bezpieczeństwa dużych aglomeracji miejskich równie destabilizującymi są katastrofy naturalne, degradacje środowiska oraz epidemie lub pandemie.

Terrorystyczne ataki na budynki WTC w Nowym Yorku oraz siedzibę Pentagonu w Waszyngtonie otworzyły zupełnie nowy rozdział w historii walki z terroryzmem. **Brawurowa, doskonale zaplanowana i przeprowadzona akcja, którą należy bezwzględnie potępić ze strony moralnej, odniosła pod względem strategicznym sukces**. Potężne państwo, światowy hegemon, zostało zaatakowane przez

---

[120] Wyzwania tu: zagrożenia i szanse wraz z towarzyszącym im ryzykiem.

organizację terrorystyczną, której zasoby nie wskazywały na możliwość bezpośredniej walki z tak silnym przeciwnikiem. Destabilizacja życia w strefie bezpośrednich uderzeń, długofalowe oddziaływanie na społeczeństwo, powiązane z obniżeniem zaufania obywateli do zdolności obronnych państwa, stanowić może wręcz książkowy **przykład działań terrorystycznych, umożliwiających osiągnięcie zakładanych celów politycznych, jeszcze poniżej progu wojny**. Dzisiejsze wyzwania muszą zatem stanowić podstawę do tworzenia strategii jutra. Przyszłość jak zwykle jest określoną niewiadomą, którą staramy się „dostrzec", „zdefiniować" i przygotować na jej przyjście. Każda, nawet wydawałoby się „najlepsza" strategia niesie jednak ze sobą określone ryzyko. Jest ono „wliczone" w samo jej tworzenie, bowiem założenia przyjęte do jej „budowy" stanowią o jej powodzeniu lub klęsce. **Przygotowanie aglomeracji miejskich na odparcie uderzenia terrorystycznego, czy też zniwelowanie do minimum przesłanek umożliwiających jego zaistnienie jest rzeczą z gruntu niemożliwą do spełnienia**. Możemy jedynie ową możliwość zaistnienia aktu terroru znacząco obniżyć lub opracować procedury ułatwiające szybki powrót do „normalności" w przestrzeni objętej destabilizacją, cokolwiek by ona nie oznaczała. Dopóki bowiem istnieć będą źródła terroryzmu lub przesłanki do jego zaistnienia, dopóty będziemy mogli jedynie przeciwstawić się zaistniałym aktom terroru, likwidując fizycznie jego twórców i odbudowując utraconą infrastrukturę.

Pozostaną jednakże każdorazowo szkody niemożliwe do naprawienia, nie odbudujemy przecież strat moralnych i nie przywrócimy życia, tym którzy zginą w aktach terroru. To jedynie **napędzać będzie kolejną spiralę przemocy, która jest swoistą polityką, bowiem jak stwierdza C. Wright Mills *„[...] polityka to walka o władzę, a ostatecznym rodzajem władzy jest przemoc"*.**[121] **Zaś *„(...) terroryzm jest tam, gdzie przecinają się polityka i przemoc w nadziei dostarczenia władzy. Terroryzm zawsze dotyczy dążenia do władzy: potrzebnej, by dominować i wywierać przymus, zastraszać i kontrolować, a ostatecznie wprowadzać zasadniczą zmianę polityczną*."**[122] jak stwierdza w swej pracy „Oblicza terroryzmu" B. Hoffman,

Należy sądzić, że podstawowymi działaniami skierowanymi przeciwko terroryzmowi w aglomeracjach miejskich, będą: działania rozpoznawczo - monitorujące, wzmacnianie ochrony infrastruktury krytycznej, zatrzymywanie bądź likwidowanie

---

[121] C. Wright Mills. The Power Elite. Oxford University Press 1956, s. 171.
[122] B. Hoffman. Oblicza terroryzmu. Warszawa 1999, s. 174.

osób biorących udział w działaniach terrorystycznych oraz uwalnianie zakładników i „odzyskiwanie" obiektów przejętych przez terrorystów. **Przy aktualnych założeniach legislacyjnych działania te stanowić będą domenę sił policyjnych, a działania wojsk specjalnych będą miały charakter uzupełniający**.

Możemy jednakże postawić tezę, że w sposób wręcz niezauważalny **zbliżamy się do granicy, po przekroczeniu której trudno będzie jednoznacznie, według dzisiejszych kryteriów, zdefiniować i rozdzielić funkcje dwóch podstawowych narzędzi podmiotu, tzn.: sił zbrojnych i policji**, zadaniem których najprościej rzecz ujmując, jest zapewnienie jego stabilnego i bezpiecznego bytu. **Oznacza to, że konieczność przeciwstawienia się zjawisku terroryzmu może doprowadzić do swoistej fuzji tych dwóch narzędzi i wytworzenie jednego narzędzia, które łączyć będzie w sobie ich cechy i zdolności**.

Powyższe konstatacje potwierdzają zatem konieczność identyfikacji pożądanych cech i zdolności sił przeznaczonych do działań skierowanych przeciwko terroryzmowi w aglomeracjach miejskich (do dalszych rozważań przyjmijmy określenie: *siły przeciwterrorystyczne*). Jest rzeczą oczywistą, że możemy jedynie wskazać na określone cechy i zdolności przez pryzmat prognozowanych wyzwań oraz rosnącej nieprzewidywalności i turbulencyjności zmian w badanym obszarze, zwłaszcza pod kątem bezpieczeństwa aglomeracji miejskich. Dlatego też w niniejszym rozdziale **nie będziemy eksponować tych cech i zdolności, które np.: w wypadku sił zbrojnych będą istotne z punktu widzenia prowadzenia działań zbrojnych poza granicami kraju, skupimy się jedynie na tych elementach i wyznacznikach, które są pożądane z punktu widzenia działań na obszarze kraju i w dużych aglomeracjach miejskich.**

Identyfikację pożądanych (koniecznych) cech i zdolności sił przeciwterrorystycznych musi oczywiście poprzedzić określenie możliwie pełnego zbioru determinantów owych cech i zdolności, oraz jego względne uporządkowanie. Szacunkowe rozmiary tego zbioru i jego swoiste rozmycie powodują znaczący brak możliwości ich pełnego dookreślenia, nawet dla odpowiednio dużego zespołu badawczego, dlatego też mimo właściwego dla badanego obszaru podejścia metodologicznego, ostatecznie przyjęte rozwiązanie problemu może wydać się znacznie uproszczone i zredukowane do niezbędnego minimum. Proces poszukiwań zespół badawczy rozpoczął od rozwiązania problemu nadrzędnego dla prowadzonych rozważań. Problem nadrzędny sformułowano i przedstawiono w rozdziale trzecim w formie analizy, oceny oraz

zarządzania ryzykiem w systemie cywilno – wojskowej ochrony miast polskich w warunkach zagrożeń terrorystycznych. Przyjęte rozwiązanie problemu stało się kluczowym dla określenia cech i zdolności sił przeciwterrorystycznych.

W rezultacie przeprowadzonych rozważań otrzymano pożądany zbiór obszarów określających determinanty użycia sił przeciwterrorystycznych w aglomeracjach miejskich, co znacznie ułatwiło i umożliwiło prowadzenie właściwych dociekań w obszarze badawczym. Przypomnijmy, że podstawę przeprowadzonej analizy stanowił między innymi rodzaj ataku terrorystycznego, co wyznaczało jednocześnie określony zbiór obszarów determinujących poszukiwane cechy i zdolności sił przeciwterrorystycznych (tabela nr 7).

Tabela 7. Pożądane cechy i zdolności sił przeciwterrorystycznych w kontekście obszarów determinujących ich użycie w aglomeracjach miejskich

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
Bezpośredni atak na obiekt	
• skuteczne w osłonie kontrterrorystycznej obszaru aglomeracji i reagujące na sytuacje kryzysowe; • możliwość minimalizacji skutków zagrożeń atakami terrorystycznymi w aglomeracji; • zapewnienie ochrony i stabilnego funkcjonowania obiektów infrastruktury krytycznej; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • skuteczne w ochronie VIP; • zrobotyzowane w zakresie usuwania niebezpiecznych ładunków; • stosujące sztuczną inteligencje i wirtualną rzeczywistość w starciu z cyberterrorystami;	• natychmiastowej reakcji i przetrwania; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • szybkiego pozyskiwania informacji, szybkiej analizy i dystrybucji; • wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do fizycznej eliminacji i ich właściwej oceny; • walki asymetrycznej i obrony przed działaniami asymetrycznymi; • prowadzenia działań przeciwterrorystycznych w cyberprzestrzeni; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji de-

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
• manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • odporne na uderzenia z użyciem środków chemicznych, biologicznych i radiologicznych; • posiadające uporczywą zdolność do działania; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • zapewniające ciągłość funkcjonowania organów władzy i administracji oraz służb państwowych; • zniechęcające potencjalnych sprawców aktów terrorystycznych; • kreatywne w działaniu, różnorodne i nowatorskie; • błyskawicznie się komunikujące; • wyposażone w broń nie zabijającą ; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	cyzyjnej; • działające w środowisku skażeń; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • skutecznego negocjowania ze sprawcami aktu; • prowadzenia długotrwałych operacji wyniszczających; • skutecznego odstraszania; • prowadzenia działań z wykorzystaniem broni nie zabijających jedynie w celu zapewnienia bezpieczeństwa zakładnikom; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.
Podłożenie ładunku wybuchowego	
• skuteczne w osłonie kontrterrorystycznej obszaru aglomeracji i reakcji na sytuacje kryzysowe; • możliwość minimalizacji skutków detonacji ładunku; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie usuwania niebezpiecznych ładunków; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • posiadające uporczywą zdolność do	• natychmiastowej reakcji i działania; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • szybkiego obiegu informacji; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu;

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
działania; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • kreatywne w działaniu, różnorodne i nowatorskie; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	• skutecznego negocjowania ze sprawcami; • skuteczne w wykorzystaniu wysokich technologii.
Podłożenie ładunku wybuchowego z zastosowaniem materiału promieniotwórczego	
• odporne na uderzenia z użyciem środków chemicznych, biologicznych i radiologicznych; • możliwość minimalizacji skutków zastosowania materiału promieniotwórczego; • dysponujące środkami zakłócającymi przekaźniki radiowe; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • kreatywne w działaniu, różnorodne i nowatorskie; • zrobotyzowane w zakresie usuwania niebezpiecznych ładunków; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • posiadające uporczywą zdolność do działania; • unikające „standaryzacji" metody działania; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	• działające środowisku skażeń; • skutecznego negocjowania ze sprawcami aktu; • natychmiastowej reakcji i przetrwania; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • szybkiego pozyskiwania informacji, szybkiej analizy i dystrybucji; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.
Podłożenie ładunku wybuchowego z zastosowaniem środka mikrobiologicznego	
• odporne na uderzenia z użyciem środków mikrobiologicznych; • dysponujące środkami wykrywania potencjalnie niebezpiecznych ładunków; • możliwość minimalizacji skutków użycia	• działające środowisku skażeń; • natychmiastowej reakcji i przetrwania; • skutecznego negocjowania ze sprawcami aktu;

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
środków mikrobiologicznych; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie usuwania niebezpiecznych ładunków; • posiadające uporczywą zdolność do działania; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • błyskawicznie się komunikujące; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	• wykorzystywania szans; • minimalizacji ryzyka; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • walki asymetrycznej i obrony przed działaniami asymetrycznymi; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • błyskawicznej adaptacji do sytuacji decyzyjnej; • skutecznego odstraszania; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.
Podłożenie ładunku wybuchowego z zastosowaniem środka chemicznego	
• odporne na uderzenia z użyciem środków chemicznych; • dysponujące środkami wykrywania potencjalnie niebezpiecznych ładunków; • możliwość minimalizacji skutków użycia środków mikrobiologicznych; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie usuwania niebezpiecznych ładunków; • posiadające uporczywą zdolność do działania; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • zniechęcające potencjalnych sprawców aktów terrorystycznych; • kreatywne w działaniu, różnorodne i	• działające środowisku skażeń; • natychmiastowej reakcji i przetrwania; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • skutecznego negocjowania ze sprawcami aktu; • skutecznego odstraszania; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
nowatorskie; • błyskawicznie się komunikujące; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	
Uprowadzenie środka transportu w komunikacji lotniczej	
• możliwość osłony kontrterrorystycznej portów lotniczych i reakcja na sytuacje kryzysowe; • możliwość minimalizacji zagrożeń atakiem terrorystycznym portu lotniczego; • zapewnienie ochrony i stabilnego funkcjonowania obiektów infrastruktury krytycznej portów lotniczych; • posiadające zdolność do działania w przestrzeni powietrznej; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie śledzenia obiektów ruchomych; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • zniechęcające potencjalnych sprawców aktów terrorystycznych; • kreatywne w działaniu, różnorodne i nowatorskie; • błyskawicznie się komunikujące; • wyposażone w broń nie zabijającą ; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	• natychmiastowej reakcji i przetrwania w przestrzeni powietrznej; • skuteczne w przestrzeni powietrznej; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do fizycznej eliminacji i ich właściwej oceny; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • szybkiego pozyskiwania informacji, szybkiej analizy i dystrybucji; • prowadzenia działań przeciwterrorystycznych w cyberprzestrzeni; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • skutecznego negocjowania ze sprawcami aktu; • skutecznego odstraszania; • prowadzenia działań z wykorzystaniem broni nie zabijających jedynie w celu zapewnienia bezpieczeństwa zakładnikom; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
Uprowadzenie środka transportu w komunikacji lądowej	
• możliwość osłony kontrterrorystycznej obiektów komunikacji lądowej wchodzących w skład infrastruktury krytycznej i reakcja na sytuacje kryzysowe; • możliwość minimalizacji możliwości zaistnienia aktu terrorystycznego w aglomeracji; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie śledzenia obiektów ruchomych; • stosujące sztuczną inteligencje i wirtualną rzeczywistość w starciu z porywaczami; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • posiadające uporczywą zdolność do działania przestrzeni lądowej; • unikające „standaryzacji" metod działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • kreatywne w działaniu, różnorodne i nowatorskie; • błyskawicznie się komunikujące; • wyposażone w broń nie zabijającą ; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	• natychmiastowej reakcji i działania w przestrzeni lądowej; • skuteczne w przestrzeni lądowej; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • szybkiego pozyskiwania informacji, szybkiej analizy i dystrybucji; • wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do fizycznej eliminacji i ich właściwej oceny; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • skutecznego negocjowania ze sprawcami aktu; • skutecznego odstraszania; • prowadzenia działań z wykorzystaniem broni nie zabijających jedynie w celu zapewnienia bezpieczeństwa zakładnikom; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.
Uprowadzenie środka transportu w komunikacji wodnej	
• możliwość osłony kontrterrorystycznej obiektów komunikacji wodnej wchodzących w skład infrastruktury krytycznej i reakcja na sytuacje kryzysowe; • są w stanie osłaniać kontrterrorystycznie obszar aglomeracji i reagować na	• natychmiastowej reakcji i działania w środowisku wodnym; • skuteczne w środowisku wodnym; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
sytuacje kryzysowe; • zapewnienie ochrony i stabilnego funkcjonowania obiektów infrastruktury krytycznej; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie śledzenia obiektów ruchomych; • stosujące sztuczną inteligencje i wirtualną rzeczywistość w starciu z terrorystami; • posiadające uporczywą zdolność do działania w środowisku wodnym; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • zniechęcające potencjalnych sprawców aktów terrorystycznych; • kreatywne w działaniu, różnorodne i nowatorskie; • błyskawicznie się komunikujące; • wyposażone w broń nie zabijającą ; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	aktu terrorystycznego; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do ich fizycznej eliminacji i właściwej oceny; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • skutecznego negocjowania ze sprawcami aktu; • skutecznego odstraszania; • prowadzenia działań z wykorzystaniem broni nie zabijających jedynie w celu zapewnienia bezpieczeństwa zakładnikom; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.
Zajęcie obiektu, w tym również z przetrzymywaniem zakładników	
• są w stanie osłaniać kontrterrorystycznie obszar aglomeracji i reagować na sytuacje kryzysowe; • możliwość minimalizacji możliwości zaistnienia aktów tego typu w obiektach infrastruktury krytycznej aglomeracji; • skuteczne w ochronie VIP; • zapewnienie ochrony i stabilnego funkcjonowania obiektów infrastruktury kry-	• natychmiastowej reakcji i działania; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do fizycznej eliminacji i ich właściwej oceny; • prowadzenia działań z wykorzystaniem broni nie zabijających jedynie w celu zapewnienia bezpieczeństwa zakładni-

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
tycznej; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie śledzenia terrorystów w obiektach aglomeracji; • stosujące sztuczną inteligencje i wirtualną rzeczywistość w starciu z terrorystami; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • posiadające uporczywą zdolność do działania; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • zapewniające ciągłość funkcjonowania organów władzy i administracji oraz służb państwowych; • zniechęcające potencjalnych sprawców aktów terrorystycznych; • kreatywne w działaniu, różnorodne i nowatorskie; • błyskawicznie się komunikujące; • posiadać kluczowe zasoby uzupełniające; • ochrona życia i zdrowia obywateli przed bezprawnymi zamachami; • zapewnienie ochrony i nienaruszalności obiektów infrastruktury krytycznej; • wyposażone w broń nie zabijającą ; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	kom; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • prowadzenia działań przeciwterrorystycznych w cyberprzestrzeni; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • skutecznego negocjowania ze sprawcami aktu; • skutecznego odstraszania; • asymetryczne; • wielowymiarowe; • zdolne do błyskawicznej adaptacji; • błyskawicznie się komunikujące; • oparte na wiedzy i informacji; • niemoralne w walce z terroryzmem; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
Uprowadzenie zakładników	
• możliwość osłony kontrterrorystycznej obiektów komunikacji powietrznej, morskiej i lądowej wchodzących w skład infrastruktury krytycznej i reakcja na sytuacje kryzysowe; • są w stanie osłaniać kontrterrorystycznie obszar aglomeracji i reagować na sytuacje kryzysowe; • skuteczne w ochronie VIP; • zapewnienie ochrony i stabilnego funkcjonowania obiektów infrastruktury krytycznej; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie śledzenia obiektów ruchomych oraz sytuacji w obiektach stałych; • stosujące sztuczną inteligencje i wirtualną rzeczywistość w starciu z terrorystami; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • posiadające uporczywą zdolność do działania; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • zniechęcające potencjalnych sprawców aktów terrorystycznych; • kreatywne w działaniu,; • błyskawicznie się komunikujące; • wyposażone w broń nie zabijającą ; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	• natychmiastowej reakcji i działania w przestrzeni powietrznej, lądowej i w środowisku wodnym; • skuteczne w przestrzeni powietrznej, lądowej i w środowisku wodnym; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do fizycznej eliminacji i ich właściwej oceny; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • działające środowisku skażeń; • manipulujące informacją oraz zdolne do wywołania psychologicznego wstrząsu; • skutecznego negocjowania ze sprawcami aktu; • prowadzenia długotrwałych operacji wyniszczających; • skutecznego odstraszania; • prowadzenia działań z wykorzystaniem broni nie zabijających jedynie w celu zapewnienia bezpieczeństwa zakładnikom; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.

POŻĄDANE	
CECHY	**ZDOLNOŚCI**
SIŁ PRZECIWTERRORYSTYCZNYCH	
1	2
Zagrożenie atakiem terrorystycznym z powietrza typu "Renegade"	
• są w stanie osłaniać kontrterrorystycznie obszar aglomeracji i reagować na sytuacje kryzysowe typu "Renegade"; • możliwość minimalizacji skutków zagrożeń atakami terrorystycznymi w aglomeracji; • zapewnienie ochrony i stabilnego funkcjonowania obiektów infrastruktury krytycznej; • manewrowe, elastyczne, szybko przemieszczające się, śmiercionośne; • bezwzględne i niemoralne dla sprawców aktów terrorystycznych; • zrobotyzowane w zakresie ochrony przed atakiem typu "Renegade"; • stosujące sztuczną inteligencje i wirtualną rzeczywistość w starciu z terrorystami; • odporne na uderzenia z użyciem środków chemicznych, biologicznych i radiologicznych; • posiadające uporczywą zdolność do działania; • unikające „standaryzacji" metody działania; • dysponujące odpornym na zakłócenia, stabilnym obiegiem informacji; • zniechęcające potencjalnych sprawców aktów terrorystycznych; • kreatywne w działaniu, różnorodne i nowatorskie; • błyskawicznie się komunikujące; • wyposażone w broń nie zabijającą ; • wyposażone w sprzęt wysoce zaawansowany technologicznie.	• natychmiastowej reakcji i działania; • wykorzystywania informacji i wiedzy w celu zyskania przewagi nad sprawcami aktu terrorystycznego typu "Renegade"; • podejmowania decyzji oraz wyborów w sytuacji ryzyka i niepewności co do jej rozwoju; • szybkiego pozyskiwania informacji, szybkiej analizy i dystrybucji; • wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do ich właściwej oceny oraz fizycznej eliminacji; • walki asymetrycznej i obrony przed działaniami asymetrycznymi; • wykorzystywania szans; • minimalizacji ryzyka; • błyskawicznej adaptacji do sytuacji decyzyjnej; • skutecznego negocjowania ze sprawcami aktu; • skutecznego odstraszania; • prowadzenia działań z wykorzystaniem broni nie zabijających jedynie w celu zapewnienia bezpieczeństwa zakładnikom; • bezwzględne dla sprawców aktu terrorystycznego; • skuteczne w wykorzystaniu wysokich technologii.

Poszukując odpowiedzi na pytanie cząstkowe: *jakie cechy i zdolności do działań w aglomeracjach miejskich powinny posiadać siły przeciwterrorystyczne*, zespół badawczy wygenerował poniższy, postulowany zbiór cech i zdolności sił przeciwterrorystycznych:

- siły przeciwterrorystyczne muszą charakteryzować się kreatywnością, innowacyjnością oraz odejściem od standardowych metod działań w sytuacjach kryzysowych;
- powinny charakteryzować się skutecznością w osłonie kontrterrorystycznej obszaru aglomeracji, doskonałą znajomością jej obiektów infrastruktury krytycznej;
- posiadać zdolność do błyskawicznej reakcji na sytuacje kryzysowe;
- możliwość minimalizacji skutków zagrożeń atakami terrorystycznymi w aglomeracji;
- powinny posiadać zdolność do długofalowego zapewnienia ochrony i stabilnego funkcjonowania obiektów infrastruktury krytycznej w sytuacji podwyższonego ryzyka;
- siły przeciwterrorystyczne powinny być wysoce manewrowe, elastyczne, bezwzględne w działaniu, śmiercionośne dla sprawców aktów terrorystycznych, przez co skutecznie odstraszające;
- bezwzględne i niemoralne dla sprawców aktów terrorystycznych, stosujące klasyczną przemoc wobec przemocy lub groźby jej zaistnienia, a jednocześnie skuteczne w ochronie ludności aglomeracji;
- skuteczne w ochronie VIP, umożliwiając tym samym utrzymanie zdolności władz aglomeracji do niezakłóconego działania;
- muszą posiadać zaawansowane technologicznie systemy rozpoznawczo - śledzące, możliwe do użycia w każdej przestrzeni i środowisku, zdolne do obserwacji celów stacjonarnych i ruchomych, zarówno w obiektach infrastruktury i infrastruktury krytycznej aglomeracji, jak i poza nimi;
- powinny posiadać wsparcie ze strony sił i służb informacyjnych państwa, komunikacji i łączności satelitarnej, tak aby w pełni wykorzystać dostępne spektrum informacji o sytuacji decyzyjnej, przy pełnej integracji wszelkich instytucji w rejonie aglomeracji;

- powinny być wyposażone w zrobotyzowane środki do usuwania niebezpiecznych ładunków, w tym ładunków ze środkami toksycznymi;
- powinny szeroko stosować sztuczną inteligencję i wirtualną rzeczywistość w starciu z cyberterrorystami oraz terrorystami;
- powinny być wyspecjalizowane w prowadzeniu działań i operacji psychologicznych, zdolne do manipulacji informacją na potrzeby operacji przeciwterrorystycznych oraz do wywołania wstrząsu psychologicznego u sprawców;
- powinny być odporne na uderzenia z użyciem środków chemicznych, biologicznych i radiologicznych oraz posiadać umiejętność działania w środowisku po uderzeniach tymi środkami;
- posiadające uporczywą zdolność do działania wspartą odpornym na zakłócenia, stabilnym obiegiem informacji;
- powinny posiadać zdolność do długofalowego wsparcia ciągłości funkcjonowania organów władzy i administracji oraz służb państwowych w aglomeracji;
- powinny być przygotowane do osłony kontrterrorystycznej obszaru aglomeracji i reakcji na sytuacje kryzysowe typu "Renegade";
- swym bezwzględnym działaniem powinny skutecznie odstraszać i zniechęcać potencjalnych sprawców aktów terrorystycznych;
- powinny być nieszablonowe, kreatywne w działaniu, stosujące techniki i metody stanowiące zaskoczenie dla sprawców ataków;
- błyskawicznie się komunikujące;
- powinny być wyposażone w broń nie zabijającą, skuteczne w prowadzeniu działań z wykorzystaniem tej broni, ale jedynie w celu zapewnienia bezpieczeństwa zakładnikom, w każdej innej sytuacji powinni działać bezwzględnie w stosunku do terrorystów ;
- powinny posiadać w pełni nowoczesny, oparty o nanotechnologie, sprzęt wysokiej klasy, zaawansowany technologicznie, umożliwiający skuteczne prowadzenie działalności przeciwterrorystycznej w aglomeracji;
- powinny posiadać zdolność do uzyskania przewagi nad sprawcami aktu terrorystycznego przy pełnym wykorzystywaniu posiadanych informacji i wiedzy o sytuacji kryzysowej;
- być zdolne do podejmowania decyzji oraz wyborów wariantu działania w obliczu ryzyka i niepewności co do rozwoju sytuacji decyzyjnej;

- posiadać zdolność do szybkiego pozyskiwania informacji, szybkiej analizy i dystrybucji (precyzyjny i szybki obieg informacji);
- powinny posiadać zdolność do wykrycia, rozpoznania oraz wiarygodnej lokalizacji celów do ich właściwej oceny i fizycznej eliminacji;
- siły przeciwterrorystyczne powinny być zdolne do walki asymetrycznej i obrony przed uderzeniami asymetrycznymi oraz skutecznie stosować broń precyzyjną
- posiadać zdolność do prowadzenia działań przeciwterrorystycznych w cyberprzestrzeni z wykorzystaniem wszelkich dostępnych środków do walki z informacją i o informację;
- powinny posiadać zdolności do szybkiego wykorzystywania pojawiających się szans i minimalizacji ryzyka w działaniu oraz powinny posiadać strategię przyswajania nowych technologii skoncentrowaną na kluczowych obszarach ich działalności;
- powinny skutecznie i błyskawicznie „adaptować" się do dynamicznych i turbulentnych zmian w sytuacji decyzyjnej;
- powinny być profesjonalnie przygotowane do prowadzenia działań negocjacyjnych;
- posiadać zdolność do prowadzenia skutecznych negocjacji ze sprawcami aktu terrorystycznego w sytuacjach kryzysowych;
- powinny umiejętnie wykorzystywać wiedzę o potencjalnych sprawcach aktów terrorystycznych, umiejętnie prowadzić skuteczne negocjacje, w każdym środowisku i przestrzeni w której przyjdzie im działać;
- powinny być przygotowane do prowadzenia długotrwałych operacji wyniszczających środowisko potencjalnych terrorystów;
- struktura sił przeciwterrorystycznych powinna zostać zbudowana w oparciu zdolnością do umiejętności inicjowania zmian strukturalnych;
- powinny posiadać zdolność do obezwładniania elektronicznego, a tym samym do eliminacji możliwości przeprowadzenia zdalnej detonacji ładunków wybuchowych w ochranianych obiektach infrastruktury krytycznej aglomeracji;
- powinny być zdolne do działań w sytuacjach nieciągłości systemu dowodzenia operacją przeciwterrorystyczną;

- powinny w pełni kontrolować sytuację zachowując przy tym zdolność do funkcjonowania i prowadzenia działań w warunkach zaskoczenia i nieprzewidywalnych zwrotów akcji;
- zdolne do działań „chirurgicznych", obezwładniania zamiast zabijania, minimalizowania zniszczeń i strat, przy jednoczesnym bezwzględnym podejściu do sprawców aktu terrorystycznego;
- powinny posiadać zdolność do działań nowego typu, przy wykorzystaniu środków walki psychologicznej, medialnej, informacyjnej);
- powinny umiejętnie wykorzystywać środowisko asymetryczne jako kluczowy element sukcesu w działaniach przeciwterrorystycznych;
- uzyskiwania i utrzymywania przewagi technologicznej w wybranych dziedzinach, wykorzystania jej w maksymalnym zakresie misji, zadań oraz warunków i form ich realizacji;
- powinny umiejętnie wykorzystywać środki chemiczne i toksyny w toku działań przeciwterrorystycznych, celem minimalizacji strat wśród ludności czy też oswobodzenia zakładników;
- powinny posiadać zdolność do błyskawicznej projekcji siły i zdolności w dowolny obszar aglomeracji;

Powyższe cechy i zdolności sił przeciwterrorystycznych działających w obszarze aglomeracji miejskich, są rezultatem wyboru relatywnie największego prawdopodobieństwa potrzeby ich zaistnienia. Z wygenerowanych w toku badań postulowanych cech i zdolności sił przeciwterrorystycznych, powyżej przedstawiono tylko te, które zdaniem zespołu autorskiego są najbardziej pożądane. Jest to swoistego rodzaju synteza cech i zdolności sił, które zespół rozpatrywał pod kątem działań w aglomeracji miejskiej w warunkach działań wewnętrznych, pomijając tym samym te cechy i zdolności, które stają się niezbędne w trakcie działań sił przeciwterrorystycznych poza granicami kraju.

Wygenerowane zbiór cech i zdolności stanowi jedynie określony pogląd na problem wykorzystania sił przeciwterrorystycznych do zwalczania zjawiska terroryzmu na warunkach określonych w części metodologicznej pracy, co oznacza, że jest zbiorem wymagającym ciągłej weryfikacji i aktualizacji zgodnie z możliwymi do zaistnienia zmianami i potrzebami kształtowanymi przez potrzebę walki ze zjawiskiem terroryzmu.

4. SPOSOBY PRZECIWDZIAŁANIA ZAGROŻENIOM TERRORYSTYCZNYM

Zamach terrorystyczny może być uznany za formę operacji specjalnej. Warto tu przywołać amerykańska definicję wojskowej operacji specjalnej , w myśl której operacje specjalne są to : „operacje prowadzone przez specjalnie zorganizowane, wyszkolone i wyposażone siły wojskowe lub paramilitarne, w celu osiągnięcia celów militarnych, politycznych, gospodarczych lub psychologicznych przy użyciu niekonwencjonalnych środków militarnych we wrogich, nieprzyjaznych lub delikatnych (wrażliwych) politycznie regionach. Operacje te są prowadzone w okresie pokoju, konfliktu i wojny, samodzielnie lub we współpracy z siłami konwencjonalnymi".[123]

Od wojskowych operacji specjalnych terroryzm odróżnia jednak to, że działania te nie mogą być prowadzone przy współpracy sił konwencjonalnych, a także to, że terroryzm łamie zasady międzynarodowego prawa konfliktów zbrojnych. Jednak zasady rządzące wojskowymi operacjami specjalnymi, oraz działaniami terrorystycznymi są praktycznie identyczne.

Są to: niekonwencjonalność działań, zaskoczenie, uzależnienie od danych rozpoznawczych, dominująca rola czynnika ludzkiego.

Działania terrorystyczne są niekonwencjonalne z kilku powodów. Po pierwsze, są one prowadzone w sposób całkowicie odmienny niż działania regularnych sił zbrojnych, wskutek tego, nie podlegają one wielu regułom na których się opierają. Przede wszystkim całkowicie zmienia się charakter prowadzonych walk. O ile w regularnej bitwie łatwiej się bronić, niż atakować, to w zamachu terrorystycznym element obrony prawie nie istnieje. Zbyt duża jest bowiem dysproporcja pomiędzy siłami terrorystów a siłami działającymi w ochronie miast. Z powodu tej dysproporcji, terroryści podejmują walkę tylko na warunkach narzuconych przez siebie, w korzystnej dla nich sytuacji. Każda inna sytuacja oznacza porażkę terrorystów[124].

Z czynnikiem tym wiąże się następny – zaskoczenie. Zaskoczenie umożliwia terrorystom osiągnięcie celu, nawet gdy siły i służby odpowiedzialne za bezpieczeństwo są przygotowane na atak.

Dokonanie skutecznego ataku terrorystycznego bez dobrego rozpoznania jest niemożliwe. Rozpoznanie jest także warunkiem uzyskania zaskoczenia. Informacje te dotyczą zarówno celu ataku, jego otoczenia, jak i reakcji sił i służb odpowiedzialnych

---

[123] Cytat za : H.Królikowski, „Próba definicji" MMS Komandos nr 10/2002

[124] http://www.specops.pl/vortal/taktyka_czarna/walka_z_terrorem/Michal_Piekarski/terrorist_tactics/terrorist_tactics.htm

za ochronę obiektów na zamach (np. czas przybycia sił policyjnych i wojskowych na miejsce ataku, itp.). Brak danych rozpoznawczych oznacza niezdolność do skutecznego działania.

Czynnik ludzki jest jednym z najważniejszych czynników warunkujących skuteczność ataku terrorystycznego. Należy podkreślić, że odmiennie niż u funkcjonariuszy lub żołnierzy sił specjalnych, w przypadku terrorystów główną rolę odgrywa fanatyzm wynikający z ideologii. Nierzadko gotowość do bezwarunkowego, poświęcenia swojego życia dla jakieś sprawy skutkuje możliwością przeprowadzania ataków o wysokim stopniu skuteczności. Mając do dyspozycji ludzi nie dbających o własne życie, można pominąć w planowaniu takie elementy jak np. ewakuacja grupy po wykonaniu ataku. Determinacja i fanatyzm terrorystów mogą także uzupełniać braki w ich wyszkoleniu i wyposażeniu. Jednak im lepiej wyszkolona jest grupa terrorystyczna, tym skuteczniejsze mogą być jej działania. Ma to istotne konsekwencje dla zwalczania zagrożenia terrorystycznego.

Sam przebieg zamachu terrorystycznego może zostać przedstawiony jako sekwencja następujących po sobie elementów. Są to : określenie celu taktycznego, określenie możliwych celów, rozpoznanie, przygotowanie, przeprowadzenie i ewakuacja[125].

Cel taktyczny zamachu wiąże się z dwoma czynnikami. Pierwszym jest cel strategiczny danej grupy terrorystycznej. Drugim jest aktualna sytuacja polityczna wewnątrz państwa – celu oraz sytuacja międzynarodowa. Obydwa te czynniki mogą w różnym stopniu wpływać na cel konkretnego zamachu.

Cel taktyczny będzie determinował kształt dalszych działań terrorystów. Będą one limitowane także przez możliwości terrorystów. Ze zbioru atrakcyjnych dla terrorystów celów ataku, wyodrębniane są te, których zaatakowanie jest aktualnie możliwe.

Następną fazą jest rozpoznanie wybranego celu (obiektu lub osoby) bądź celów, aby określić jaka forma ataku będzie najskuteczniejsza. W oparciu o zebrane informacje, przygotowywany jest atak. W tej fazie przygotowywany jest plan działania, a także gromadzone są środki mające służyć do jego przeprowadzenia (pojazdy, fałszywe dokumenty, broń itp.).

---

[125] Tamże.

Kolejną fazą jest przeprowadzenie zamachu. Forma zamachu może być różna, w zależności od celu. Podstawowe formy zamachów zostały wymienione w trakcie analizy zagrożeń.

Oprócz wyżej wymienionych form zamachów terrorystycznych, możemy mieć też do czynienia z innymi, rzadziej spotykanymi i miej typowymi. Są to działania polegające na wszczynaniu buntów w więzieniach, zamieszek ulicznych, itp. działań. Z reguły angażują one, oprócz samych terrorystów duże grupy ludzi luźno z nimi związanych. Natomiast terroryści będą próbowali przejąć funkcję inspiratorów i prowodyrów takich zajść.

Ostatnim elementem zamachu terrorystycznego jest z reguły ewakuacja terrorystów (o ile nie mamy do czynienia z zamachem samobójczym). Ewakuacja jest właściwie jedynym elementem defensywnym, jaki mogą zastosować terroryści. Jeżeli terroryści zdołali się oddalić z miejsca zamachu nie zwracając niczyjej uwagi, ryzyko bezpośredniego pościgu jest małe. Często stosowaną zasadą jest podzielenie się zamachowców na mniejsze grupy i korzystanie z różnych dróg ewakuacji.

4.1. Przeciwdziałanie zagrożeniom terrorystycznym założenia ogólne

Dotychczas prowadzone badania w aspekcie zagrożeń terrorystycznych miast polskich pozwalają twierdzić, że były one, są i w dającej się przewidzieć przyszłości będą przedmiotem zainteresowania i możliwych ataków grup terrorystycznych. Przeciwdziałanie zagrożeniom terrorystycznym w miastach wymaga podjęcia, obok licznych uregulowań prawnych i przedsięwzięć zarówno taktycznych jak i technicznych, a także działań o charakterze organizacyjnym.

W toku badań ustalono, że przedsięwzięcia organizacyjne powinny wynikać i być planowane oraz podejmowane przede wszystkim przez wzgląd na zbiór właściwości charakteryzujących duże aglomeracje miejski, a ułatwiających przeprowadzenie ataku terrorystycznego oraz na wnioski wypływające z analizy przeprowadzonych dotąd podstawowych źródeł zagrożeń terrorystycznych. Wspomniane przedsięwzięcia powinny dotyczyć sił i środków oraz infrastruktury miejskiej, jak i infrastruktury krytycznej i jej otoczenia.

Dotyczyć to powinno zadań (przedsięwzięć, czynności) realizowanych przez odpowiednie siły w zakresie czynności:

- operacyjno - rozpoznawczych,
- porządkowo – ochronnych,
- przygotowania sił i środków do działań,
- wymiany informacji i współdziałania.

Siły i środki przeznaczone do działań przeciwterrorystycznych w zakresie czynności operacyjno – rozpoznawczych powinny realizować:

1. Rozpoznanie operacyjne dotyczące obywateli polskich oraz cudzoziemców zamieszkałych na stałe lub przebywających czasowo na obszarze miasta, co do których zachodzi podejrzenie działalności o charakterze terrorystycznym, uczestniczenie w grupach, organizacjach lub związkach podejrzewanych o działalność terrorystyczną lub jej wspieranie.
2. Prowadzić rozpoznanie operacyjne grup, organizacji i związków, co do których istnieje podejrzenie o działalność terrorystyczną oraz finansowanie takiej działalności w kraju lub poza jego granicami.
3. Pozyskiwać poufne osobowe źródła informacji wywodzące się z wcześniej wymienionych struktur przestępczych lub umożliwiające bezpośrednie dotarcie do środowisk posiadających wiedzę o nich lub których kontakt z ww. jest podyktowany

wykonywaniem zawodu (np. obsługa hoteli, schronisk, noclegowni, restauracji, instruktorów tzw. szkół przetrwania, agencji towarzyskich).

4. Prowadzić rozpoznanie operacyjne środowisk wywodzących się z państw tzw. wysokiego ryzyka (celem uzyskiwania informacji o osobach wywodzących się z tych środowisk, a w szczególności o: ich liczebności, legalności pobytu i zamiarach, ewentualnej przestępczej działalności, istniejących grupach przestępczych.

W zakresie czynności porządkowo – ochronnych siły i środki powinny:

1. Na bieżąco analizować zagrożenia rejonów i obiektów, ze szczególnym uwzględnieniem miejsc newralgicznych, w tym placówek dyplomatycznych i obiektów użytkowanych przez przedstawicielstwa państw, które w przeszłości były obiektem zamachów terrorystycznych
2. Wzmacniać dodatkową służbą patrolową (policyjno – wojskową) rejony i miejsca które ze względu na przebywanie dużej liczby ludności (dworce kolejowe i autobusowe i inne obiekty komunikacji, centra handlowe, rejony urzędów administracji publicznej, miejsc organizowania imprez masowych itp.) mogą być obiektami ataku
3. Zintensyfikować działania prewencyjne w rejonach lotnisk, w tym prywatnych, oraz portów lotniczych. Nawiązać kontakt z osobami odpowiedzialnymi za zapewnienie bezpieczeństwa tych obiektów w celu określenia stanu ich zabezpieczenia i uzgodnienia sposobu powiadamiania w przypadku zagrożenia.
4. Utrzymywać ścisły nadzór nad specjalistycznymi uzbrojonymi formacjami ochronnymi, zwłaszcza wykonującymi zadania ochronne w obiektach produkcji i przechowywania niebezpiecznych substancji chemicznych, środków uzbrojenia i materiałów wybuchowych poprzez:
   a) sprawdzenie, czy wszystkie obszary, obiekty i urządzenia podlegające obowiązkowej ochronie posiadają uzgodnione plany ochrony oraz czy ochrona wykonywana jest według przygotowanych planów,
   b) nawiązanie kontaktu z osobami odpowiedzialnymi za bezpieczeństwo, poinformowanie ich o możliwych zagrożeniach, przedstawienie rozwiązań dotyczących: - zwiększenia rygorów pełnienia służby i stawiania zadań, - wzmożenia nadzoru nad tymi służbami w zakresie prawidłowości podejmowanych przez nich działań,
   c) wystąpienie do organów samorządowych, na terenie których działają straże gminne, o objęcie przez te straże ochroną obiektów komunalnych.

5. Wzmożenie nadzoru nad konwojowaniem osób, dokumentów i przedmiotów o szczególnym nadzorze.
6. Objęcie szczególną ochroną prewencyjną osób i obiektów podlegających ochronie.
7. Wdrożenie kontroli bezpieczeństwa: samolotów, pasażerów, bagażu w komunikacji lotniczej krajowej i międzynarodowej.

W zakresie czynności przygotowania sił i środków do działań powinny:

1. Zapewnić natychmiastowe, w trybie alarmowym, skierowanie do interwencji zespołów minersko-pirotechnicznych, wydzielonych pododdziałów SZ oraz służb ratowniczych.
2. Zwiększyć mobilność pododdziałów antyterrorystycznych zarówno wojskowych, jak i policyjnych oraz przeprowadzić szkolenia w zakresie alarmowego uruchamiania tych pododdziałów.
3. Dokonać przeglądu, aktualizacji i uzgodnień z właściwymi służbami procedur postępowania w przypadku wystąpienia zdarzeń z użyciem niebezpiecznych środków chemicznych, biologicznych lub radiacyjnych.

W zakresie wymiany informacji i współdziałania powinny:

1. Analizować wszystkie uzyskane informacje na temat możliwości zagrożenia terrorystycznego i wymiana ich z ABW, SWW, SKW, BOR, ŻW, SG oraz innymi jednostkami Policji i innymi służbami porządkowymi.
2. Zapewnić sprawny obieg informacji o możliwych zagrożeniach i zdarzeniach w systemie funkcjonowania służb dyżurnych jednostek policyjnych i wojskowych.
3. Utrzymywać ścisłą wymianę informacji z innymi służbami o zagrożeniach.
4. Międzynarodową grupą PWGT w zakresie rozpoznawania i zwalczania terroryzmu.
5. Europolem i Interpolem.
6. Ościennymi państwami w ramach współdziałania i współpracy transgranicznej.
7. Mediami.

4.2. Organizacja przeciwdziałania zagrożeniom lotnisk jako szczególnego elementu aglomeracji miejskiej[126].

Ze względu na dotychczasowe badania w aspekcie zagrożeń terrorystycznych miast polskich szczególną rolę odgrywają porty lotnicze, co pozwala twierdzić, że były one, są i w dającej się przewidzieć przyszłości przede wszystkim będą przedmiotem zainteresowania i ataków grup terrorystycznych. Przeciwdziałanie zagrożeniom terrorystycznym lotnisk wymaga podjęcia, obok licznych uregulowań prawnych i przedsięwzięć technicznych, także działań o charakterze organizacyjnym, realizowanych zarówno w samym porcie lotniczym, jak i jego najbliższym otoczeniu.

W toku badań ustalono, że antyterrorystyczne przedsięwzięcia organizacyjne powinny wynikać i być planowane oraz podejmowane przede wszystkim przez wzgląd na zbiór właściwości charakteryzujących porty lotnicze, a ułatwiających przeprowadzenie ataku terrorystycznego oraz na wnioski wypływające z analizy przeprowadzonych dotąd podstawowych źródeł zagrożeń terrorystycznych. Wspomniane przedsięwzięcia powinny dotyczyć personelu i klientów portów i linii lotniczych, infrastruktury portu lotniczego, i jego otoczenia, struktury przestrzeni powietrznej obejmującej procedury startu i lądowania statków powietrznych oraz przebywających na płycie lotniska, startujących i lądujących statków powietrznych.

Do właściwości portu lotniczego ułatwiających atak terrorystyczny zaliczono:

- duży przepływ ludzi i bagaży z różnych kierunków świata (choroby zakaźne, substancje przenoszone na ubraniu);
- obecność osób ważnych, znanych, sławnych;
- duży obszar, trudny do skontrolowania i wyizolowania;
- duża liczba pracowników lotniska (brak możliwości całkowitej kontroli tych osób i ich intencji, możliwość sabotażu);
- nagromadzenie znacznej ilości substancji łatwopalnych (w magazynach i w samolotach, także gazy: tlen);
- duże uzależnienie poziomu bezpieczeństwa od techniki, sprzętu, zasilania (urządzenia radionawigacyjne, łączność lotnicza, bramki pirotechniczne itp.);
- stosunkowa łatwość zdezorganizowania lotów poprzez zakłócenie częstotliwości lotniczych, podszycie się pod kontrolera – podawania błędnych komend,

---

[126] Autorzy celowo opisali przeciwdziałanie zagrożeniom terrorystycznym lotnisk, gdyż są one szczególnym elementem infrastruktury krytycznej w aglomeracjach miejskich, a zatem najbardziej narażonym obiektem ataków terrorystycznych.

wykonanie lotu na podejściu Np. paralotnią, modelem lub aparatem bezzałogowym. Możliwość spowodowania w ten sposób nawet katastrofy;

- stałe, duże zagęszczenie osób na stosunkowo niedużej powierzchni;
- ograniczone i zamknięte strefy w terminalach potęgujące niekorzystne oddziaływanie w przypadku paniki;
- współzależność poszczególnych służb lotniskowych (wyeliminowanie jednej tylko grupy np. kontrolerów, kierowców cystern, strażaków może spowodować duże zagrożenie);
- łatwość podłożenia ładunku niebezpiecznego (samo pozostawienie bagażu) powoduje paraliż terminala (zarządzana jest ewakuacja) – na część przylotową i odlotową można dostać się bez przechodzenia przez jakąkolwiek kontrolę.

Natomiast z przeprowadzonych analiz i ocen wynika następująca hierarchia zagrożeń terrorystycznych portów lotniczych atakami z wykorzystaniem:

1. materiałów wybuchowych;
2. przenośnych przeciwlotniczych zestawów rakietowych;
3. granatników i broni strzeleckiej;
4. uprowadzonych statków powietrznych;
5. cyberterroryzmu;
6. min przeciwlotniczych;
7. środków przeciwpancernych.

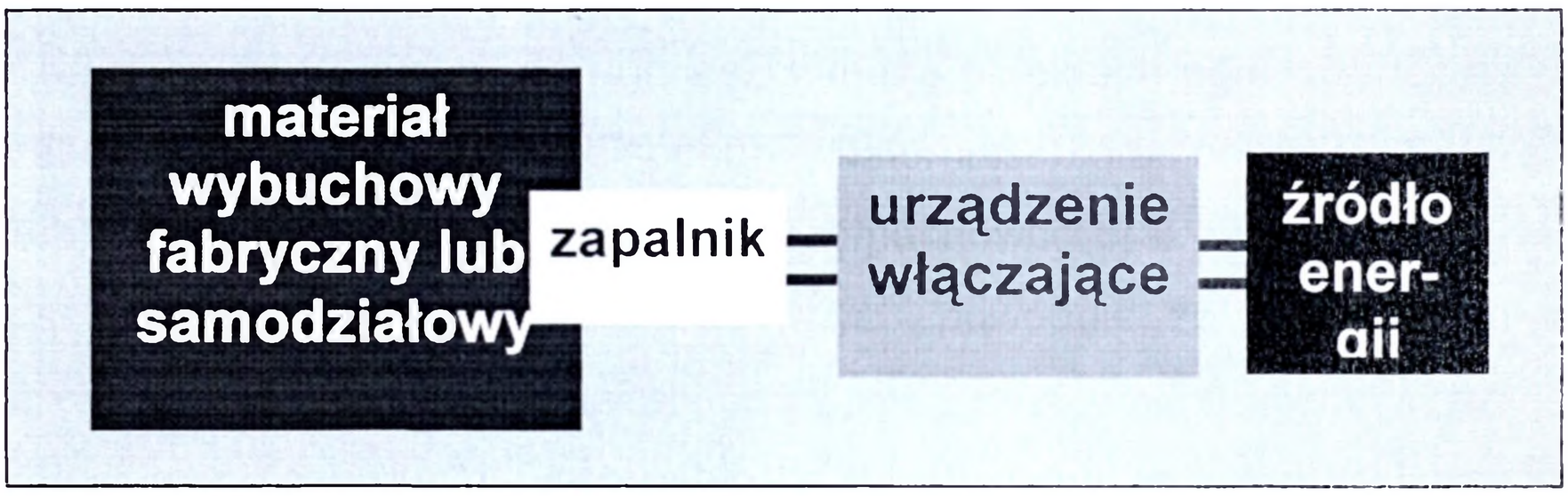
4.2.1. Przeciwdziałanie zagrożeniom z użyciem materiałów wybuchowych

Najwyższe miejsce w hierarchii zagrożeń zajmują różnego rodzaju urządzenia wybuchowe. Analiza i ocena zagrożenia ze strony takich urządzeń pozwala postawić tezę, że zagrożeniu tego rodzaju można już skutecznie zapobiegać przez zastosowanie różnorodnych środków technicznych i proceduralnych. Niemniej pozostaje on wciąż jednym z zasadniczym źródeł zagrożenia dla cywilnego portu lotniczego i w związku z tym należy dążyć do utrzymywania właściwej czujności w tym zakresie.

Podjęcie jakichkolwiek procedur organizacyjnych przeciwdziałających atakowi terrorystycznemu z użyciem urządzeń wybuchowych wymaga przypomnienia, że urządzenia tego typu mogą swym wyglądem przypominać dowolny przedmiot. Zatem

stosownie do przeznaczenia przedmiotu, jaki przypomina bomba, będzie ona dostarczana na teren portu lotniczego i umieszczana w obiektach portu czy też na pokładzie statku powietrznego na różne sposoby. Natomiast biorąc pod uwagę praktycznie nieograniczoną wyobraźnię potencjalnego zamachowca oraz fakt, że może on dysponować szeroką gamą środków wybuchowych, powoduje, że umieszczenia w porcie lotniczym klasycznie wyglądającej bomby jest bardzo mało prawdopodobne.

Pewna wskazówkę dla personelu portu lotniczego, a szczególnie tej części personelu, która odpowiada za bezpieczeństwo stanowi fakt, że podkładane urządzenia zamachowe niezależnie od wyglądu zewnętrznego składają się zawsze co najmniej z czterech elementów[127].



Rys. 13. Schemat ideowy podkładanych urządzeń wybuchowych *(Źródło: opracowanie własne na podstawie S. Nakonieczny, Przygotowanie odpowiedzi … wyd. cyt.)*

Zgodnie z przyjętymi założeniami urządzenie wybuchowe podkładane w porcie lotniczym może mieć na przykład zewnętrzną formę:

- typowego bagażu kabinowego,
- bagażu towarzyszącego,
- bagażu pozostawionego bez opieki (torby, teczki, reklamówki, torby papierowej),
- elementu wyposażenia cateringowego,
- paczki, listu pocztowego
- zaparkowanego samochodu ciężarowego, busa, osobowego.
- elementu cargo (w dowolnym opakowaniu do dużego kontenera włącznie)

---

[127] Zobacz S. Nakonieczny, *Przygotowanie odpowiedzi na zamach bombowy*, materiały konferencji „zarządzanie w sytuacjach kryzysowych, Uniwersytet Kardynała Wyszyńskiego, Warszawa 2004.

- materiałów i urządzeń związanych z budową, remontem, rozbudową portu lotniczego.

Natomiast za szczególnie zagrożone wrażliwe na atak bombowy miejsca portu lotniczego uważa się[128]:

- wieżę kontroli ruchu lotniczego;
- generatory energetyczne;
- lotnicze urządzenia naziemne;
- magazyny paliw i smarów (MPS);
- bocznice kolejowe;
- ujęcia wody;
- płyty postojowe statków powietrznych;
- hangary.
- radary;
- radiolatarnie kierunkowe i bezkierunkowe;
- urządzenia systemów lądowania ILS;
- anteny radiowe wysokiej częstotliwości;
- generatory prądu;
- stacje meteorologiczne;
- pomieszczenia producentów zaopatrzenia pokładowego;
- magazyny ładunków przeznaczonych do przewozu lotniczego.

Wobec dużej liczby i różnorodności form wykorzystania materiałów wybuchowych w ataku terrorystycznym w dalszej części opracowania pojęcie atak bombowy oznaczało będzie każdy akt terrorystyczny z wykorzystaniem jakiegokolwiek materiału wybuchowego użytego w jakiejkolwiek formie.

Należy pamiętać, że terrorysta może podłożyć bombę w porcie lotniczym z zamiarem spowodowania wybuchu i zadania strat pasażerom, personelowi portu, bądź też zniszczenia urządzeń infrastruktury portu lub statku powietrznego. Nie można jednak wykluczyć podłożenia bomby w takim stanie, aby nie wybuchła (np. z odłączonym źródłem zasilania) lub spowodowania wybuchu o oddziaływaniu jedynie akustycznym w celu zastraszenia personelu portu, wywołania zjawiska paniki i zakłócenia pracy portu lotniczego. Ponadto należy liczyć się z możliwością ataku bombowego przeprowadzonego w pobliżu portu lotniczego, szczególnie w wypadku, gdy

---

[128] Zobacz *Krajowy Program Ochrony Lotnictwa Cywilnego* wprowadzony Rozporządzeniem Rady Ministrów z dnia 15 lipca 2003 roku, § 29.1.

terroryści będą mieli ograniczone możliwości wniesienia, wwiezienia ładunku wybuchowego na teren portu lotniczego. Dogodnym miejscem mogłyby być ogólnodostępne miejsca parkingowe.

Zatem przy projektowaniu rozmieszczenia miejsc parkingowych przy miejsca bezpośrednio przylegające do budynków terminalu powinny być zarezerwowane dla personelu portu. Warto także przewidzieć monitorowanie parkingu, a sam parking zaplanować tak, aby możliwe było w razie potrzeby z jednej strony blokowanie do niego dostępu, a z drugiej szybka, sprawna ewakuacja pojazdów, w tym pojazdu-ładunku wybuchowego.

Ponadto proponuje się następujące procedury organizacyjne formułowania planów przeciwdziałania zagrożeniu atakiem bombowym oraz przeciwdziałania przy podłożeniu bomb w portach lotniczych. Przedmiotowe procedury opisano w aspekcie podejmowanych kroków zaradczych, stanu zagrożenia bombowego, wykrycie bomby i jej wybuchu.

Przygotowanie portu lotniczego na atak bombowy wymaga zrealizowania następujących czynności zaradczych[129]:

1. Wyznaczenie łańcucha dowodzenia.
2. Ustalenie centrum kierowania.
3. Ustalenie podstawowych i zastępczych sposobów komunikowania się.
4. Wyznaczenie zespołu do oceny zagrożenia bombowego.
5. Opracowanie procedur postępowania personelu portu lotniczego w przypadku zamachu bombowego.
6. Opracowanie procedur korzystania z pomocy specjalistów minerów - pirotechników.
7. Opracowanie planu ewakuacji ludzi z zagrożonej strefy portu lotniczego[130].
8. Wyznaczenie obszarów portu lotniczego do bezwzględnego przeszukania.
9. Wyznaczenie zespołów przeszukujących i określenie technik przeszukiwania.
10. Określenie systemu kierowania akcją przeszukiwania.
11. Opracowanie procedur działania na wypadek wybuchu bomby.
12. Bieżące weryfikowanie stanu zabezpieczenia fizycznego portu lotniczego.

---

[129] Opracowano na podstawie J. Litwiński, *Bezpieczeństwo wspólnego transportu lotniczego po 11 września 2001 roku* (w) *„Bezpieczne niebo"*, Warszawa 2002 oraz S. Nakonieczny, *Przygotowanie odpowiedzi* ... wyd. cyt.

[130] Nie wolno ewakuować „przez bombę"

Natomiast w wypadku wystąpienia stanu zagrożenie bombowego należy podjąć następujące czynności[131].

Jeśli odebrano przez telefon groźbę wykonania ataku bombowego należy:

1. Zapamiętać (zapisać, nagrać) rozmowę w szczegółach.
2. Zwrócić uwagę na wszelkie dźwięki w tle i na szczegóły dotyczące głosu i nawyków mówiącego.
3. Możliwie długo przeciągać rozmowę wykorzystując dowolny pretekst.
4. Jeśli ktoś inny odebrał rozmowę, należy go szczegółowo przepytać.

Jeśli groźba przekazana została przesyłką pocztową należy zabezpieczyć przesyłkę w celu zachowania danych do późniejszej analizy specjalistycznej prowadzonej przez policję lub inne służby bezpieczeństwa.

Następnie osoba, która odebrała informacje o potencjalnym zagrożeniu atakiem bombowym powinna:

1. Poinformować kierownictwo portu lotniczego lub osobę wyznaczoną do przejęcia dowodzenia w sytuacjach nadzwyczajnych i poinformować służby ochrony lotniska.
2. Powiadomić ekspertów pirotechników, policję, straż graniczną, straż pożarową i służby medyczne.
3. Zaalarmować służby techniczne (elektryków, hydraulików).
4. Zadecydować, czy przeprowadzić ewakuację portu lotniczego.
5. Przekazać w sposób niewywołujący paniki personelowi i klientom portu instrukcje postępowania.
6. Ustanowić ścisłą kontrolę wszystkich przychodzących do portu lotniczego przesyłek, teczek personelu, bagażu pasażerów.
7. Przeprowadzić planowe i metodyczne przeszukanie zagrożonego obszaru, najlepiej przez, lub w obecności osób, które ten teren najlepiej znają.
8. W czasie stanu alarmowego nie używać w porcie lotniczym wind ani schodów ruchomych.

Z kolei po znalezieniu bomby należy:

1. Nie dotykać jej, ani nie zanurzać w wodzie.
2. Nie narażać niepotrzebnie personelu - otoczyć miejsce kordonem i powiadomić pirotechników.

---

[131] Opracowano na podstawie danych ze strony internetowej serwisu poświęconego Ustawie z dnia 22 stycznia 1999 o ochronie informacji niejawnych, http://www.iniejawna.pl

3. Jeśli do tej pory tego nie wykonano, nakazać ewakuację terenu i pozostawić drzwi i okna otwarte. Obszary ewakuacyjne i punkty zbiorcze powinny być najpierw sprawdzone czy niema na ich terenie podejrzanych urządzeń.
4. Wyłączyć zasilanie elektryczne, gaz i przewody paliwowe wiodące do obszarów zagrożonych.
5. Usunąć z otoczenia wszystkie materiały palne.
6. Postawić w stan gotowości personel medyczny.
7. Przygotować sprzęt przeciwpożarowy. Poinformować policję, straż graniczną i straż pożarną. Pozostać na miejscu (pozostawić kompetentne osoby na miejscu), aby udzielać informacji pirotechnikom i służbom przeciwpożarowym z chwilą, gdy przybędą.
8. Umieścić worki z piaskiem, maty zabezpieczające i inne podobne materiały głuszące - według instrukcji ekspertów pirotechników.
9. Ponieważ bomby mogą być eksplodowane drogą radiową, wszystkie nadajniki, w tym również aparaty radiowe nadawczo-odbiorcze w promieniu 250m muszą w miarę możliwości zostać wyłączone, za wyjątkiem tych, które będą potrzebne pirotechnikom.

Wreszcie po wybuchu bomby należy:

1. Wezwać policję, jednostkę pirotechniczną, straż pożarną i brygadę ratowniczą (według potrzeb) i pomagać im w ich działaniach.
2. Ewakuować personel z zagrożonego obszaru portu lotniczego, po uprzednim sprawdzeniu czy drogi ewakuacji i punkty zborne (do których następuje ewakuacja) są wolne od podejrzanych urządzeń.
3. Zabezpieczyć dowody rzeczowe z miejsca eksplozji. do chwili przybycia personelu śledczego i pirotechników.

Poza dotychczas zaproponowanymi, należy stosować specjalne, odrębne procedury w wypadku zagrożenia bombami – przesyłkami pocztowymi. Bomby pocztowe mogą być dwóch rodzajów i różnią się zasadniczo wymiarami: bomby listowe (a w tym bomby-książki) i bomby w postaci normalnych paczek pocztowych. Chociaż szersze użycie bomb pocztowych było początkowo ograniczone do niewielu politycznych grup terrorystycznych, to nie można wykluczyć, że ta taktyka zostanie skopiowana przez inne grupy terrorystyczne i stosowana także jako narzędzie zastraszenia w portach lotniczych oferujące wysoką szansę sukcesu, przy niewielkim ryzyku.

W wypadku tego typu zagrożenia bombowego należy:

1. Uruchomić specjalne procedury sprawdzania i kontroli dla wszystkich przesyłek pocztowych.
2. Jeśli przez jakiś czas po przybyciu poczta pozostaje nieposortowana, należy wyznaczyć na te przesyłki przejściowy magazyn z dala od miejsc pracy personelu portu lotniczego i przebywania klientów portu.
3. Przygotować obszar do składowania przesyłek podejrzanych wykazanych przez kontrolę i ustanowić wokół niego pewien minimalny obszar bezpieczeństwa.
4. Opracować procedury identyfikacji/weryfikacji dla (podejrzanych) przesyłek pocztowych zidentyfikowanych przez kontrolę.
5. Przeprowadzić treningi personelu, aby zapewnić dokładne zrozumienie wszystkich faz planu postępowania z bombami pocztowymi.
6. Procedury "prześwietlania" (lub kontroli). Przesyłki powinny być traktowane jako podejrzane jeśli:

- stempel pocztowy lub nazwisko nadawcy wskazuje, że przesyłka pochodzi z niezwykłego miejsca lub od niezwykłego nadawcy.
- odręczny napis na przesyłce jest w nieznanym stylu.
- paczka w jakiś sposób jest niejednolita lub "przeważa" na jedną stronę.
- przesyłka jest podejrzanie ciężka w stosunku do wymiarów. (Skuteczne bomby listowe zwykle ważą powyżej 50g).
- list jest grubszy niż 5mm.
- przesyłka "sprężynuje" od góry, od dołu lub z boku.
- na kopercie lub paczce jest drobne nakłucie lub perforacja.
- na kopercie lub paczce są tłuste plamy.
- przesyłka wydziela niezwykły zapach, szczególnie zapach migdałów lub marcepana.
- przesyłka wydaje dźwięk taki jak luźne części metalu.
- wewnątrz koperty daje się wyczuć takie jak karton lub kawałek metalu.

4.2.2. Przeciwdziałanie zagrożeniom z użyciem przenośnych przeciwlotniczych zestawów rakietowych

Całkowicie odmienne od urządzeń wybuchowych, chociaż nie wiele mniejsze zagrożenie dla portów lotniczych, a szczególnie startujących i lądujących w tych portach statków powietrznych stanowią przenośne przeciwlotnicze zestawy rakietowe (PPZR) różnych typów. Przeprowadzone analizy i oceny tego typu zagrożeń pozwoliły na postawienie tezy, że podejmowane przedsięwzięcia organizacyjne przeciwdziałania tego typu zagrożeniom powinny obejmować przede wszystkim:

- wspomaganie prognozowania zagrożeń terrorystycznych w wymiarze powietrznym, a w tym zagrożeń poszczególnych rejsów statków powietrznych i stosownie do jego rezultatów określanie najbezpieczniejszych sposobów realizacji operacji startu i lądowania;
- monitorowanie i nadzór rejonów zagrożonych, w tym skuteczne ograniczenie dostępu do stref i miejsc szczególnie newralgicznych;
- wypracowanie skutecznych procedur alarmowych i wykształcenie nawyków ich powszechnego stosowania;
- upowszechnienie świadomości zagrożeń wśród całego personelu wszystkich instytucji współużytkujących port lotniczy;
- ochronę statków przez lotnictwo wojskowe, posiadające pokładowe systemy obrony przez PPZR.

Prognozowanie zagrożeń poszczególnych rejsów statków powietrznych jest prostym i skutecznym sposobem prewencyjnym eliminowania możliwych zagrożeń ze strony PPZR. Procedury prognozowania zagrożeń są efektywne zwłaszcza, w sytuacjach, w których operatorzy ruchu lotniczego portu wspomagani są komputerowymi systemami prognozowania takich zagrożeń w stosunku do konkretnych rejsów statków powietrznych, w konkretnych warunkach, w konkretnym porcie lotniczym. Istota tego rozwiązania polega na zebraniu danych o topografii portu i jego okolic, a także danych charakteryzujących typowe rodzaje zagrożeń. Ponadto należy gromadzić dane o bieżących i przewidywanych warunkach meteorologicznych. Zebrane dane dają podstawę decyzyjną dla kierującego, pozwalającą mu wytyczyć konkretny profil i trasę startu lub lądowania, omijającą rejony niebezpieczne. Wspomniane dane gromadzone są najczęściej w ramach aplikacji komputerowych takich, jak np. Air SimGuard izraelskiej firmy RONTAL.

Przy monitorowaniu i nadzorze rejonów należy wyróżnić dwa różniące się zasadniczo rodzaje tych rejonów.

Pierwszy – dotyczy rejonów najbardziej prawdopodobnego użycia środków niszczących statki powietrzne. Są to rejony dogodne do odpaleń PPZR, przeciwpancernych pocisków kierowanych i granatników, oddziaływania bronią strzelecką, a także zamontowania min przeciwśmigłowcowych. Najczęściej rejony te usytuowane są poza chronionym terenem portu lotniczego (za wyjątkiem rejonów montowania wymienionych rodzajów min). Sytuację monitorowania i nadzoru tych rejonów komplikuje to, że większość współczesnych cywilnych portów lotniczych usytuowana jest na terenie lub w pobliżu dużych aglomeracji miejskich i przemysłowych. Tereny dogodnych odpaleń środków, które mogą być użyte przeciwko statkom powietrznych są zatem najczęściej powszechnie dostępne, często usytuowane w osiedlach mieszkaniowych lub przemysłowych, będąc w różnym, często prywatnym posiadaniu. Ograniczenie do nich publicznego dostępu jest w większości przypadków praktycznie niemożliwe.

Drugim rodzajem rejonów są obszary będące w dyspozycji portu lotniczego. Praktycznie prawie wszędzie są to rejony o reglamentowanym dostępie. Najbardziej rozpowszechnionym sposobem ograniczenia dostępu jest ogrodzenie tego rejonu, wraz z różnymi wspomagającymi systemami technicznymi. Jednak jak wskazują doświadczenia dużych portów lotniczych o dużej intensywności zagrożeń, sama reglamentacja dostępu nie jest wystarczająca, ponieważ można ją stosunkowo łatwo pokonać fałszując dokumenty akredytacyjne czy tożsamości. Ponadto w porcie posiadającym tylko jeden system reglamentacji dostępu do całego obszaru, jego pokonanie praktycznie powoduje dostęp do wszystkich newralgicznych rejonów i urządzeń portu. Zdecydowanie skuteczniejszym zabezpieczeniem jest wielostopniowy system dostępu do kilku wydzielonych rejonów portu, oparty na wydzieleniu kilka stref bezpieczeństwa, ze ściśle przestrzeganym ograniczeniem wejścia wszystkich osób wyłącznie do upoważnionych stref. Rozwiązanie takie opracowała firma Eagle Integrated Solutions, pod kryptonimem Security Ops Pro. W systemie takiego nadzoru, monitorowanym przez kamery przemysłowe, sprzężonym z automatyczne filtrującymi bramkami (śluzami), przemieszczenie każdej osoby i pojazdu przebywających wewnątrz takiej strefy jest śledzone i rejestrowane. Każdy pracownik (pojazd) posiada dostęp tylko do strefy wynikającej z jego kompetencji zawodowych, uzasadniony spełnianymi przez niego funkcjami. W prezentowanym systemie nie ma możliwości

dowolnego przemieszczania się pracowników po całym terenie portu. System automatycznie alarmuje o nieuprawnionym przekroczeniu strefy lub nawet takiej próbie, uruchamiając grupy interwencyjne ochrony.

Warunkiem skuteczności takiego systemu, są zaostrzone procedury wydawania odpowiedniej akredytacji tylko przez jeden organ odpowiedzialny za bezpieczeństwo całego portu. Wydanie akredytacji jest poprzedzone odpowiednim sprawdzeniem osoby ubiegającej się o zatrudnienie w dowolnej instytucji funkcjonującej w porcie. Sprawdzenie to niestety jest bardzo żmudne, kosztowne i wymagające specjalnych uregulowań prawnych, upoważniających do takiego działania służby odpowiedzialne za bezpieczeństwo portu.

Wypracowanie skutecznych procedur alarmowych i wykształcenie nawyków ich powszechnego stosowania jest nie mniej ważne od samego stwierdzenia zaistnienia takiego zagrożenia. Obowiązkowe powinno być dla każdego portu lotniczego określenie szczegółowych procedur dla wszystkich służb, pionów, ale również dla wszystkich osób pracujących i przebywających w nim, ujętych w plany i wynikające z nich instrukcje reagowania kryzysowego. W planie reagowania kryzysowego należy określić charakterystyczne rodzaje stanów kryzysowych, np.: pożaru, podłożenia ładunku wybuchowego, napadu, katastrofy statku powietrznego, nieuprawnionego wtargnięcia w wyznaczoną strefę, nieuprawnionego zawładnięcia statkiem powietrznym, nieuprawnionego pojawienia się niezidentyfikowanego statku powietrznego w rejonie kontrolowanym portu, wystąpienia zagrożenia użycia PPZR lub innych środków, itd. Należy bezwzględnie określić osoby lub organy upoważnione do ogłaszania takich stanów oraz ukonkretnić sytuacje, w których takie stany mogą być ogłoszone. Plany reagowania kryzysowego muszą precyzyjnie wskazywać na odpowiedzialne służy podejmujące określone działania oraz określać ich kompetencje. Ponadto należy precyzyjnie określić sposoby zachowania wszystkich osób nie biorących czynnego udziału w akcji antykryzysowej (całego personelu, wszystkich instytucji funkcjonujących w porcie i osób postronnych).

Takie procedury, ujęte w odpowiednich planach i instrukcjach należy upowszechnić wśród całego personelu. Warunkiem zatrudnienia każdego pracownika we wszystkich instytucjach funkcjonujących w porcie lotniczym powinna być pełna ich znajomość i umiejętność stosowania, systematycznie doskonalona i kontrolowana.

Reasumując zespół autorski zaleca następujące organizacyjne rozwiązania zabezpieczające porty lotnicze przed atakiem terrorystycznym z użyciem PPZR:

1. Istnieje wiele rodzajów oraz możliwych środków oddziaływania terrorystycznego na statki powietrzne podczas ich startów i lądowań w porcie lotniczym. Oceniamy, że spośród możliwych zagrożeń najgroźniejsze tworzone są przez przenośne przeciwlotnicze wyrzutnie rakietowe.
2. Mogące być obecnie w dyspozycji grup terrorystycznych PPZR tworzą zagrożenia dla cywilnych statków powietrznych podczas operacji starów i lądowań w promieniu ok. 4 km od trasy lotu, na wysokościach od 0,5 do 3 km. Wyprodukowanie i sprzedanie dotąd ogromnej ilości PPZR uniemożliwia skuteczną i wiarygodną kontrolę ich użycia. Spośród wszystkich wyprodukowanych na całym świecie PPZR, grupy terrorystyczne najlepszy dostęp mają do zestawów starszej generacji, których głowice samonaprowadzające pracują w paśmie podczerwieni, i których można używać w warunkach dobrej widoczności optycznej. Możliwości tych zestawów ogranicza wiele czynników, w tym przede wszystkim ich dostępność. Zestawy starszych generacji posiadają mniejsze możliwości, zamykające się w stosunku do samolotów startujących z odległością rażenia od 5-7 do 25 km od lotniska, a lądujących w odległości od 55 km do 10 km od lotniska. Najbardziej narażone na oddziaływanie PPZR są samoloty w okolicach punktów wspólnych dla tras wszystkich rejsów wysokiego ryzyka. Najczęściej jest to miejsce wspólne dla wszystkich rejsów, położone na siódmym kilometrze po starcie. Jest to miejsce, gdzie w praktyce poszczególne rejsy wchodzą w optymalną dla PPZR strefę rażenia, na wysokości około 500 m. Koncentrację zagrożeń właśnie w tym rejonie potęgują również: pełne zatankowanie samolotów przy starcie, występujące tam obszary ścisłej zabudowy oraz wykonywanie tam przez samoloty lotu z maksymalnie dopuszczalnym proceduralnie zakresem pracy silników. Wynika stąd, że należy wytypować rejony szczególnego monitorowania, które należy określić indywidualnie dla każdego lotniska. Monitorowaniem należy objąć również dachy budynków znajdujących się w tych rejonach.
3. Należy nawiązać współpracę instytucjonalną i środowiskową w zakresie powiadamiania o symptomach świadczących o mogących wystąpić zagrożeniach przede wszystkim z: Policją, Strażą Pożarną, Strażą Miejską, wojskiem, aeroklubem, Związkiem Harcerstwa Polskiego, władzami miejskimi i dzielnicowymi, itp., w zakresie monitorowania wymienionych rejonów szczególnie niebezpiecznych oraz meldowania o wszelkich podejrzanych symptomach z tym związanych. Wskazane jest przeprowadzenie w tym celu szkolenia z osobami władz miejskich

i dzielnicowych, odpowiedzialnych za bezpieczeństwo oraz poinformowanie odpowiednich samorządów o zagrożeniach ze strony przede wszystkim przenośnych przeciwlotniczych zestawów rakietowych, sposobem ich przenoszenia, rozmiarach i wyglądzie oraz sposobem użycia przez terrorystów. Niezbędne jest również nawiązanie współpracy z wyspecjalizowanymi agencjami oraz organizacjami, takimi jak Agencja Bezpieczeństwa Wewnętrznego, Straż Graniczna, Wojskowe Służby Wywiadu i Kontrwywiadu, Policja Państwowa w celu uzyskiwania informacji o możliwości przenikania terrorystów na terytorium naszego kraju oraz o potencjalnych zagrożeniach. Dzięki temu możliwe byłoby prognozowanie zagrożeń i wariantów własnych działań.

4. Wymienionym zagrożeniom terrorystycznym można przeciwstawić się budując kompleksowy system bezpieczeństwa, obejmujący przedsięwzięcia organizacyjne, techniczne i prawne. Opracowanie koncepcji takiego systemu należy zlecić wyspecjalizowanym instytucjom, a wdrożenie pionowi bezpieczeństwa portu. System bezpieczeństwa ma obejmować wszystkie instytucje i ich pracowników funkcjonujących na terenie portu.
5. W pierwszej kolejności należy skutecznie ograniczyć dostęp do wytyczonych w tym celu, stref bezpieczeństwa portu. Stref tych powinno być kilka, a dostęp do nich chroniony odpowiednimi urządzeniami technicznymi, monitorującymi i uniemożliwiającymi nieuprawniony dostęp. Zbudowanie skutecznego systemu ochrony uwarunkowane jest, obok reglamentacji dostępu, również procedurą wydawania zezwoleń (certyfikatów bezpieczeństwa) tylko dla osób niebudzących żadnych zastrzeżeń. Procedurą sprawdzającą muszą być objęci zarówno stali pracownicy wszystkich instytucji funkcjonujących w porcie, jak również pracownicy sezonowi, pracownicy podwykonawców (np. pracownicy firm budowlanych, sprzątających, cateringowych, biur podróży, parkingowych, wynajmu samochodów, itp.).
6. Warunkiem zatrudnienia pracownika w porcie, w dowolnej instytucji, musi być uzyskanie certyfikatu bezpieczeństwa, który upoważnia do pracy, określa upoważnienie dostępu do konkretnej strefy bezpieczeństwa, jest również świadectwem wiedzy i umiejętności bezpieczeństwa. Certyfikacja pracowników stałych powinna być cykliczna, a zalecanym okresem ważności certyfikatu – co najwyżej 3 lata.

7. Należy określić kilka typowych sytuacji zagrożeń terrorystycznych i dla nich opracować procedury przeciwdziałania im. Takimi sytuacjami mogą być:
   - próba wtargnięcia w zakazaną strefę;
   - bezprawne wtargnięcie w zakazaną strefę bezpieczeństwa (różnicując ich znaczenie oraz uruchamiane środki);
   - pojawienie się groźby zestrzelenia statku powietrznego zbliżającego się do lotniska – przerwanie procedury lądowania i skierowanie danego samolotu na inne lotnisko;
   - pojawienie się groźby zestrzelenia statku startującego (różnicując uruchamiane procedury i środki w zależności od fazy startu) – przerwanie startu w pierwszej fazie lub dynamiczny nabór wysokości powyżej 3000 m.
6. Przygotować systemy kursów i szkoleń, wszystkich służb i osób bezpośrednio angażowanych do każdego z rodzaju akcji, ale także całego personelu portu lotniczego i wszystkich instytucji tam funkcjonujących. Obok szkoleń teoretycznych, podtrzymywać nawyki poprzez uruchamianie akcji bezpieczeństwa dla celów szkoleniowych (alarmy szkoleniowe).
7. Wejść w porozumienie z przewoźnikami w zakresie wprowadzenia rozwiązań uodporniających statki powietrzne korzystające z portu lotniczego na skutki oddziaływania PPZR.

4.2.3. Przeciwdziałanie zagrożeniom z użyciem granatników i broni strzeleckiej przeciwpancernych pocisków kierowanych i min przeciwlotniczych

Analiza porównawcza parametrów granatników i broni strzeleckiej z ruchem lotniczym w przeciętnym polskim porcie lotniczym pozwala wnioskować, że groźne w skutkach dla takiego portu może być użycie wielkokalibrowych (12,5; 12,7 mm) karabinów snajperskich.

Wprawdzie na każdym lotnisku można wyznaczyć prawdopodobną strefę niebezpieczną dla portu lotniczego od ognia granatników, ale ich użycie przeciwko statkom powietrznym lub ludziom przemieszczającym się na płycie lotniska wydaje się w warunkach polskich bardzo mało prawdopodobne. Taka ocena zagrożenia ze strony granatników lotnisk w Polsce wynika przede wszystkim z faktu, że groźny w skutkach atak pociskiem granatnikowym (niezależnie od typu granatnika) musiałby być w prak-

tyce atakiem samobójczym. We wspomnianą hipotetyczną strefę niebezpieczną granatnik, ze względu na jego niewielkie rozmiary i wagę, może być wniesiony w różnego rodzaju torbach np. sportowych lub w bagażu tzw. podręcznym.

Natomiast nie sposób wykluczyć, przy wszystkich zidentyfikowanych niedogodnościach takiego działania, użycia w celach terrorystycznych przeciwpancernych pocisków kierowanych (PPK) super lekkiego lub krótkiego zasięgu. W strefie zasięgu rażenia PPK występuje zwykle wokół portu lotniczego wiele dogodnych sektorów strzelania dla przenośnych PPK, które wyznaczyć należy w czasie rekonesansu w dzień (okiem uzbrojonym) i w nocy z wykorzystaniem urządzeń noktowizyjnych. Rekonesans powinien pozwolić uzyskać rzeczywistą mapę sektorów, z których mogłoby nastąpić odpalenie pocisku rakietowego. Mapa taka stanowiłaby podstawę kolejnego rekonesansu, którego celem powinno być określenie lokalizacji miejsc, z których najdogodniej jest odpalić pocisk rakietowy PPK z zestawu przenośnego super lekkiego (kilkaset metrów) lub krótkiego zasięgu (zależnie od typu pocisku nawet do 4000 m). Przeprowadzenie wspomnianych działań powinno pozwolić organom kierowniczym portu lotniczego podjęcie przedsięwzięć organizacyjnych, które ograniczyłyby znacznie zagrożenia atakiem terrorystycznym z użyciem PPK.

Przeciwdziałanie zagrożeniu minami przeciwlotniczymi w polskich portach lotniczych obecnie wymaga zabiegów organizacyjnych, polegających na zidentyfikowaniu na płycie lotniska (w jego obrębie) miejsc trawiastych, z których potencjalnie ustawiona mina mogłaby razić statek powietrzny i ich okresowe patrolowanie przez przeszkolony personel ochrony. Możliwe warianty użycia pojedynczych min przeciwlotniczych służyć mogą za punkt odniesienia do rekonesansu, który należy przeprowadzić bezpośrednio na płycie lotniska z zaangażowaniem wyspecjalizowanych grup personelu wojsk inżynieryjnych. Mimo małego prawdopodobieństwa tego rodzaju zagrożenia, nie można wykluczyć ustawienia miny przeciwlotniczej na przedłużeniu dróg startowych, lądowania (lub w ich pobliżu). Niezbędna jest codzienna (najlepiej o świcie) kontrola dróg startowych i terenu położonego wzdłuż tych dróg w odległości do 250 m od ich osi, szczególnie na przedłużeniu dróg startowych oraz w okolicach ich przecięcia, ukierunkowana na wykrycie min przeciwlotniczych.

Znaczne i trudne do zidentyfikowania zagrożenie, niewymagające poświęcenia życia terrorysty stanowią wielkokalibrowe karabiny snajperskie. Przeciwdziałanie tego typu zagrożeniu wymagałoby jednak podobnych zabiegów organizacyjnych, jak w przypadku PPK czy też min przeciwlotniczych. Do zidentyfikowania możliwych sek-

torów i lokalizacji miejsc strzelania w dzień i w nocy należy przeprowadzić rekonesanse dzienny i nocny z udziałem specjalistów snajperów, używających tego właśnie typu broni. Identyfikacja taka pozwoliłaby na wprowadzenie przedsięwzięć zabezpieczających płytę lotniska i terminale przed terrorystycznym działaniem snajpera. Niezwykle niebezpieczne byłyby przede wszystkim działania nękające snajpera terrorysty w stosunku do personelu i (lub) pasażerów w porcie lotniczym. Działanie tego typu mogłoby sparaliżować w praktyce działanie portu, skutkować - poza ofiarami w ludziach - oczywistymi stratami finansowymi. Biorąc pod uwagę wyposażenie i wyszkolenie światowych grup terrorystycznych, wskazany sposób działania terrorystów mógłby być dla nich praktycznie bezinwestycyjny i najbezpieczniejszy ze wszystkich dotąd wyróżnionych.

Wymienione przesłanki pozwalają sformułować wniosek, że o ile wskazane organizacyjne działania zabezpieczające przed atakiem snajperskim nie są do tej pory zrealizowane, należy je w obecnej sytuacji Polski wykonać tak szybko jak to możliwe.

4.2.4. Przeciwdziałanie zagrożeniom z użyciem uprowadzonych statków powietrznych

Konieczność przeciwdziałania w portach lotniczych aktom terroru z użyciem uprowadzonych statków powietrznych po 11 września nie wymaga oddzielnego uzasadnienia. Niezależnie od skali, miejsca i czasu wystąpienia zagrożenia terrorystycznego lotniska, można przewidywać następujące warianty działania terrorystów wykorzystujących samolot jako środek ataku:

- uderzenia pojedynczym samolotem;
- uderzenie grup samolotów i niszczenie wybranych obiektów lotniskowych (w rejonie lotniska z dużym portem lotniczym ląduje wiele samolotów z różnych miejsc o zbliżonym czasie lądowania – kilka do kilkunastu minut pomiędzy lądowaniami);
- jednoczesne uderzenie z kilku kierunków na różne lotniska;
- uderzenie lotnictwa wraz ze środkami bezpilotowymi, samosterującymi;
- możliwość zastosowania innych aparatów latających (poza samolotami) (balony, śmigłowce, motolotnie).
- Powyższe warianty zagrożeń terrorystycznych mogą być zrealizowane poprzez:

9. Uprowadzenie środka komunikacji lotniczej poza granice RP.

W celu przeciwdziałania aktom bezprawnego zawładnięcia prywatnego sprzętu lotniczego w celach terrorystycznych należy wykonać następujące przedsięwzięcia organizacyjne.

1. Wdrożyć program kontroli miejsc bazowania prywatnych statków powietrznych, w promieniu co najmniej 100 km od danego lotniska. Przedmiotem tych kontroli powinien by przede wszystkim stan zabezpieczenia danych statków powietrznych w ich miejscu przechowywania oraz zmiany ich bazowania.
2. Wszystkie statki powietrzne w tym obszarze należy objąć szczególnym dozorem przed bezprawnym użytkowaniem, przez:
   - usuwanie z samolotów na postoju ich źródeł zasilania;
   - montowanie dodatkowych (ukrytych) wyłączników zapłonu;
   - ograniczanie zapasów paliwa w zbiornikach;
   - stosowanie zabezpieczeń mechanicznych i elektronicznych;
   - patrolowanie lotnisk i lądowisk (demonstrowanie obecności).
3. Brać pod uwagę możliwość uprowadzenia samolotu, szczególnie tuż po starcie, gdy jest on jeszcze niemal całkowicie zatankowany paliwem i użycie go do uderzenia na lotnisko (kluczowe obiekty lotniskowe).
4. Zwiększyć kontrolę oraz koordynację ruchu statków powietrznych operujących w promieniu do 100 km od danego lotniska na wysokości lotu do 3000 m; w promieniu do 50 km na wysokościach do 2000 m; i w promieniu do 10 km na wysokościach lotu do 500 m.
5. W związku z realnym zagrożeniem bezprawnego zawładnięcia lekkiego statku powietrznego bazującego w pobliży portu lotniczego i oddziaływania nim na samoloty cywilnej komunikacji lotniczej należy ograniczyć liczbę lotów i zwiększyć kontrolę oraz koordynację ruchu tych statków w promieniu co najmniej 100 km od danego portu lotniczego, na wysokości lotu do 3000 m; w promieniu do 50 km na wysokościach do 2000 m; i w promieniu do 10 km na wysokościach lotu do 500 m. w razie braku możliwości zmiany parametrów lotu takiego statku powietrznego (brak reakcji załogi na podawane komendy) i realnej groźby przecięcia się toru lotu samolotu pasażerskiego przerwać procedurę lądowania lub startu w pierwszej fazie, a po wystartowaniu podać komendy na zmianę trasy lotu i wysokości tak, aby uniknąć ewentualnego ataku.

6. Wystąpić z wnioskiem do właściwych instytucji (Urzędu Lotnictwa Cywilnego, Policji, Aeroklubu, itp.) o wzmożenie zabezpieczenia sprzętu lotniczego przed bezprawnym ich użytkowaniem, szczególnie na małych lotniskach i lądowiskach.

4.2.5. Przeciwdziałanie zagrożeniom z użyciem cyberterroryzmu

W dobie nowoczesnych technologii informatycznych pojawia się także nowe zagrożenie tzw. cyberterroryzmem. Terminem tym określa się działalność terrorystyczną ukierunkowaną na zniszczenie lub zakłócenie pracy infrastruktury informatycznej. W przypadku lotnisk przedmiotem ataku informacyjnego – celem zniszczenia lub jego zmodyfikowania (zakłócenia) – mógłby być komputerowy system wspomagania kontroli lotów lub przepływające w nim informacje. Znamiennym w tym względzie jest fakt, że ataku takiego można dokonać z dowolnego miejsca i w dowolnym miejscu na świecie, wszędzie tam, gdzie działanie jakiegoś systemu uzależnione jest od technologii informatycznej.

Zasadniczymi formami ataku informacyjnego może być: atak informatyczny i atak elektroniczny. Przy czym ten pierwszy prowadzony jest w sferze przetwarzania danych cyfrowych i polega zasadniczo na skrytym wprowadzeniu przez atakującego złośliwego kodu komputerowego celem osiągnięcia zamierzonego efektu. Kody te mogą przybierać formę: wirusów, robaków, bomb logicznych, bomb programowanych czasowo, koni trojańskich lub ich kombinacji odpowiednich do pożądanych efektów. Druga forma – atak elektroniczny – polega na użyciu energii elektromagnetycznej celem zaatakowania wybranych elementów infrastruktury lub sprzętu z zamiarem obniżenia lub pozbawienia jego zdolności użytkowych. W zależności od zastosowanego zakresu widma promieniowania elektromagnetycznego może to być atak laserowy lub atak elektromagnetyczny. Ze względu zaś na stopień porażenia zaatakowanego obiektu można tu wyróżnić zakłócanie i tzw. atak w pełnym wymiarze. Zakłócanie powoduje z reguły czasowe obniżenie zdolności funkcjonowania zaatakowanych urządzeń, zaś atak w pełnym wymiarze powoduje w zasadzie fizyczną destrukcję elementów tych systemów, co w konsekwencji prowadzi do trwałego wyłączenia ich z pracy (utraty funkcji wynikających z ich przeznaczenia).

Przeciwdziałanie zagrożeniom atakiem cyberterrorystycznym w porcie lotniczym wymaga ciągłej realizacji następujących czynności organizacyjnych[132]:

W zakresie polityki korzystania z Internetu w porcie lotniczym:

1. Internet może być wykorzystywany do publikowania i przesyłania niesklasyfikowanych informacji uznanych za możliwe i celowe do udostępnienia poza portem lotniczym lub których ewentualne przechwycenie nie spowoduje szkody dla portu lotniczego lub jego klienta.
2. Informacje klasyfikowane powinny być przesyłane z i do portu lotniczego (w tym szczególnie do systemów kontroli lotu) tylko po ich zaszyfrowaniu z wykorzystaniem odpowiedniego oprogramowania i urządzeń.
3. Przesyłanie z i do portu lotniczego (w tym szczególnie do systemów kontroli lotu) przez Internet zaszyfrowanych informacji klasyfikowanych powinno odbywać się tylko w sytuacjach, kiedy nie sa dostępne dedykowane w tym celu systemy teleinformatyczne i kiedy ryzyko utraty dostępności tych informacji jest akceptowalne.
4. Połączenie sieci i systemów teleinformatycznych portu lotniczego (w tym szczególnie systemów kontroli lotu) z Internetem i innymi sieciami publicznymi powinno być możliwe tylko dla systemów ściśle określonych przez wzgląd ich znaczenia dla funkcjonowania portu lotniczego i powinno być przedmiotem formalnego dopuszczenia takiego połączenia przez organ portu lotniczego odpowiedzialny za jego bezpieczeństwo teleinformatyczne.

Natomiast w zakresie wdrażania w portach lotniczych przedsięwzięć proaktywnych ograniczających poziom ryzyka dla krytycznej infrastruktury teleinformatycznej portu lotniczego należy:

1. Prowadzić ciągła ocenę podatności systemów i sieci teleinformatycznych na atak cyberterrorystyczny.
2. Systematycznie prowadzić testy penetracyjne.
3. Prowadzić warsztaty i szkolenia poświęcone przeciwdziałaniu cyberterroryzmowi z personelem portu lotniczego.
4. Opracowywać materiały szkoleniowe.

---

[132] Opracowano na podstawie, R. Kośla, *Cyberterroryzm – definicja zjawiska, zagrożenia dla Polski*, wystąpienie zastępcy dyrektora departamentu bezpieczeństwa teleinformatycznego ABW.

5. Ciągle monitorować i analizować sytuacje zagrożeń cyberterroryzmem i opracowywać lub udoskonalać narzędzia dla administratora systemów i sieci teleinformatycznej portu w celu lepszego zapobiegania i wykrywania incydentów.
6. Prowadzić prace badawcze związane z incydentami cyberterroryzmu.

4.2.5. Przeciwdziałanie zagrożeniom materiałami radioaktywnymi, rozszczepialnymi i chemicznymi

Materiały radioaktywne i rozczepiane tworzą kolejny rodzaj zagrożeń, którym należy się przeciwstawić w porcie lotniczym. Zagrożenia te związane są przede wszystkim z:

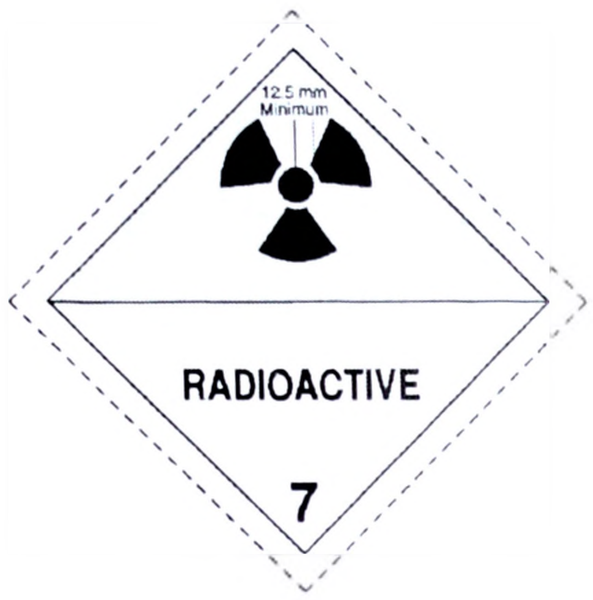
- transportem materiałów i źródeł promieniotwórczych do/z oraz na terenie lotniska;
- niewłaściwą obsługą przesyłek;
- przemytem materiałów radioaktywnych.

Transport źródeł promieniotwórczych i materiałów jądrowych w ruchu międzynarodowym i krajowym regulowany jest przepisami zawartymi w *Zasadach bezpiecznego przewozu materiałów radioaktywnych* wydanych przez Międzynarodową Agencję Energii Atomowej (MAEA) w Wiedniu. W dokumencie tym ustalono normy bezpieczeństwa, zapewniające akceptowalny poziom zagrożenia ludzi od promieniowania oraz zagrożenia mienia i środowiska naturalnego przy przewozie materiałów promieniotwórczych. Zgodnie z ustaleniami wspomnianego dokumentu podczas przewozu materiałów promieniotwórczych do portu lotniczego oraz na jego terenie należy chronić ludzi, mienie i środowisko naturalne przed skutkami promieniowania. Wypełnienie tego zalecenia wymaga przestrzegania w czasie transportu materiałów promieniotwórczych do lotniska i na jego terenie określonych warunków bezpieczeństwa. Jednym z nich jest używanie do przewożenia materiałów radioaktywnych specjalnie przygotowanymi i oznakowanych pojazdów.



Źródło: *fotografia pozyskana z prezentacji T. Dziubiak, Transport materiałów radioaktywnych, Warszawa 2005*

Fotografia 1. Pojazd przewożący materiały radioaktywne do porty lotniczego



Źródło: rysunek pozyskany z prezentacji z T. Dziubiak, Transport ..., wyd. cyt.

Rys. 14. Obowiązkowe oznakowanie umieszczane na pojazdach przewożących materiały radioaktywne do portu lotniczego

W lotniczych przepisach transportowych przewożone materiały jądrowe, źródła promieniotwórcze oraz urządzenia zawierające takie źródła podzielono przez wzgląd na poziom zagrożenia promieniowaniem, jaki stwarzają one podczas transportu na dwie grupy:

- przesyłki wyłączone,
- przesyłki i inne niż wyłączone.

Przesyłki wyłączone nie stwarzają zagrożenia promieniowaniem podczas przewozu, jak i ewentualnej awarii i zawierają materiały o ograniczonej aktywności substancji promieniotwórczych.. Natomiast przesyłki i inne niż wyłączone zawierają materiały stanowiące pewne zagrożenie i dlatego podlegają szczególnym wymaganiom bezpieczeństwa obchodzenia się z nimi.

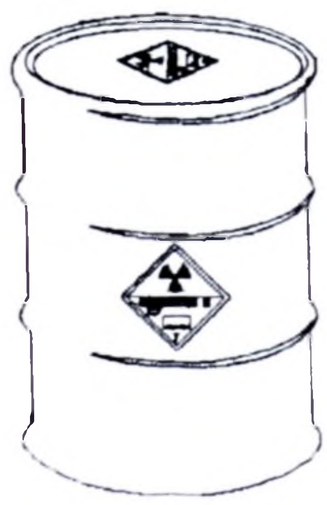
Transportem lotniczym przewozi się także izotopy promieniotwórcze. Wytwarzają one pole promieniowania o określonym natężeniu i wymagają specjalnego zabezpieczenia w czasie transportu.

Wszelkie materiały promieniotwórcze i jądrowe podzielono na sześć kategorii według kryterium zwiększającego się potencjalnego zagrożenia radiologicznego::

- materiały objęte przepisami transportowymi,
- rudy i koncentraty uranu oraz świeże paliwo reaktorów,
- niskoatktywne odpady promieniotwórcze,
- preparaty promieniotwórcze i generatory nuklidów promieniotwórczych,
- wysokoaktywne źródła promieniotwórcze,
- wypalone paliwo jądrowe oraz wysokoaktywne odpady.

W transporcie lotniczym może dojść także do transportu paliwa jądrowego.

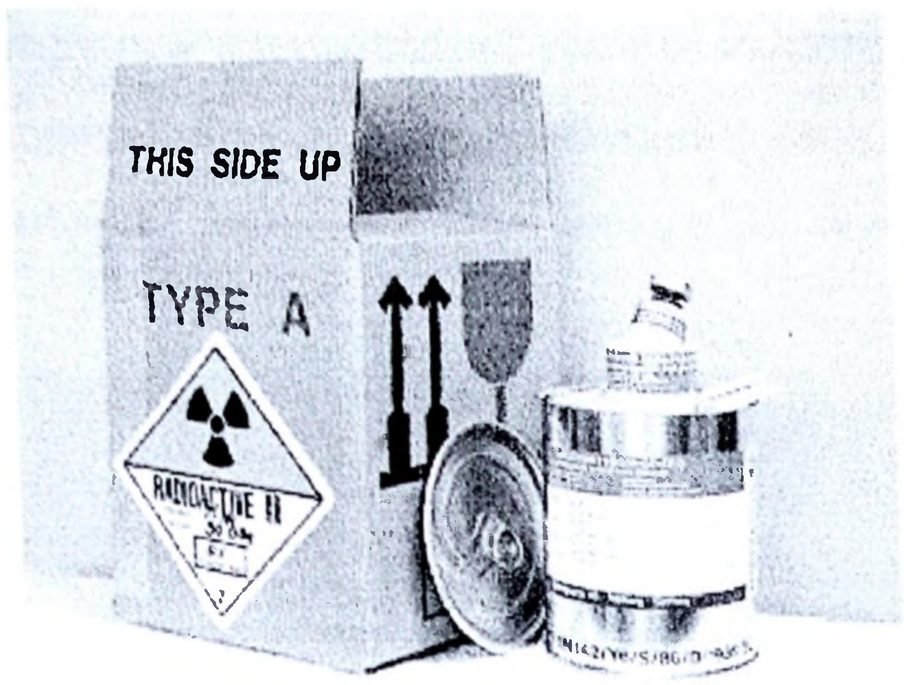
W zależności od stopnia zagrożenia otoczenia podczas transportu materiałów promieniotwórczych przewiduje się stosowanie różnych typów pojemników transportowych. Typ najprostszy, odpowiadający wzmocnionemu opakowaniu przemysłowemu, stosuje się do przewozu niewielkich ilości materiałów niskoaktywnych takich, jak rudy i koncentraty uranowe. Pojemnik taki musi jednak odpowiadać międzynarodowym standardom przewozu konwencjonalnych materiałów niebezpiecznych.



Źródło: rysunek pozyskany z prezentacji z T. Dziubiak, Transport ..., wyd. cyt.

Rys. 15. Pojemnik stosowany w transporcie lotniczym do przewozu materiałów promieniotwórczych o niskiej aktywności właściwej

Z kolei opakowanie typu A charakteryzuje trwałość, a ponadto opakowanie to daje gwarancje, że w normalnych warunkach transportu zabezpiecza zawartość przed utratą ,czy zwiększeniem poziomu promieniowania na zewnątrz.



Źródło: fotografia pozyskana z prezentacji z T. Dziubiak, Transport ..., wyd. cyt.

Fotografia 2. Opakowanie typu A do transportu materiałów radioaktywnych stosowany w transporcie lotniczym

Natomiast w wypadku, gdy aktywność promieniotwórcza przekracza ograniczenia narzucone opakowaniom typu A stosuje się opakowania typu B(U), które ograniczają prawdopodobieństwo uwolnienia zawartości lub zwiększenia dawki promieniowania nawet podczas ciężkiego wypadku.

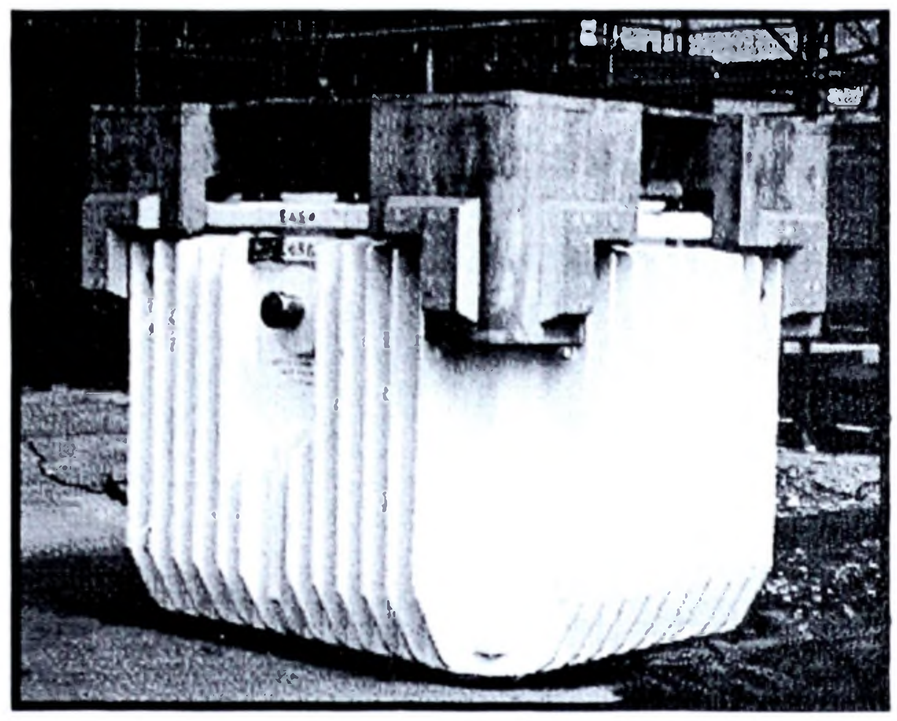


Źródło: fotografia pozyskana z prezentacji z T. Dziubiak, Transport ..., wyd. cyt.

Fotografia 3. Opakowanie typu B do transportu materiałów radioaktywnych stosowany w transporcie lotniczym

W transporcie lotniczym wykorzystuje się także opakowania typu C, które spełniają wszystkie wymogi dla opakowań typu A i B(U), a ponadto przechodzą dodatkowe testy na odporność termiczną, nakłuwanie, zderzenie przy dużej szybkości oraz wysokie ciśnienie.

Do transportu materiałów rozszczepialnych stosowane są specjalne opakowania typu AF, B(U)F), sprawdzane z uwzględnieniem zdolności do rozszczepiania promieniotwórczej zawartości. Spełniają one wszystkie wymagania dla opakowań typu A lub typu B.



Źródło: fotografia pozyskana z prezentacji z T. Dziubiak, Transport ..., wyd. cyt.

Fotografia 4. Opakowanie typu (AF, B(U)F) do transportu materiałów radioaktywnych stosowany w transporcie lotniczym

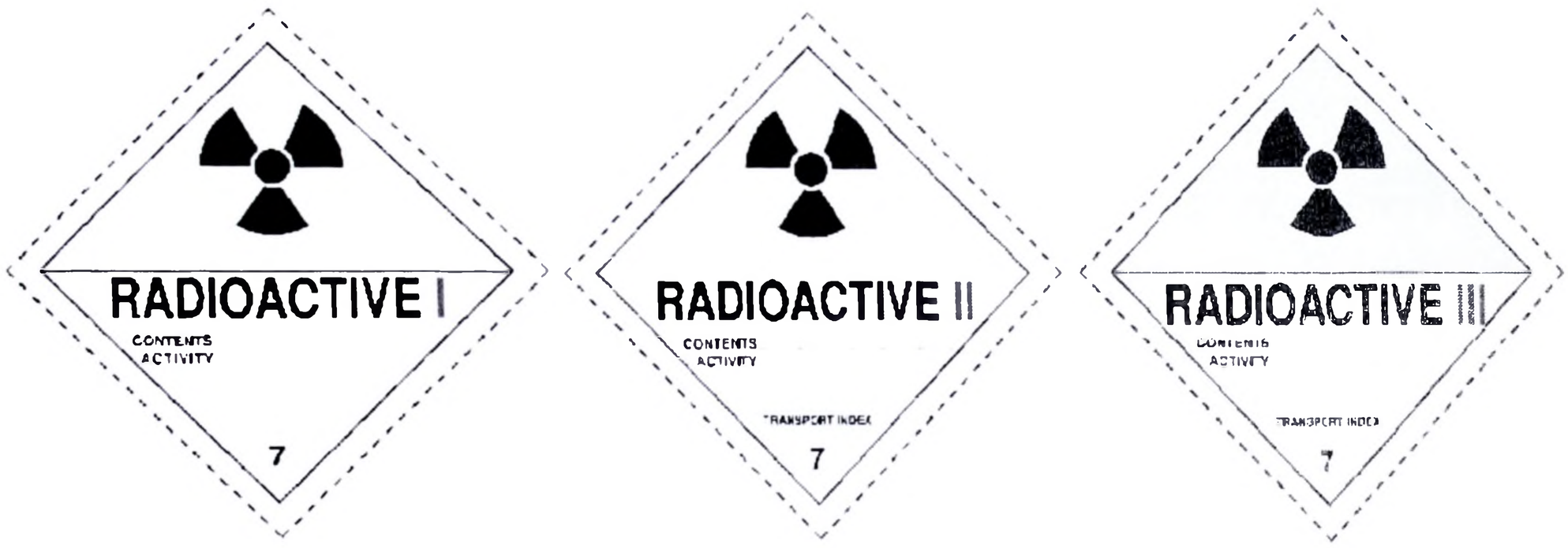
Świeże paliwo jądrowe drogą lotniczą transportuje się w pojemnikach osłonowych. Transport taki jest możliwy tylko dla potrzeb reaktorów badawczych. Elementy paliwowe pakowane są po sześć sztuk w lekkich pojemnikach rurowych. Należy podkreślić, że promieniowanie świeżego paliwa jest w porównaniu z promieniowaniem paliwa wypalonego wręcz śladowe.

Paliwo wypalone wytwarza bardzo silne promieniowanie gamma, emitowane przez produkty rozszczepienia i ich pochodne, i jest jednocześnie źródłem ciepła powstającego z rozpadu promieniotwórczego produktów rozszczepienia uranu. Pojemniki do transportu lotniczego tego rodzaju paliwa powinny posiadać szczelne i trwałe zamkniecie, osłonę przed promieniowaniem emitowanym przez transportowane materiały promieniotwórcze oraz odpowiedni system odprowadzania ciepła na zewnątrz.

Przewóz materiałów radioaktywnych do portu lotniczego, o aktywności większej od dopuszczalnej w przepisach przewozowych, wymaga uzyskanie zezwolenia Prezesa Państwowej Agencji Atomistyki.

Obsługa przesyłek z materiałami promieniotwórczymi jest istotnym elementem, bezpieczeństwa radiologicznego w porcie lotniczym. Przyjmowane i akceptowane do transportu lotniczego przesyłki poza wymaganiami ogólnymi, muszą spełniać

odpowiednie kryteria wytrzymałościowe w zakresie swych właściwości ochronnych.. Pracownicy lotniska obsługujący przesyłki promieniotwórcze muszą zawsze sprawdzać, czy posiadają one atest producenta potwierdzający, że przeszły odpowiednie badania. Każda przesyłka powinna posiadać na zewnętrznej powierzchni opakowania napis identyfikujący w czytelny i trwały sposób nadawcę i odbiorcę lub jednego z nich. Przesyłka taka powinna być także zaopatrzona w czytelny i trwały numer rozpoznawczy materiału poprzedzony literami „UN" oraz w prawidłową nazwę przewozową. Ponadto relatywnie do największego zmierzonego poziomu promieniowania w odległości 1 m od zewnętrznej powierzchni przesyłki oraz największego zmierzonego poziomu promieniowania na jej zewnętrznej powierzchni, każdą przesyłkę oznacza się tabliczką oznaczającą kategorię natężenia promieniowania: Tabliczki te o kolorach i liczbach rzymskich: I-Biała, II-Żółta, III-Żółta i umieszcza się na dwóch przeciwległych stronach przesyłki.



Źródło: rysunek pozyskany z prezentacji z T. Dziubiak, Transport ..., wyd. cyt.

Rys. 16. Oznaczenia przesyłek z materiałami promieniotwórczymi w transporcie lotniczym

Firma transportu lotniczego przewożąca przesyłki promieniotwórcze zapewnia właściwie ułożenie i posegregowanie opakowań oraz dołączenie do nich instrukcji postępowania z przesyłką w razie awarii. Ponadto, każdej przesyłce musi towarzyszyć dokument przewozowy stosowany w lotniczych przewozach materiałów promieniotwórczych, który powinien zawierać wszystkie potrzebne informacje. Niestosowanie się do scharakteryzowanych może spowodować w skrajnych przypadkach powstanie incydentu lub awarii radiologicznej, którego skutki dla organizmu ludzkiego przedstawia tabela 8.

Tabela 8. Skutki napromieniowania - dawki jednorazowe na całe ciało pochłonięte w krótkim okresie czasu

Lp.	Otrzymana dawka	Objawy	Skutki
1.	0,5 Sv	zmiany morfologiczne krwi	odwracalne
2.	1 Sv	złe samopoczucie	żadnych trwałych uszkodzeń
3.	2 Sv	nudności i wymioty u 25% osób	żadnych trwałych uszkodzeń
4.	2 ÷ 3 Sv	zaburzenia w tkankach krwiotwórczych	25% zgonów
5.	3 ÷ 5 Sv	dawka letalna	50% zgonów w przeciągu 30 dni
6.	5 ÷ 8 Sv		100% zgonów w przeciągu 30 dni
7.	10 Sv		100% zgonów w przeciągu kilku dni
8.	50 Sv		100% zgonów w przeciągu kilku godzin

Źródło: B. Filipiak, K. Józefowicz, Ochrona przed promieniowaniem jonizującym, Otwock-Świerk, 2003.

Rozległość stref skażeń substancjami radioaktywnymi oraz napromieniowania zależy od aktywności przewożonych przesyłek oraz rozmiarów jej uszkodzenia, a okres utrzymania się skażenia zwykle jest długi. Substancja promieniotwórcza może skazić teren lotniska i roślinność do głębokości kilkudziesięciu centymetrów, co wymagać będzie zdjęcia skażonej wierzchniej warstwy gruntu. Na wielkość skutków awarii i rozmiar strefy skażenia po zniszczeniu lub uszkodzeniu przesyłek, wywierają wpływ liczne czynniki. Najważniejsze z nich to aktywność substancji promieniotwórczej, rodzaj substancji, warunki meteorologiczne oraz wielkość awarii. Substancje radioaktywne swe szkodliwe właściwości zachowują do 20-80 lat.

Bezpieczeństwo radiologiczne portu lotniczego zagrożone jest najbardziej w wyniku zaistnienia następujących sytuacji:

- **prób przemytu materiałów radioaktywnych** - przyczyny nielegalnego przemytu wynikają często z zaprzestania kontroli administracyjnej i zaniku procedur bezpieczeństwa radiacyjnego np. w czasie długotrwałego magazynowania tych materiałów w instalacjach. Wówczas materiały zgromadzone w takich urządzeniach jak głowice teleterapeutyczne, przekaźniki przemysłowe, głowice defektoskopów itp. mogą być mimowolnie sprzedawane na przykład, jako części materiału do złomowania,

- **znakowania substancjami promieniotwórczymi materiałów, urządzenia oraz pieniędzy**. Sytuacje takie są łatwe do wykrycia, ale pomimo tego mogą stanowić zagrożenie dla personelu lotniska pasażerów oraz osób kontrolujących. Często osoby przewożące tego typu materiały nie wiedzą o ich skażeniu,

- **nielegalny przewóz substancji promieniotwórczych zawartych w materiałach jądrowych**. Przewóz taki realizowany jest często przez osoby mające małą wiedzę o technicznych właściwościach tych materiałów, stwarzanym niebezpieczeństwie lub ich rynkowej wartości.

- **niekontrolowane wwiezienie materiałów i odpadów promieniotwórczych.** Zagrożenia takie na lotniczym przejściu granicznym jest wynikiem sfałszowania deklaracji przewozowej (ukrycie rzeczywistego charakteru sprowadzanych materiałów).

Tabela 9. Przypadki ujawnionych prób nielegalnego przewozu materiałów radioaktywnych w Porcie Lotniczym Warszawa

Lp.	Data ujawnienia	Ilość szt.	Nazwa izotopu	Powód zatrzymania	Uwagi
1.	04.06.1999	2	J-125	Brak stosownych dokumentów przewozowych	Waga przesyłki 6 kg
2.	14.06.1999	1	A-241	Brak stosownych dokumentów przewozowych	Waga przesyłki 17 kg
3.	08.04.2000	1	In-111	Brak stosownych dokumentów dotyczących transportu i wykorzystania izotopu.	Nie zezwolono na wjazd do Polski osobie przewożącej izotop In-111
4.	12.03.2001	-		Podejrzenie o skażenie samolotu Boeing 737, rejs Moskwa - Warszawa.	
5.	23.07.2001	6	Ra-226	Busole (wskazówki pomalowano farbą z izotopem Ra – 226).	Nieoznakowana przesyłka tranzytowa

Źródło: T. Hadyś, Studium analizy przypadków wykrytych materiałów promieniotwórczych i jądrowych, na granicy państwowej, przez polską Straż Graniczną, Warszawa 2004.

W tabeli 9 opisano kilka wypadków zatrzymania przesyłek zawierających substancje promieniotwórcze oraz jeden wypadek podejrzenia o skażenie samolotu sub-

stancjami promieniotwórczymi. W takim wypadku pasażerowie, załoga, ładunek oraz wyładowany samolot przechodzą czynności kontrolne, trwające nawet kilka godzin. Samolot na ten czas jest wyłączany z bieżącej eksploatacji, co powoduje wymierne straty dla przewoźnika lotniczego oraz utrudnia funkcjonowanie portu lotniczego.

Proces ochrony portu lotniczego przed zagrożeniami materiałami radioaktywnymi i rozszczepialnymi władze portu realizują wraz z agentem handlingowym oraz Strażą Graniczną. Odpowiedzialność za tę ochronę ponoszą w porcie lotniczym dwa biura: **Biuro Ochrony** oraz **Biuro Techniczne**.

Biuro Ochrony posiada w swoich strukturach wyspecjalizowaną Służbę Zarządzania Ochroną i Bezpieczeństwem, która opracowuje projekty inwestycyjne, koncepcje rozwoju, oraz plany modernizacji portu lotniczego w zakresie ochrony oraz bezpieczeństwa radiologicznego. Służba ta opracowuje doraźne oraz okresowe analizy stanu ochrony radiologicznej. Odpowiada także za merytoryczne wdrażanie przepisów krajowych i europejskich regulujących problemy nierozprzestrzeniania broni masowego rażenia oraz ochrony lotnictwa cywilnego przed aktami bezprawnej ingerencji. Specjaliści tej Służby współpracują z Międzynarodową Organizacją Lotnictwa Cywilnego – ICAO (International Civil Aviation Organization), Komisją Europejską, Urzędem Lotnictwa Cywilnego, Międzynarodową Agencją Energii Atomowej – MAEA (International Atomic Energy Agency), Europejską Komisja Lotnictwa Cywilnego – ECAC (European Civil Aviation Conference), Europejską Wspólnotą Energii Atomowej – EURATOM, Państwową Agencją Atomistyki – PAA.

Służba Zarządzania Ochroną i Bezpieczeństwem przygotowuje wraz z Biurem Prawnym wewnętrzne regulacje prawne z zakresu ochrony radiologicznej i bezpieczeństwa portu lotniczego. W strukturze tej służby znajduje się również Zespół Zarządzania Kryzysowego, który odpowiada za zapewnienie obsługi logistycznej i wsparcia merytorycznego lokalnego sztabu kryzysowego.

Z kolei do zadań **Biura Technicznego** należy utrzymanie w ciągłej sprawności technicznej urządzeń do kontroli bezpieczeństwa oraz detekcji promieniowania jonizującego. Biuro Techniczne przez swoją wyspecjalizowaną Służbę Inżynierii Obiektowej monitoruje na bieżąco pracę oraz stan techniczny urządzeń. Dokonuje przeglądów okresowych urządzeń, wykorzystując zarówno własnych specjalistów, jak i specjalistów producenta urządzeń detekcyjnych w ramach zawartych umów gwarancyjnych i pogwarancyjnych. W strukturze opisywanej służby funkcjonuje Zespół Specjalistów Służby Inżynierii Obiektowej, w którym pracuje specjalista ds. systemów

specjalnych, który posiada również uprawnienia inspektora ochrony radiologicznej nadawane decyzją prezesa Państwowej Agencji Atomistyki[133].

Inspektor ochrony radiologicznej, po konsultacji z Biurem Ochrony, opracowuje projekty wewnętrznych regulacji prawnych z zakresu bezpieczeństwa radiologicznego oraz ochrony radiologicznej portu lotniczego. Inspektor ten nadzoruje przestrzeganie w porcie lotniczym zadań ochrony mających związek z promieniowaniem radioaktywnym. Nadzoruje on prowadzenie działalności oraz prowadzenie dokumentacji w zakresie bezpieczeństwa jądrowego oraz ochrony radiologicznej, pracowników oraz osób przebywających w porcie w warunkach narażenia na promieniowanie jonizujące. Inspektor ten nadzoruje zapewnienie warunków, w których pracownik może być dopuszczony do pracy na danym stanowisku. Szkoli tych pracowników na stanowisku w zakresie ochrony radiologicznej i bezpieczeństwa jądrowego.

Opracowuje także program pomiarów dozymetrycznych w środowisku pracy, ewidencji i pomiarów dawek indywidualnych i przedstawianie ich w formie raportów do zatwierdzenia kierownikowi jednostki organizacyjnej. Natomiast w trakcie zdarzenia radiacyjnego ma obowiązek nadzorować postępowanie zgodne z lotniskowym planem postępowania awaryjnego[134]. Ponadto występuje on do dyrektora portu lotniczego, z wnioskiem o zmianę warunków pracy tych pracowników, których wyniki poziomu otrzymanych dawek wskazują podwyższony poziom.

Ważnym działaniem inspektora ochrony radiologicznej w porcie lotniczym jest sprawdzanie i badanie urządzeń ochronnych oraz przyrządów pomiarowych w zakresie ochrony przed promieniowaniem jonizującym, skuteczności stosowanych środków oraz ich właściwego użytkowania. Inspektor weryfikuje kwalifikacje pracowników w zakresie ochrony radiologicznej oraz bezpieczeństwa jądrowego[135].

Z kolei agent handlingowy[136] przez swoją wyspecjalizowaną komórkę organizacyjną: Pion Cargo LOT GROUND SERVICES Sp. z o.o. (LGS) realizuje w porcie Lotniczym obsługę i przewóz materiałów niebezpiecznych zgodnie z przepisami in-

---

[133] Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie stanowisk mających istotne znaczenie dla bezpieczeństwa jądrowego i ochrony radiologicznej oraz inspektorów ochrony radiologicznej (Dz. U. nr 21, poz. 173).

[134] Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych (Dz. U. Nr 20. poz. 169) .

[135] Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie stanowisk mających istotne znaczenie dla bezpieczeństwa jądrowego i ochrony radiologicznej oraz inspektorów ochrony radiologicznej (Dz. U. Nr 21, poz. 173) .

[136] *Agent handlingowy [handling agent] – podmiot prowadzący obsługę naziemną pasażerów, bagażów, załóg i samolotów w imieniu linii lotniczej*, http://www.airport-poznan.com.pl/pl/slownik.html, 28.05.2009.

strukcji technicznych ICAO oraz instrukcji technicznych Międzynarodowego Stowarzyszenia Transportu Lotniczego (International Air Transport Association) IATA DGR[137]. Cargo dysponuje pięcioma pomieszczeniami chłodniami z możliwością dostosowywania temperatury do potrzeb ładunków. Magazyny specjalne przeznaczone są do przechowywania przesyłek specjalnych takich jak: materiały radioaktywne, żywe zwierzęta, poczta dyplomatyczna, przesyłki wartościowe. Personel Pionu Cargo posiada odpowiednie kwalifikacje spełniające zalecenia międzynarodowe i krajowe w zakresie obsługi ładunków lotniczych.

Wreszcie Straż Graniczna chroni terytorium państwa przed niedozwolonym przewozem substancji szkodliwych oraz zwalczanie przemytu materiałów niebezpiecznych, w tym radioaktywnych. Placówka Straży Granicznej (PSG) w porcie lotniczym realizując swe zadania, zapobiega, między innymi, transportowaniu przez granicę państwową szkodliwych substancji chemicznych, materiałów promieniotwórczych i jądrowych oraz odpadów. W ramach prowadzonej kontroli chemiczno-radiometrycznej funkcjonariusze PSG posiadają uprawnienia do zatrzymywania, kontroli, cofania z granicy substancji chemicznych oraz materiałów promieniotwórczych[138]. Kontrolerzy PSG zostali przeszkoleni w Instytucie Energii Jądrowej w Świerku. Placówka Straży Granicznej stworzyła system techniczny, który skutecznie wspiera działania funkcjonariuszy. W skład systemu kontroli radiometrycznej wchodzą między innymi urządzenia radiometryczne takie, jak: stacjonarne monitory promieniowania, przenośne monitory promieniowania stanowiące stałe wyposażenie przejścia granicznego Warszawa-Okęcie

Reasumując organizacja przedsięwzięć przeciwdziałania w porcie lotniczym całemu spektrum zagrożeń terrorystycznych, szczególnie w aspekcie właściwości portu ułatwiających atak terrorystyczny wymaga szczególnego podejścia. Napięcie psychiczne, stres i deficyt czasu towarzyszył będzie wykonaniu każdego przedsięwzięcia antyterrorystycznego. Zatem właściwe wykonanie procedury przeciwdziałania terroryzmowi musi być poprzedzone szczegółowo opracowanymi instrukcjami postępowania, które powinny zawierać szczegółowe procedury dla każdego rodzaju scharakteryzowanych sytuacji zagrożeń, ujmujące:

- rodzaj grożącego niebezpieczeństwa;

---

[137] Podręcznik IATA DGR (International Air Transport Association - Dangerous Goods Regulation) Międzynarodowe Stowarzyszenie Transportu Lotniczego - Regulacje dotyczące Towarów Niebezpiecznych, wydanie 47, 1 stycznia-31 grudnia 2008r.

[138] Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. nr 78 poz. 462).

- precyzyjnie określony cel podejmowanej akcji;
- odpowiedni kryptonim (hasło) przypisany każdemu rodzajowi zagrożenia;
- osoby (organy) mające uprawnienia do podjęcia decyzji o uruchomieniu procedury bezpieczeństwa;
- osobę (organ) odpowiedzialną za kierowanie akcją, wraz ze szczegółowymi kompetencjami do podejmowania określonych decyzji i warunki ograniczające je;
- angażowane siły i środki, wskazując na sposób i warunki ich uruchomienia oraz instytucje współodpowiedzialne i sposób ich powiadomienia;
- zasięg realizowanej akcji i wynikające z niej restrykcje;
- uprawnienia do zakończenia akcji;
- czynności wszystkich osób biorących udział w akcji oraz osób przebywających w rejonie akcji.

5. KONCEPCJA SYSTEMU OCHRONY MIAST POLSKICH W WARUNKACH ZAGROŻEŃ TERRORYSTYCZNYCH

W myśleniu o ochronie miast w warunkach zagrożeń terrorystycznych można wyróżnić dwie zasadnicze strategie. Pierwsza koncentruje się na działaniach przygotowujących służby do działań w sytuacjach szczególnych, druga zaś skupia się na takim kształtowaniu otoczenia, aby minimalizować straty wynikłe w przypadku ich zagrożenia. Dotychczasowe przepisy cywilno i wojskowe regulujące sposób przeciwdziałania zagrożeniom terrorystycznym (np. procedury dotyczące łączności i współdziałania) na szczeblu krajowym okazały się niewystarczające, chociaż ich ustalanie pozostaje nadal w gestii władz państwowych.

Wzrost znaczenia ochrony miast polskich w warunkach zagrożeń terrorystycznych, powoduje, że staje się on pierwszoplanowym elementem systemu bezpieczeństwa w RP. Skuteczność i efektywność działania systemu stają się coraz trudniejsze, ze względu na ciągłe zagrożenie wystąpieniem ataków terrorystycznych, które mogą przybrać postać wypadków o charakterze masowym, jak również katastrof lotniczych.

Cywilno – wojskowy system ochrony miast polskich w warunkach zagrożeń terrorystycznych, winien sprostać zwiększonym wymaganiom, a tym samym umożliwić niezawodne i sprawne działanie.

System cywilno – wojskowej ochrony miast polskich powinno charakteryzować zastosowanie nowoczesnych środków transportu naziemnego i powietrznego oraz stanowisk kierowania akcjami przeciwterrorystycznych, jak również odpowiedni dobór kadr w jednostkach odpowiedzialnych za bezpieczeństwo i walkę z terrorystami.

Specyfika prowadzenia działań w wypadkach o charakterze masowym, jak również katastrofach lotniczych wymaga, aby cywilno – wojskowy system ochrony miast polskich był zdolny do właściwej oceny zaistniałej sytuacji i podjęcia w jak najkrótszym czasie działań.

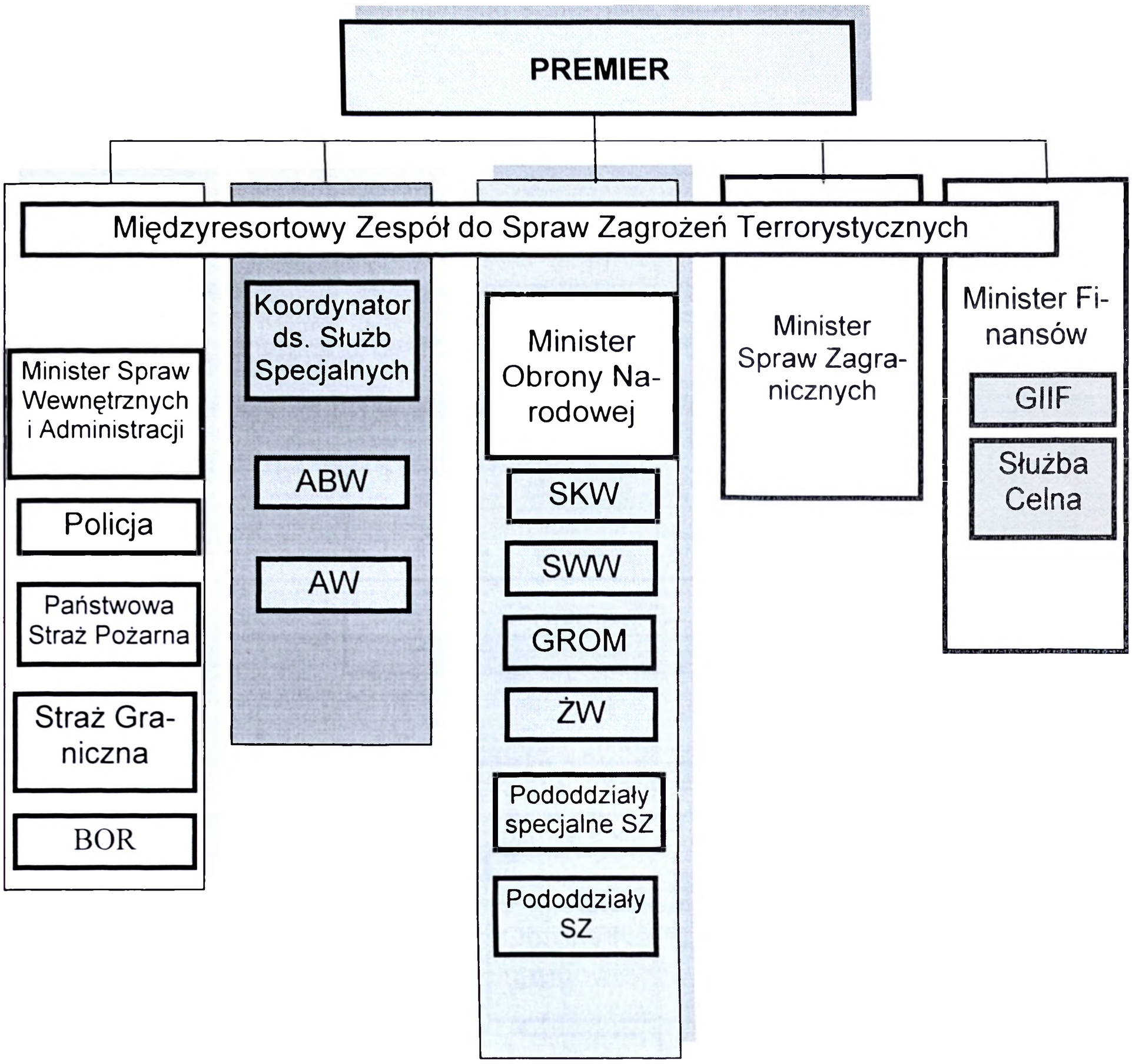
Cywilno – wojskowa ochrona miast polskich realizowana przez wyspecjalizowane siły wyposażone w najnowocześniejszy sprzęt nie spełni wymagań, jeśli nie będzie oparty o niezawodne, cyfrowe urządzenia i trakty łączności radiowej, radiolinowej lub satelitarnej, bowiem utrudni to przekazywanie informacji o zdarzeniach.

Dlatego też w przyszłości system ochrony miast powinien:

- być wyposażony w najnowszej generacji środki umożliwiające prowadzenie działań przeciwterrorystycznych;
- być wyposażony w nowoczesne pojazdy umożliwiające transport sił w rejony zagrożone;
- być wyposażony w cyfrowe urządzenia i trakty łączności radiowej lub satelitarnej umożliwiające kierowanie i współdziałanie podczas akcji;
- być wyposażony w sprzęt informatyczny pozwalający na tworzenie baz danych o siłach i środkach mogących brać udział w akcjach po wystąpieniu zdarzenia.

Podstawą systemu ochrony miast w warunkach zagrożeń terrorystycznych powinny być siły i środki podmiotów przeznaczonych do walki z terroryzmem, a także siły i środki odpowiedzialne za ratownictwo.

W ujęciu systemowym, szeroko propagowanym przez prof. Piotra Sienkiewicza, w każdym obiekcie złożonym, rozpatrywanym jako system, zawsze występuje element centralny (tzw. funkcja centrum). W systemie ochrony miast polskich złożonym ze wskazanych powyżej podsystemów, na dzień dzisiejszy, elementem centralnym jest Premier Rządu (rys.17).



Rys. 17. System cywilno – wojskowej ochrony miast polskich w warunkach zagrożeń terrorystycznych *(Źródło: Opracowanie własne)*.

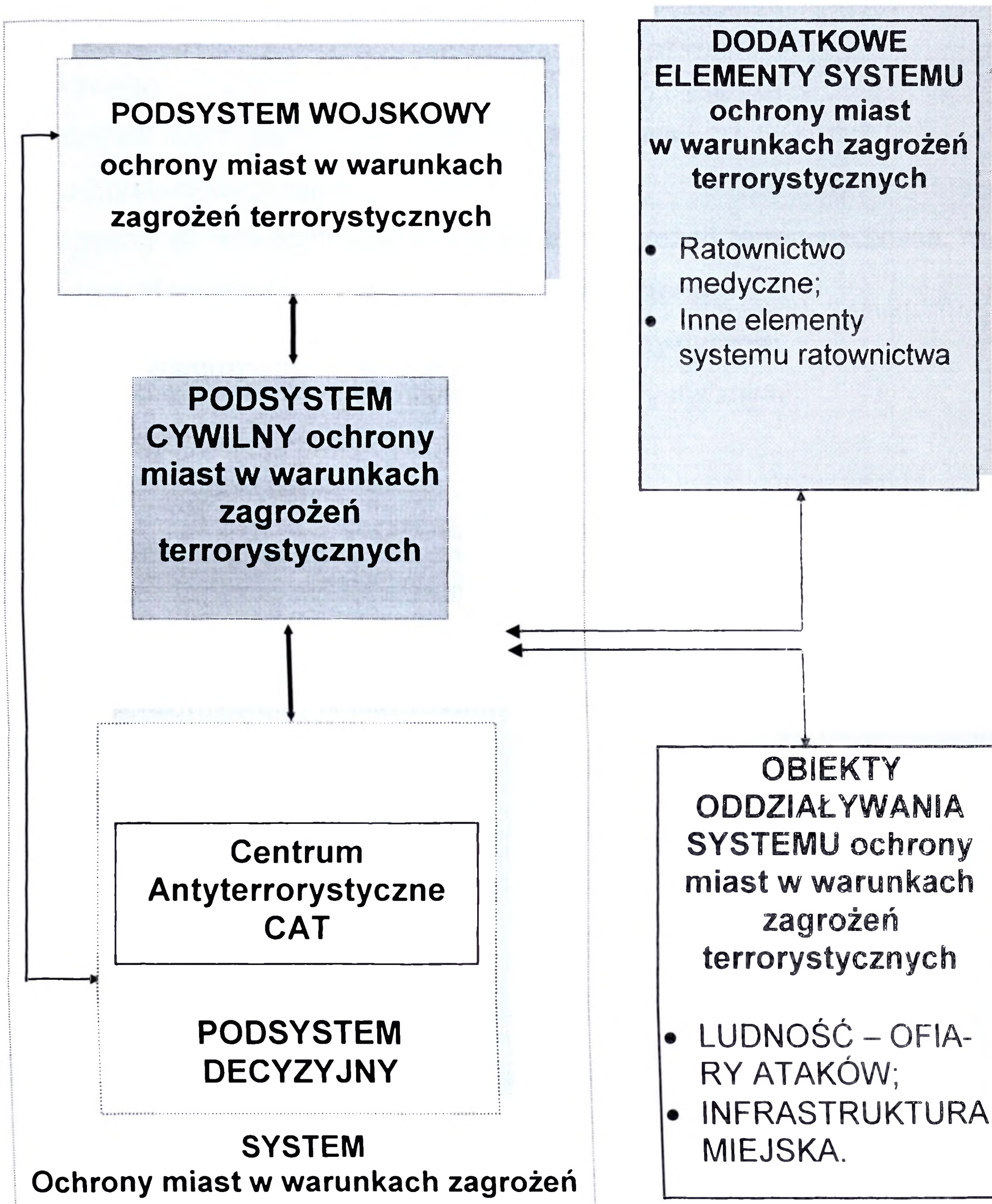
Można ją traktować jako organ koordynujący[139] na poziomie strategicznym ochrony miast polskich w warunkach zagrożeń terrorystycznych w RP. Wpływ na funkcjonowanie systemu ochrony miast polskich wywierają:

- Ministerstwo Spraw Wewnętrznych i Administracji (MSWiA);
- Służby Specjalne wraz z Koordynatorem ds. Służb Specjalnych;
- Ministerstwo Obrony Narodowej (MON)
- Ministerstwo Spraw Zagranicznych (MSZ);
- Ministerstwo Finansów (MF).

---

[139] Według prof. P. Sienkiewicza, koordynacja jest podstawową funkcją realizowaną przez każdy element centralny (centrum) systemu; zob. P. Sienkiewicz, *Podstawy teorii systemów,* Warszawa 1993r., s.20.

Jak wynika z przedstawionego schematu, łączą się przede wszystkim cywilne i wojskowe podsystemy.



Rys. 18. Cywilno – wojskowy system ochrony miast polskich w warunkach zagrożeń terrorystycznych *(Opracowanie własne).*

Analiza funkcjonowania systemu ochrony miast polskich przeprowadzona została w oparciu o schemat, który odzwierciedla procesy zachodzące w systemie. Jego budowę przedstawiono na rys.18.

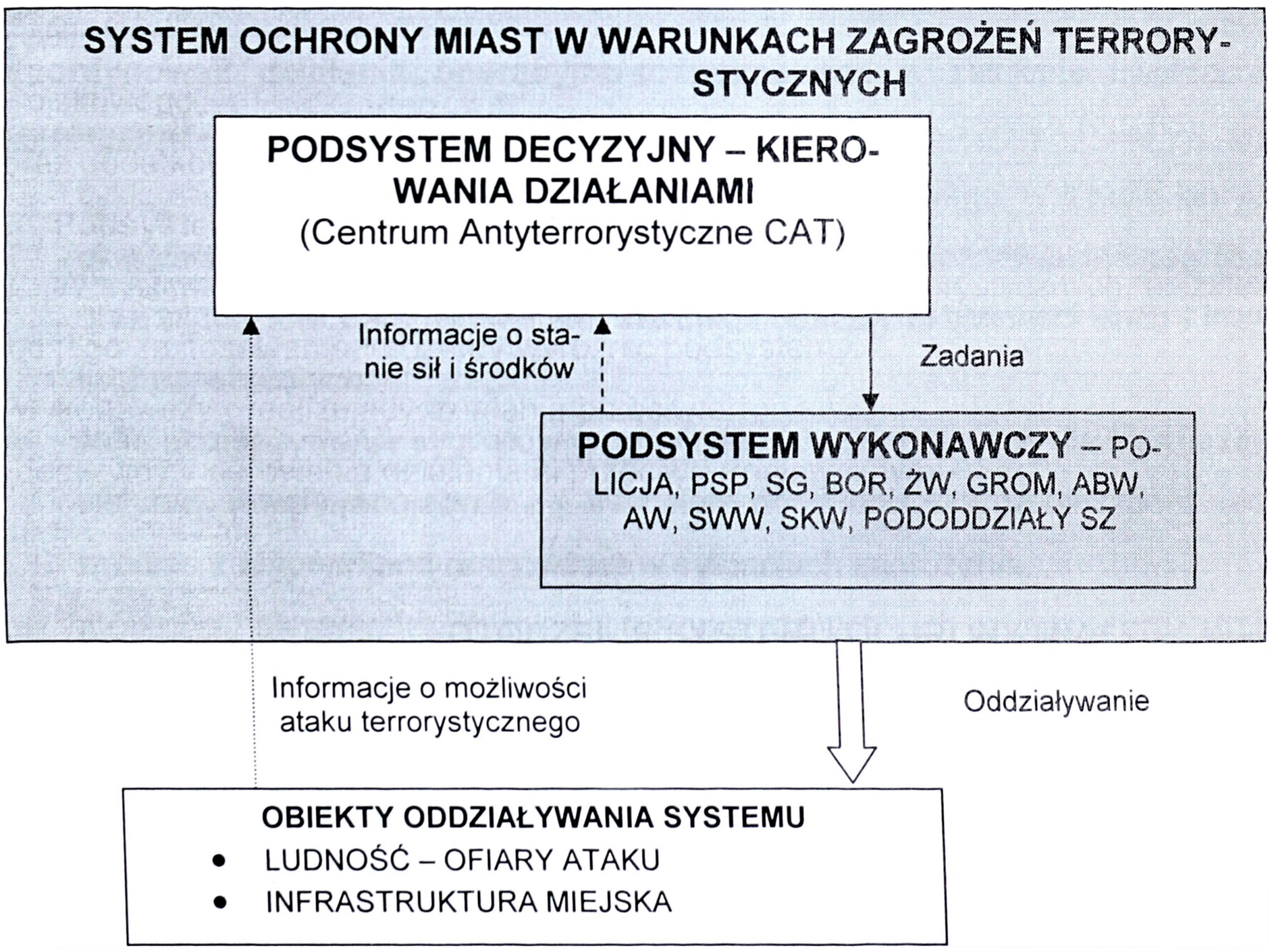
System ochrony miast polskich składa się z następujących podsystemów:

- decyzyjnego;
- cywilnego;
- wojskowego;
- oraz dodatkowych elementów systemu ratownictwa.

Podsystem decyzyjny

W systemie ochrony miast w warunkach zagrożeń terrorystycznych, niezależnie od jego zastosowania, możemy wyróżnić podsystemy:

a. wykonawczy - realizujący działania przeciwterrorystyczne;
b. decyzyjny - kierowania działaniami przeciwterrorystycznymi.



Rys. 19. Model systemu ochrony miast w warunkach zagrożeń terrorystycznych *(Opracowanie własne)*

Podsystem wykonawczy stanowią wyspecjalizowane służby (POLICJA, PSP, SG, BOR, ŻW, GROM, ABW, AW, SWW, SKW, PODODDZIAŁY SZ) wyposażone w sprzęt i środki pozwalające skutecznie zapobiegać niepożądanym następstwom zdarzeń, zagrażających życiu i zdrowiu ludności.

Podsystem decyzyjny (kierowania działaniami) realizuje procesy informacyjno-decyzyjne systemu: przyjmuje informacje o zdarzeniach (wymagających działań), określa sposób przeciwdziałania im i kieruje bezpośrednim oddziaływaniem podsystemu wykonawczego. Każdy z ośrodków decyzyjnych, odpowiednio do swoich kompetencji, powinien:

- **wspomagać proces decyzyjny w przypadku realnego zagrożenia atakiem terrorystycznym - CAT niezwłocznie po uzyskaniu wiedzy o możliwym zamachu przekazywać będzie Prezesowi Rady Ministrów, Ministrowi Spraw Wewnętrznych i Administracji (docelowo również Rządowemu Centrum Bezpieczeństwa) wszelkie dane pozwalające na przygotowanie i zabezpieczenie sił i środków niezbędnych do prawidłowego reagowania kryzysowego;**
- **koordynować działania operacyjno-rozpoznawcze w zakresie zwalczania terroryzmu - realizowane m.in. poprzez:**
  - cykliczne lub doraźne narady osób szczebla decyzyjnego, w trakcie których określane będą zadania do realizacji w ramach rozpoznawanych zagrożeń oraz wytyczane perspektywiczne kierunki i obszary aktywności służb i instytucji państwowych;
  - stałe przekazywanie sygnałów o potencjalnych zagrożeniach dla kierownictw instytucji współpracujących z CAT celem 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 - potencjalnych celów ataku terrorystycznego.

W zakresie analityczno-informacyjnym:

- sporządzać aktualne, syntetyczne i całościowe informacje 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;

- zakres prognoz - długo- i krótkookresowych - poziomu zagrożenia terrorystycznego Polski;
- analiz zagrożenia terrorystycznego w innych państwach w kontekście bezpieczeństwa strategicznych interesów i obywateli RP;
- udział w sporządzaniu ocen funkcjonowania systemów ochrony elementów infrastruktury krytycznej kraju pod kątem usunięcia ewentualnych nieprawidłowości
- udział w opracowywaniu i nowelizowaniu procedur reagowania kryzysowego na wypadek ataku oraz sporządzanie algorytmów działań przed zamachem;
- wspomaganie po ewentualnym zamachu terrorystycznym - na płaszczyźnie analityczno-informacyjnej - działań służb podległych MSWiA oraz innych podmiotów uczestniczących w ochronie antyterrorystycznej Polski;
- posiadać i na bieżąco aktualizować zbiory danych (informacji podstawowych) o posiadanym potencjale sił, środków i zasobów oraz możliwościach jego wykorzystania,
- gromadzić i zdobywać wiedzę, analizując doświadczenia innych w tym zakresie, o przyczynach i źródłach powstawania zagrożeń oraz ich skutkach;

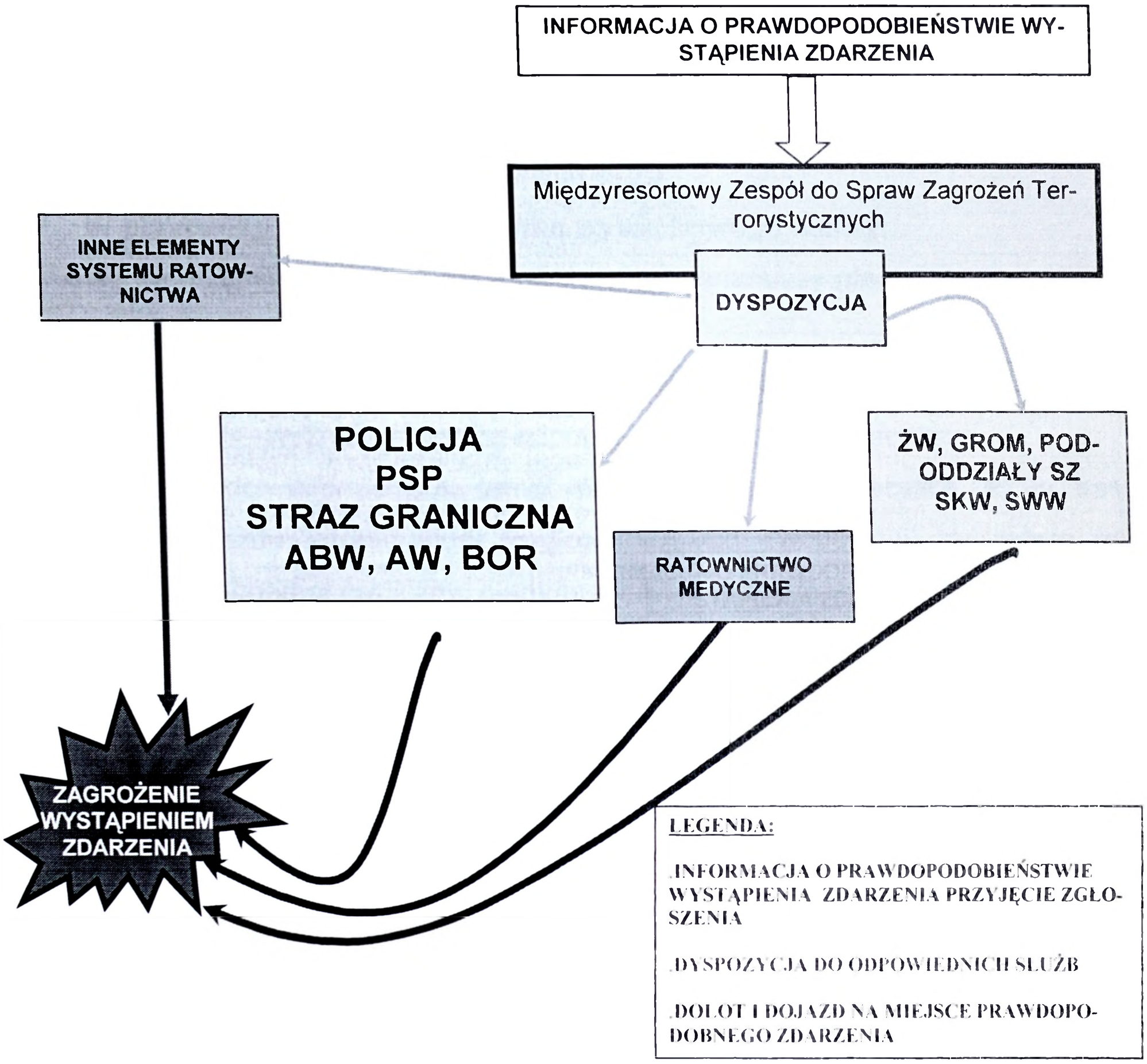
Z analizy czynności wykonywanych w procesie działań przeciwterrorystycznych od chwili prawdopodobieństwa zaistnienia zdarzenia, wymagającego takich działań do ich zakończenia, wynika, że niezależnie od dziedziny jego wystąpienia mamy do czynienia z cyklem realizacyjnym działań obejmującą[140]:

1. **Informacja o prawdopodobieństwie wystąpienia zdarzenia**, wymagająca interwencji (udziału) sił i środków.
2. **Analiza zdarzenia i podjęcie decyzji** o zakresie zastosowania działań (interwencji).
3. **Przemieszczenie sił i środków do miejsca zdarzenia**.
4. **Prowadzenie działań przez** siły i środki.
5. **Powrót z działań.**
6. **Zakończenie działań,** tj. sporządzenie dokumentacji z przeprowadzonych działań oraz odtworzenie stanu zdatności sił i środków do realizacji następnych zadań.

---

[140] Kołodziński, E.: Komputerowe wspomaganie procesów informacyjno – decyzyjnych ratownictwa. II Konferencja naukowa ZARZĄDZANIE KRYZYSOWE nt. „Ratownictwo w sytuacjach kryzysowych" Akademia Morska w Szczecinie 18.06.2004 r. s.156.

Skuteczność działania systemu zależy od jakości realizacji czynności przypisanych jego podsystemom, w wyróżnionych etapach cyklu realizacyjnego działań. Każdy podsystem, a w tym każdy jego element składowy stanowiący nieodzowną i integralną część całości systemu.



Rys. 20. Ogólny schemat działania systemu ochrony miast podczas prawdopodobieństwa wystąpienia zdarzenia *(Opracowanie własne)*

Informacja o prawdopodobieństwie wystąpienia zdarzenia

Procedura przyjęcia zgłoszenia o prawdopodobieństwie wystąpienia zdarzenia zależy od źródła informacji. Działania prowadzone są wówczas zgodnie z procedurą postępowania przewidzianą dla prawdopodobieństwa wystąpienia danego zdarzenia. W przypadku przeciwnym zachodzi konieczność identyfikacji: miejsca, rodzaju, i skali

potencjalnego zagrożenia. Rzeczą istotną jest zweryfikowanie prawdziwości zajścia zdarzenia w celu wyeliminowania fałszywego alarmu.

Analiza sposobu działań i podjęcie decyzji

Po przyjęciu zgłoszenia o zajściu zdarzenia zachodzi konieczność analizy sposobu prowadzania działań, oceny czy siły i środki, jakimi dysponuje dany szczebel organizacyjny są w stanie samodzielnie przeprowadzić akcję oraz czy zachodzi potrzeba powiadomienia o zdarzeniu innych służb.

W przypadku podłożenia ładunku wybuchowego należy:

1. Wysłać na miejsce incydentu bombowego funkcjonariuszy nieetatowej grupy rozpoznania minersko-pirotechnicznego (NGRMP).
2. Nawiązać współpracę ze stanowiskami dowodzenia służb ratowniczych, inspekcji, służb miejskich - wyznaczyć osobę odpowiedzialną za obieg informacji.
3. Zbierać wszelkich informacji na temat miejsca zdarzenia (specyfika terenu, trasy dojazdu i odjazdu, infrastruktura mediów miejskich - wodociągi, energetyka, gazownictwo) - schemat graficzny, plany budynków, mapy topograficzne.
4. Wprowadzić procedury, postępowania.
5. Zbilansować dostępne siły i środki pod kątem niezbędnych potrzeb do prawidłowego zabezpieczenia miejsca zdarzenia, ewakuacji ludności, zabezpieczenia dróg dojazdu, pilotowania pojazdów służb medycznych i ratowniczych - określenie potrzeb w zakresie uzupełnienia stanów osobowych, sprzętu transportowego i łączności z innych jednostek.

W przypadku podłożenia ładunku wybuchowego z zastosowaniem materiału promieniotwórczego należy:

1. Powiadomić natychmiast Wojewódzkiego Inspektora Oddziału Radiologicznego funkcjonującego na terenie danego województwa (zazwyczaj jego siedzibą jest Wojewódzka Stacja Sanitarno-Epidemiologiczna).
2. Dokonać analizy zdarzenia, w tym: oceny zagrożenia, prognozy jego dalszego rozwoju, sposobu pozyskiwania, gromadzenia, analizowania i wymiany informacji na potrzeby dowodzenia i współdziałania i na tej podstawie wypracować koncepcję działania.
3. Rozpocząć informowanie i ostrzeganie zagrożonej ludności.

4. Ustalić warianty współdziałania ze służbami ratowniczymi w związku z zaistniałym zdarzeniem.
5. Na bieżąco opracowywać plany działania wynikające z rozwoju zagrożenia i potrzeby zabezpieczenia bezpieczeństwa i porządku w miejscu prowadzenia działań ratowniczych.
6. Na bieżąco analizować siły i środki niezbędne do zabezpieczenia akcji ratowniczej, w tym: siły i środki własne oraz siły wsparcia, a także możliwości ich przemieszczania i wyposażenia w sprzęt ochronny niezbędny do prowadzenia działań.
7. Zapewnić funkcjonowanie systemów łączności w zakresie współdziałania sił biorących udział w akcji ratowniczej.
8. Zapewnić obieg informacji o zdarzeniu i podejmowanych.

W przypadku podłożenia ładunku wybuchowego z zastosowaniem środka mikrobiologicznego należy:

1. Dokonać analizy zdarzenia, w tym: oceny zagrożenia, prognozy jego dalszego rozwoju, sposobu pozyskiwania, gromadzenia, analizowania i wymiany informacji na potrzeby dowodzenia i współdziałania, na tej podstawie wypracować koncepcje działania.
2. Zlecić identyfikację osób pierwotnie narażonych na kontakt z czynnikiem biologicznym i ich dalszych kontaktów z innymi osobami.
3. Rozpocząć informowanie i ostrzeganie zagrożonej ludności
4. Ustalić warianty współdziałania ze służbami ratowniczymi w związku z zaistniałym zdarzeniem.
5. Na bieżąco opracowywać plany działania wynikające z rozwoju zagrożenia i potrzeby zabezpieczenia bezpieczeństwa i porządku w miejscu prowadzenia działań ratowniczych.
6. Zapewnić funkcjonowanie systemów łączności w zakresie współdziałania sił biorących udział w akcji ratowniczej.
7. Zapewnić obieg informacji o zdarzeniu i podejmowanych działaniach Policji i innych służb.

W przypadku podłożenia ładunku wybuchowego z zastosowaniem środka chemicznego należy:

1. Dokonać analizy zdarzenia, w tym: oceny zagrożenia, prognozy jego dalszego rozwoju, sposobu pozyskiwania, gromadzenia, analizowania i wymiany informacji na potrzeby dowodzenia i współdziałania, na tej podstawie wypracować koncepcję działania.
2. Rozpocząć informowanie i ostrzeganie zagrożonej ludności.
3. Ustalić warianty współdziałania ze służbami ratowniczymi w związku z zaistniałym zdarzeniem.
4. Na bieżąco opracowywać plany działania wynikające z rozwoju zagrożenia i potrzeby zabezpieczenia bezpieczeństwa i porządku w miejscu prowadzenia działań ratowniczych.
5. Na bieżąco analizować siły i środki niezbędne do zabezpieczenia akcji ratowniczej, w tym siły i środki wsparcia, a także możliwości ich przemieszczania i wyposażenia w sprzęt ochronny niezbędny do prowadzenia działań.
6. Utrzymywać bieżącą współpracę z instytucjami biorącymi udział w akcji ratowniczej.
7. Zapewnić funkcjonowanie systemów łączności w zakresie współdziałania sił biorącymi udział w akcji ratowniczej.

W przypadku uprowadzenie środka transportu w komunikacji lotniczej należy:

1. Dokonać wstępnej analizy i weryfikacji informacji.
2. Przekazać informacji zgodnie z kompetencjami do: Policji, MON i innych służb odpowiedzialnych za bezpieczeństwo
3. Podjąć działania operacyjno-rozpoznawcze ukierunkowane na weryfikowanie informacji o zdarzeniu
4. Podjąć decyzję o użyciu odpowiednich sił wojskowych i policyjnych (po dokonaniu wstępnej oceny i analizy sytuacji), tj.:
   - specjalistycznych jednostek i komórek organizacyjnych Policji w portach lotniczych,
   - jednostek lub komórek antyterrorystycznych policji, SG oraz MON,
   - Centralnego Biura Śledczego KGP w zakresie rozpoznania operacyjnego,

5. Prowadzić pełną analizę oraz rozpoznanie niezbędne do planowania rozwiązania siłowego, w tym:
   - zewnętrznego dotyczącego miejsca zdarzenia (plany, topografia całego rejonu działania),
   - wewnętrznego dotyczącego samolotu (dane organizacyjno-techniczne),
   - osobowego (dane pasażerów, ich bagażu, członków załogi i ich doświadczenia, porywaczy).
6. W trybie alarmowym skierować do działań siły pododdziału antyterrorystycznego, oddziału prewencji, zespołu negocjatorów, psychologów, grupy operacyjno-dochodzeniowej, pogotowia ratunkowego. Państwowej Straży Pożarnej

W przypadku uprowadzenie środka transportu w komunikacji lądowej należy:

1. Dokonać wstępnej analizy i weryfikacji informacji.
2. Przekazać informacje zgodnie z kompetencjami do odpowiednich służb.
3. Zarządzić akcję lub operację (w zależności od rodzaju i poziomu zagrożenia)
4. Powiadomić w trybie alarmowym oraz skierować do działań policyjne lub wojskowe pododdziały antyterrorystyczne, pododdziały prewencji Policji i ŻW, Zespół Negocjatorów, PSP oraz służby ratownictwa medycznego.
5. Prowadzić analizę niezbędną do uzyskania informacji o:
   - - miejscu zdarzenia lub pościgu,
   - - terrorystach,
   - - zakładnikach,
   - - rodzaju środka transportu.

W przypadku uprowadzenie środka transportu w komunikacji wodnej należy:

1. Dokonać wstępnej analizy i weryfikacji informacji.
2. Przekazać informacje zgodnie z kompetencjami do odpowiednich służb.
3. Zarządzić akcję lub operację (w zależności od rodzaju i poziomu zagrożenia)
4. Powiadomić w trybie alarmowym oraz skierować do działań policyjne lub wojskowe pododdziały antyterrorystyczne, pododdziały prewencji Policji i ŻW, specjalistyczne jednostki Policji (Policja Wodna), Centralne Biuro Śledcze KGP w zakre-

sie rozpoznania operacyjnego, Zespół Negocjatorów, PSP oraz służby ratownictwa medycznego.

5. Prowadzić analizy niezbędne do planowania rozwiązania siłowego, a dotyczącego: - miejsca zdarzenia (akwen, głębokość, odległość od brzegu), - jednostki pływającej (dane techniczne, jednostki bliźniacze), - osób (pasażerów, terrorystów).

W przypadku zajęcia obiektu, w tym również z przetrzymywaniem zakładników (uprowadzeniem zakładników) należy:

1. Przyjąć informację o zaistniałym zdarzeniu, dokonać jej oceny i podjąć wstępne czynności zgodnie z algorytmem postępowania.
2. Powiadomić służby odpowiedzialne za bezpieczeństwo.
3. Zapewnić sprawny obieg informacji.
4. Opracować plan obezwładnienia sprawców uprowadzenia osoby (osób) przez siły antyterrorystyczne.

W przypadku zdarzeń o dużych rozmiarach, wymagających uczestnictwa wszystkich dostępnych sił i środków wyznaczana jest:

- **służba wiodąca** - pełniąca rolę kierowniczą w danym zdarzeniu;
- **służby pomocnicze** - wspomagające działania podmiotu kierowniczego;
- **służby współdziałające** - biorące udział w akcji w ograniczonym zakresie, do wykonania określonych czynności.

Podjęta decyzja przekazywana jest do uczestników akcji, którzy rozpoczynają swoje działania zgodnie z procedurami określającymi ich role i zadania w przypadku danego zdarzenia i przyjętego sposobu działań.

Przemieszczenie sił i środków do miejsca zdarzenia

Czas jaki upływa od chwili podjęcia decyzji o siłach i środkach uczestniczących w akcji do chwili rozpoczęcia jej prowadzenia przez nich zależy od: sprawności organizacyjnej elementów wykonawczych, poziomu wyszkolenia zespołów ludzkich, jakości sprzętu i środków jakimi dysponują jednostki, a także czasu dojazdu (koncentracji) sił i środków. Z kolei czas dolotu (dojazdu) sił i środków do miejsca prowadzenia działań zależy, między innymi, od: długości drogi do przebycia oraz możliwej prędkości poruszania się sił i środków. Oczywistym jest, że najkrótsza droga, po których mogą poruszać się siły i środki nie oznacza najkrótszego czasu ich dojazdu.

Prowadzenie działań

Skuteczność przeprowadzenia działań przez siły i środki wydzielone do tego celu zależy od racjonalnego ich zadysponowania w zakresie ilości i wyposażenia oraz od umiejętności sprawnego ich przeprowadzenia. Przydzielenie za małych środków wydłuża czas prowadzenia akcji i zmniejsza ich skuteczność, zaś z kolei nadmiarowy przydział powoduje nieuzasadniony wzrost kosztów oraz utrudnienia organizacyjne w prowadzeniu akcji.

W przypadku podłożenia ładunku wybuchowego należy:

1. Dokonać przeszukania lub rozpoznania stanu zagrożenia i oceny sytuacji przez funkcjonariusza NGRMP.
2. Zbierać wszelkich informacji na temat miejsca zdarzenia (specyfika terenu, trasy dojazdu i odjazdu, infrastruktura mediów miejskich - wodociągi, energetyka, gazownictwo) - schemat graficzny, plany budynków, mapy topograficzne.
3. Wyznaczyć miejsce koncentracji sił odwodu oraz przysłanych z innych jednostek (np. siły wojskowe).

W przypadku podłożenia ładunku wybuchowego z zastosowaniem materiału promieniotwórczego należy:

1. Zabezpieczyć możliwość swobodnego działania sił i środków biorących udział w akcji ratunkowej poprzez m.in.: izolację terenu, umożliwienie swobody dojazdu i wyjazdu ekip ratowniczych, niedopuszczanie do zjawisk paniki, ochronę pozostawionego mienia oraz miejsc składowanego mienia porzuconego.

W przypadku podłożenia ładunku wybuchowego z zastosowaniem środka mikrobiologicznego należy:

1. Zorganizować punkty dezynfekcji, dezynsekcji, deratyzacji dla sił i środków biorących udział w akcji.
2. Zlecić identyfikację osób pierwotnie narażonych na kontakt z czynnikiem biologicznym i ich dalszych kontaktów z innymi osobami.
3. Prowadzić intensywne rozpoznanie w celu zidentyfikowania miejsca i sposobu uwolnienia czynnika biologicznego oraz ustalenia i zatrzymania sprawcy (sprawców).

4. Zabezpieczyć możliwość swobodnego działania sił biorących udział w akcji ratunkowej poprzez m.in.: izolację terenu, umożliwienie swobody dojazdu i wyjazdu ekip ratowniczych, niedopuszczanie do zjawisk paniki, ochronę pozostawionego mienia oraz miejsc składowanego mienia porzuconego.
5. Zorganizować ochranę punktów medycznych i miejsc zbiórek poszkodowanych, a także punkty pomocy humanitarnej.
6. Egzekwować zalecenia zawarte w ogłoszeniach i komunikatach kierującego działaniami ratowniczymi, a także przepisy aktów prawnych z tym związanych wydane przez władze państwowe i lokalne.

W przypadku podłożenia ładunku wybuchowego z zastosowaniem środka chemicznego należy:

1. Zorganizować punkty dezynfekcji, dezynsekcji, deratyzacji dla sił i środków własnych.
2. Ochraniać punkty medyczne i miejsca zbiórek poszkodowanych, a także punkty pomocy humanitarnej.
3. Egzekwować zalecenia zawarte w ogłoszeniach i komunikatach kierującego działaniami ratowniczymi, a także przepisy aktów prawnych z tym związane wydane przez władze państwowe i lokalne.

W przypadku uprowadzenie środka transportu w komunikacji lotniczej należy:

1. Informować na bieżąco dowódcę operacji o rozwoju sytuacji oraz o czasie do przybycia sił wsparcia.

W wariancie działania bez użycia siły

1. Zablokować dostęp podmiotów niezaangażowanych w rozwiązanie sytuacji kryzysowej (hermetyzacja portu) - wystawienie posterunków kontrolno-blokadowych.
2. Zabezpieczyć miejsca zdarzenia przez policjantów służby prewencyjnej oraz żołnierzy ŻW (pierścień zewnętrzny izolujący teren działań od zewnątrz, uniemożliwiający przedostanie się osób postronnych).
3. Utworzenie wewnętrznego pierścienia przez policjantów i żołnierzy z pododdziałów antyterrorystycznych, zabezpieczając ewentualne działania siłowe i uniemożliwiając ucieczkę porywaczy.

4. Patrolować rejon zdarzenia oraz zapewnić ochronę wydzielonych stref - ogólnodostępnej i zastrzeżonej (określonych w programie ochrony lotniska) we współdziałaniu z innymi służbami.
5. Prowadzić szczegółową kontrolę bezpieczeństwa pasażerów i ich bagażu.
6. Aktywizować działania prewencyjne na terenie całego portu lotniczego i rygorystyczne egzekwowanie obowiązujących przepisów prawa.
7. Zapewnić wsparcie służb naziemnych lotniska w ochronie pozostałych statków powietrznych.
8. Skierować zespoły negocjacyjne (podlegające dowódcy operacji), by tą drogą podejmować próbę likwidacji lub neutralizacji zagrożenia w celu:
   - - poddania się terrorystów (aresztowanie),
   - - ewakuacji pasażerów i załogi (uwolnienie),
   - - wypracowania stosownej sytuacji dla rozwiązania siłowego.

W wariancie z użyciem siły

W wariancie tym, w zależności od skali zagrożenia i jego rozwoju, przeprowadzenie operacji wymaga użycia pododdziału antyterrorystycznego (kilku w zależności od sytuacji). Metody i formy oraz sposoby prowadzenia działań przez wymienione pododdziały szczegółowo określa zarządzenie nr 6 pf Komendanta Głównego Policji z dnia 6 lutego 2003 r. w sprawie metod i form działania pododdziałów antyterrorystycznych oraz komórek minersko-pirotechnicznych Policji[141]. Dowodzący działaniami antyterrorystycznymi przygotowuje - w myśl szczegółowych przepisów - realizację zadań własnych (określając cele, organizację działań, rodzaj i sposób wykonywania zadań szczegółowych, siły i środki, zasady podległości, współdziałania i koordynacji w trakcie działań). Powyższe ustala z dowodzącym operacją i przedstawicielami innych służb. Rozwiązanie siłowe obejmuje szturm na samolot w celu:

- eliminacji powstałego zagrożenia (zatrzymanie porywaczy),
- ewakuacji pasażerów i załogi (uwolnienie).

Po zakończeniu szturmu należy:

- Udzielić pierwszej pomocy lekarskiej osobom poszkodowanym.
- Podjąć działania zmierzające do identyfikacji osób uwolnionych (syndrom sztokholmski).

---

[141] Zarządzenie NR 1429 Komendanta Głównego Policji z dnia 31 grudnia 2004 r. w sprawie wprowadzenia w Policji procedur reagowania w sytuacjach kryzysowych

- Podjąć działania zmierzające do likwidacji ewentualnych zagrożeń bombowych, pożarowych, chemicznych itd.

W przypadku uprowadzenie środka transportu w komunikacji lądowej należy:

Podjąć działania operacyjno-rozpoznawcze ukierunkowane na weryfikowanie informacji o zdarzeniu.

4. Prowadzić rozpoznania niezbędne do uzyskania informacji o:

- miejscu zdarzenia lub pościgu,
- terrorystach,
- zakładnikach,
- rodzaju środka transportu.

5. Informować na bieżąco dowódcę operacji o rozwoju sytuacji.

W wariancie bez użycia siły:

1. Wyznaczyć oraz zabezpieczyć miejsca zgrupowania dla sił własnych oraz służb ratowniczych (łącznie z lądowiskiem dla śmigłowców).
2. Odizolować strefy zagrożone z ruchu.
3. Zablokować dostęp podmiotów niezaangażowanych w rozwiązanie sytuacji kryzysowej, wystawić posterunki kontrolno-blokadowe.
4. Zabezpieczyć miejsca zdarzenia przez policjantów służby prewencyjnej oraz żołnierzy ŻW pierścieniem zewnętrznym uniemożliwiającym dostęp osób postronnych oraz ucieczkę terrorystów.
5. Skierować zespół negocjacyjny (podlegający dowódcy operacji), by tą drogą podejmować próbę likwidacji zagrożenia.

W wariancie z użyciem siły:

1. Wyznaczyć oraz zabezpieczyć miejsca zgrupowania dla sił własnych oraz służb ratowniczych (łącznie z lądowiskiem dla śmigłowców).
2. Odizolować strefy zagrożone z ruchu.
3. Zablokować dostęp podmiotów niezaangażowanych w rozwiązanie sytuacji kryzysowej, wystawić posterunki kontrolno-blokadowe.
4. Zabezpieczyć miejsca zdarzenia przez policjantów służby prewencyjnej oraz żołnierzy ŻW pierścieniem zewnętrznym uniemożliwiającym dostęp osób postronnych oraz ucieczkę terrorystów.

5. Skierować do działań pododdział antyterrorystyczny (w wariancie tym, w zależności od skali zagrożenia, przeprowadzenie operacji bezwzględnie wymaga zaangażowania właściwego wojskowego lub policyjnego pododdziału antyterrorystycznego. Metody, formy oraz sposoby prowadzenia działań przez pododdziały antyterrorystyczne określa zarządzenie nr 6 pf Komendanta Głównego Policji z dnia 6 lutego 2003 r.)[142].

- Udzielić pierwszej pomocy lekarskiej osobom poszkodowanym.
- Podjąć działania zmierzające do identyfikacji osób uwolnionych.
- Podjąć działania zmierzające do likwidacji ewentualnych zagrożeń bombowych, pożarowych, chemicznych itd.

W przypadku uprowadzenie środka transportu w komunikacji wodnej należy:

1. Podjąć na lądzie działania operacyjno-rozpoznawczych ukierunkowane na weryfikowanie informacji o zdarzeniu.
2. Prowadzić pełne rozpoznanie niezbędne do planowania rozwiązania siłowego, a dotyczące: - miejsca zdarzenia (akwen, głębokość, odległość od brzegu), - jednostki pływającej (dane techniczne, jednostki bliźniacze), - osób (pasażerów, terrorystów).
3. Informować na bieżąco dowódcę operacji o rozwoju sytuacji oraz o czasie do przybycia sił wsparcia.
4. Zablokować dostęp podmiotów niezaangażowanych w rozwiązanie sytuacji kryzysowej (izolacja portu, zabezpieczenie akwenu posterunkami pływającymi, patrolowanie śmigłowcem).
5. Aktywizować działania prewencyjne na terenie całego portu i rygorystyczne przestrzeganie przepisów prawa.
6. Zapewnić wsparcie służbami wojskowymi i policyjnymi w ochronie innych jednostek pływających.
7. Skierować zespół negocjacyjny do podjęcia próby negocjacji w celu uwolnienia zakładników, poddania się terrorystów, wypracowania dogodnej sytuacji dla rozwiązania siłowego.

---

[142] Tamże.

8. W razie konieczności zastosowanie rozwiązania siłowego (w wariancie tym w zależności od skali zagrożenia i jego rozwoju, przeprowadzenie operacji wymaga użycia wojskowego i policyjnego pododdziału antyterrorystycznego w zależności od sytuacji).
9. Udzielić pierwszej pomocy lekarskiej osobom poszkodowanym.
10. Ewakuować osoby na ląd stały (śmigłowce, jednostki pływające).
11. Podjąć działania zmierzające do likwidacji na jednostce pływającej zagrożeń bombowych, pożarowych, chemicznych.
12. Podjąć działania zmierzające do identyfikacji osób uwolnionych (wystąpienie syndromu sztokholmskiego).
13. Przywrócić ruch na zablokowanym akwenie.

W przypadku zajęcia obiektu, w tym również z przetrzymywaniem zakładników (uprowadzeniem zakładników)należy:

1. Prowadzić czynności operacyjno-rozpoznawcze
2. Szczegółowo realizować opracowany plan działania (obezwładnienia sprawców uprowadzenia osoby/osób) przez siły antyterrorystyczne.
3. Współdziałać z innymi podmiotami biorącymi udział w działaniach antyterrorystycznych oraz ratowniczych (służby wodociągowe, energetyczne, gazowe, telekomunikacyjne).
4. Brać udział w prowadzonych działaniach ewakuacyjnych osób mieszkających w sąsiednich budynkach, zapewnić bezkolizyjny przejazd grup ratownictwa medycznego i technicznego.

Powrót z miejsca zdarzenia

Środki powracające z akcji, w miarę możliwości, mogą być użyte do neutralizacji innego zdarzenia. Możliwość tę zapewnia ciągłe przesyłanie informacji o stanie środków (statusy środków) i ich bieżącym położeniu (GPS).

Zakończenie działań

Zakres czynności wykonywanych w tym etapie obejmuje:

- sporządzenie dokumentacji (sprawozdania) z przeprowadzonej akcji;
- odtworzenie stanu zdatności sił i środków uczestniczących w akcji do prowadzenia kolejnych działań.

ZAKOŃCZENIE

Podsumowując całość badań podjętych w ramach niniejszej pracy należy stwierdzić, że w dającej się przewidzieć perspektywie czasu 20-25 lat najprawdopodobniej zagrożenia terrorystyczne państwa, a szczególnie miast polskich będą narastać wraz z rozwojem techniki i technologii pozwalającej terrorystom na globalne transgraniczne ponadnarodowe oddziaływanie.

Polska podtrzymując swe zaangażowanie w walkę ze światowym terroryzmem liczyć się musi z koniecznością prowadzenia tej walki także na terytorium kraju. Tworzony, krajowy system antyterrorystyczny musi działać za pomocą wyspecjalizowanych sił i środków rozmieszczonych w zintegrowanych wewnętrznie i skoordynowanych zewnętrznie strukturach. System ten musi być zasilany informacyjnie, rzeczowo, osobowo w ramach systemu bezpieczeństwa państwa, którego stanowi ważny element. Poza podstawowymi funkcjami monitorowania i analizy sytuacji, informowania i reagowania, przedmiotowy system powinien być zdolny do przyjęcia działań wspomagających prowadzonych przez całe społeczeństwo według zasady: globalnemu zagrożeniu należy się globalnie przeciwstawiać. Zarys takiego właśnie systemu zawarto w rozdziale piątym koncepcyjnym niniejszej pracy.

W pracy wykonano wszystkie założone zadania badawcze: scharakteryzowano militarne i niemilitarne podmioty państwa przeciwstawiające się zagrożeniom terrorystycznym miast polskich, wyjaśniono sposób zarządzać ryzykiem w systemie cywilno-wojskowej ochrony miast polskich w warunkach zagrożeń terrorystycznych, opisano metody, sposoby przeciwdziałania podejmowane w systemie cywilno-wojskowym, a chroniące elementy infrastruktury krytycznej miast polskich przed atakiem terrorystycznym lub minimalizujące jego skutki, wreszcie zaproponowano koncepcję systemu ochrony miast polskich zapewniającą sprawne jego działania w warunkach zagrożeń terrorystycznych.

Można zatem uznać, że rozwiązano główny problem badawczy pracy: do czego zmierzający, przy pomocy jakich środków i technologii działania cywilno-wojskowy system antyterrorystyczny zapewni możliwie najpełniejszą ochronę miast polskich przed atakami terrorystycznymi? i osiągnięto założony cel obydwu etapów badań.

Jednak wszystkie rozwiązane problemy naukowe spowodowały powstanie kilkunastu następnych wymagających rozwiązania w toku dalszych badań. Za te najpilniejsze z nich zespół autorski uznał konieczność przeprowadzenia, na kanwie pod-

stawy teoretycznej niniejszej pracy, przeprowadzenie szczegółowych badań zmierzających do zoptymalizowania zastosowanych w koncepcji cywilno-wojskowego systemu antyterrorystycznego rozwiązań.

BIBLIOGRAFIA

1. Agencja Bezpieczeństwa Wewnętrznego rok po reformie (lipiec 2003), http://www.abw.gov.pl/Raporty/raport_02.htm.
2. Bolechów B., Terroryzm w świecie podwubiegunowym, Toruń 2002.
3. Center for Chemical Process Safety SVA, CCPS Equivalent Methods (Exxon-Mobil Chemical, BASF, Air Products, Georgia Pacific), Sandia National Lab VAM-C F: Guidelines for analyzing and managing the security vulnerabilities of fixed chemical sites, New York, August 2002
4. Chloupek I., Sztandar dla GROM-u, „MMS Komandos", nr 11, Kraków 1996.
5. Chyła L., Grabarczyk Z., Samorański W., Czyżykowski Z., Służba w polskich misjach specjalnych ONZ, Informator, dodatek do nr 11 „Przeglądu Wojsk Lądowych", Warszawa 1996.
6. Dennison B., Zarządzanie ryzykiem w sektorze publicznym. Podręcznik wdrożenia systemu zarządzania ryzykiem w administracji publicznej w Polsce. Wyd. Ministerstwo Finansów 2004r.
7. Doktryna Operacji Specjalnych Unii Europejskich EU SOF.
8. Doktryna Połączonych Operacji Specjalnych AJP 3.5 (final draft).
9. European Union Special Operations Forces Doctrine, October 2007.
10. Filar M., Terroryzm w polskim prawie karnym na tle prawa międzynarodowego i porównawczego, (w:) pod. red. R.Bäcker, Od Blokad ulicznych do World Trade Center, Toruń 2002 r.
11. Gołota C., Struktura organizacyjna i zadania Policji polskiej, Szczytno 1994.
12. Góralski D., Liedel K., System przeciwdziałania terroryzmowi w Polsce, (w:) pod red. K. Liedela, J. Marszałek-Kawa., Sz. Wudarski, Polityczne metody zwalczania terroryzmu, Toruń 2006 r.
13. Hadyś T., Rola i zadania Straży Granicznej w przeciwdziałaniu zagrożeniom terrorystycznym. Wyd. Zeszyty Naukowe AON, 2003r., nr 1 (50)A.
14. Hoffman B., Oblicza terroryzmu, Warszawa 2001.
15. Jałoszyński K., Krajowe pododdziały antyterrorystyczne – historia i dzień dzisiejszy, „Policja" 2000, Nr 1-2.
16. Jenkins B. M., The Likelihood of Nuclear Terrorism, RAND Corporation P-7119, Santa Monica, lipiec 1986.

Regulacje dotyczące Towarów Niebezpiecznych, wydanie 47, 1 stycznia-31 grudnia 2008r.

32. Polityka NATO w zakresie operacji specjalnych MC 437/1.
33. Polska wobec terroryzmu, Instytut Studiów Strategicznych, Zeszyt nr 49, Kraków 2002 r.
34. Praca zbiorowa Zintegrowany system ratowniczy w czasie pokoju. Państwowa Straż Pożarna jako główna siła w Krajowym Systemie Ratowniczo – Gaśniczym, WKO AON, Warszawa 1996.
35. Rak J.; Tchórzewska – Cieślak B.., Metody analizy i oceny ryzyka w systemie zaopatrzenia w wodę. Oficyna Wydawnicza Politechniki Rzeszowskiej, Rzeszów 2005.
36. Rak J.R., Wybrane elementy zarządzania ryzykiem w przedsiębiorstwie wodociągowym. Ochrona środowiska Nr4 2007r.
37. Red. nauk. Gryz J., Kwećka R., Współczesny wymiar terroryzmu przeciwdziałanie zjawisku, Wyd. AON. 2007r.
38. Ryan M., Mann C., Stilwell A., Encyklopedia oddziałów specjalnych, Taktyka, historia, strategia, uzbrojenie, Bellona, Warszawa 2003.
39. Rybak J., Eksportowi żołnierze, (w) „Żołnierz Polski", nr 1–2, Warszawa 2003.
40. Rybak J., Grom.pl: Tajne operacje w Afganistanie, Zatoce Perskiej i Iraku, „Jeden Świat", Warszawa 2005.
41. Rybak J., Grom.pl: Tajne operacje w Afganistanie, Zatoce Perskiej i Iraku, „Jeden Świat", Warszawa 2005.
42. Rybak J., Komandosi, jednostki specjalne Wojska Polskiego, Bellona, Warszawa 2003.
43. Schroeder M., Płotica M., Żuber J., Krajowy System Ratowniczo – Gaśniczy w systemie bezpieczeństwa państwa. Czy jesteśmy bezpieczni?, KG PSP KCKR, Warszawa 1994.
44. Sienkiewicz P., Podstawy teorii systemów, Warszawa 1993r.
45. Skuza A., Teoretyczne założenia systemu szkolenia pododdziałów specjalnych, „Zeszyty Naukowe" WSO Szczytno 1988, Nr 1/60.
46. Wasilewski A., Kuleta D., Żydowo P., Bezpieczeństwo europejskie a polskie siły zbrojne, (w) „Myśl Wojskowa", maj - czerwiec, Bellona, Warszawa 2006.
47. Weinberger C., Schweizer P., Następna wojna światowa, ALBATROS, Warszawa 1998r.

48. Wright Mills C.. The Power Elite. Oxford University Press 1956.
49. Wróblewski D., Model współdziałania jednostek Państwowej Straży Pożarnej z jednostkami Obrony Cywilnej w zakresie działań ratowniczych, rozprawa doktorska, Warszawa, AON 2001r.
50. Żywczyk M., Szkolenie funkcjonariuszy pododdziałów specjalnych MO przeznaczonych do fizycznego zwalczania terroryzmu, „Zeszyty Naukowe" WSO Nr 1/60. Szczytno 1988r.

AKTY PRAWNE

1. Decyzja Ministra Spraw Wewnętrznych z dnia 28 lutego 1976 r. w sprawie utworzenia Wydziału Zabezpieczenia Komendy Stołecznej Milicji Obywatelskiej do zwalczania aktów przemocy.
2. Decyzja Nr 296 Komendanta Głównego Policji z dnia 29 grudnia 2000 r. w sprawie powołania pododdziałów antyterrorystycznych Policji.
3. Decyzja Nr 5/04 Dyrektora Głównego Sztabu Policji z dnia 29 czerwca 2004 r.
4. Decyzja Nr Pf 74/Org./SSG/ZOiU-P1 Ministra Obrony Narodowej z dnia 2.12.2008r. w sprawie sformowania Jednostki Wsparcia Dowodzenia i Zabezpieczenia Wojsk Specjalnych.
5. Dziennik Ustaw" nr 172 z 2004 r., poz. 1805.
6. Dziennik Ustaw" nr 7 z 2002 r., poz.58.
7. Dziennik Ustaw" nr 74 z 2002 r., poz. 676.
8. Konstytucji RP z dnia 2 kwietnia 1997 roku – (Dz. U. Nr 78 z 1997 r., poz. 483).
9. Monitor Polski" nr 44 z 2003 r., poz. 656.
10. Rozporządzenie Ministra Obrony Narodowej z dnia 26 lipca 2006 r.w sprawie postępowania kwalifikacyjnego wobec kandydatów do służby w Służbie Wywiadu Wojskowego
11. Rozporządzenie Ministra Obrony Narodowej z dnia 27 września 2006 r. w sprawie szczegółowego sposobu żądania pomocy lub zwracania się o tę pomoc przez żołnierzy i funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego
12. Rozporządzenie Ministra Obrony Narodowej z dnia 28 września 2006 r. w sprawie szczegółowych zasad i trybu szkolenia zawodowego funkcjonariuszy Służby Wywiadu Wojskowego

13. Rozporządzenie Ministra Spraw Wewnętrznych i Administracji z dnia 22 września 2000 roku w sprawie szczegółowych zasad wyposażenia jednostek organizacyjnych Państwowej Straży Pożarnej Dz. U. z 2000 r., nr 93.
14. Rozporządzenie Prezesa Rady Ministrów z dnia 4 października 2006 r. w sprawie współdziałania Służby Kontrwywiadu Wojskowego i Służby Wywiadu Wojskowego z odpowiednimi organami, służbami i instytucjami uprawnionymi do wykonywania czynności operacyjno-rozpoznawczych
15. Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie stanowisk mających istotne znaczenie dla bezpieczeństwa jądrowego i ochrony radiologicznej oraz inspektorów ochrony radiologicznej (Dz. U. nr 21, poz. 173).
16. Rozporządzenie Rady Ministrów z dnia 18 stycznia 2005 r. w sprawie planów postępowania awaryjnego w przypadku zdarzeń radiacyjnych (Dz. U. Nr 20. poz. 169) .
17. Rozporządzenie Rady Ministrów z dnia 2 lipca 2002 r.Dz.U.02.103.929
18. Rozporządzenie Rady Ministrów z dnia 27 września 2006 r. w sprawie postępowania przy użyciu broni palnej przez żołnierzy i funkcjonariuszy Służby
19. Rozporządzenie Rady Ministrów z dnia 31 lipca 2001 w sprawie szczegółowych zasad kierowania i współdziałania jednostek ochrony przeciwpożarowej biorących udział w działaniu ratowniczym, Dz. U. z 2001 nr 82 poz. 895.
20. Rozporządzenie szefa MSWiA z dnia 19 grudnia 2005r.,Dz.U. Nr 266 poz. 2243.
21. Ustawa o Policji z dnia 6 kwietnia 1990 roku (tj. Dz. U. Nr 7, poz. 58 z późn. zm.)
22. Ustawa z dnia 11 września 2003 r. o służbie wojskowej żołnierzy zawodowych
23. Ustawa z dnia 12 października 1990 r. o Straży Granicznej (Dz. U. nr 78 poz. 462).
24. Ustawa z dnia 16 marca 2001r. o Biurze Ochrony Rządu, Dz. U. z 2004r., nr 163, poz. 1712
25. Ustawa z dnia 22 stycznia 1999 o ochronie informacji niejawnych, http://www.iniejawna.pl
26. Ustawa z dnia 24 maja 2002r. o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu, Dz. U. z 2002r., nr 74, poz. 676
27. Ustawa z dnia 24 sierpnia 1991 r. o Państwowej Straży Pożarnej, Dz. U. z 2009, Nr 12 poz. 68

28. Ustawa z dnia 24 sierpnia 2001 r. o Żandarmerii Wojskowej i wojskowych organach porządkowych (Dz. U. nr 123 z 2001 r., poz. 1353 z późn. zm.)
29. Ustawa z dnia 9 czerwca 2006 r. o służbie funkcjonariuszy Służby Kontrwywiadu Wojskowego oraz Służby Wywiadu Wojskowego
30. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz o Służbie Wywiadu Wojskowego (Dz. U. Nr 104, poz. 709 i Nr 218, poz. 1592).
31. Ustawa z dnia 9 czerwca 2006 r. o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego
32. Ustawa z dnia 9 czerwca 2006 r. Przepisy wprowadzające ustawę o Służbie Kontrwywiadu Wojskowego oraz Służbie Wywiadu Wojskowego
33. Zarządzenie Komendanta Głównego Policji Nr 14/00 z dnia 18 października 2000 r. zmieniające zarządzenie w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji.
34. Zarządzenie Komendanta Głównego Policji Nr 6/90 z dnia 3 sierpnia 1990 r. w sprawie organizacji oddziałów prewencji i pododdziałów antyterrorystycznych Policji.
35. Zarządzenie Ministra Obrony Narodowej z dnia 28 maja 2008 r. w sprawie nadania statutu Służbie Wywiadu Wojskowego
36. Zarządzenie Ministra Spraw Wewnętrznych Nr 067/90 z dnia 3 lipca 1990 r. w sprawie uchylenia niektórych tajnych i tajnych specjalnego znaczenia aktów normatywnych obowiązujących w resorcie spraw wewnętrznych.
37. Zarządzenie Nr 1429 Komendanta Głównego Policji z dnia 31 grudnia 2004 r. w sprawie wprowadzenia w Policji procedur reagowania w sytuacjach kryzysowych
38. Zarządzenie Nr 25 Komendanta Głównego Policji z dnia 31 grudnia 2002 r. w sprawie szczegółowych zasad organizacji i zakresu działania komend, komisariatów i innych jednostek organizacyjnych Policji (Dz. Urz. KGP z 2003 r. Nr 2, poz. 4, zmiany: Dz. Urz. Z 2003 r. Nr 22, poz. 127 i z 2004 r. Nr 10, poz. 44).
39. Zarządzenie nr 54 Prezesa Rady Ministrów z dnia 30 kwietnia 2002, niepublikowane
40. Zarządzenie MON nr Z-8 z dnia 15.02.2007 r. w sprawie siedziby i szczegółowego zakresu działania Dowództwa Wojsk Specjalnych.

41. Ustawa z dnia 24 maja 2007 r. o zmianie ustawy o powszechnym obowiązku obrony Rzeczpospolitej Polskiej oraz o zmianie niektórych innych ustaw.
42. Decyzja Ministra Obrony Narodowej Numer Pf-74/Org./SSG/ZOiU-P-1 z dnia 2 grudnia 2008 roku w sprawie sformowania Jednostki Wsparcia Dowodzenia i Zabezpieczenia Wojsk Specjalnych.

ŹRÓDŁA INTERNETOWE

1. http://abw.gov.pl.
2. http://airport-poznan.com.pl/pl/slownik.html, 28.05.2009.
3. http://bip.abw.gov.pl/palm/bip/19/18/Kolegium_ds_sluzb_specjalnych.html
4. http://bor.gov.pl.
5. http://grom.mil.pl/cichociemni_pliki/cichociemni.htm.
6. http://kgpsp.gov.pl
7. http://liedel.pl/terroryzm.20.04.2007 r.
8. http://mfiles.pl/pl/index.php/Ryzyko
9. http://mswia.gov.pl/aktual_150904_raport.html.
10. http://policja.pl/portal/pol/560/Biuro_Operacji_Antyterrorystycznych.html
11. http://specops.pl/vortal/taktyka_czarna/walka_z_terrorem/Michal_Piekarski/terrorist_tactics/terrorist_tactics.htm
12. http://wikipedia.org/wiki/ Zarządzanie _ryzykiem_(projektowanie).
13. http://wikipedia.org/wiki/Ryzyko
14. http://wikipedia.org/wiki/Zarządzanie_ryzykiem
15. http://wojskaspecjalne.mil.pl.

WYKAZ TABEL

Tabela 1. Typy i znaczenie potencjalnych zagrożeń 83
Tabela 2. Skala opisowa prawdopodobieństwa 101
Tabela 3. Skala opisowa skutków 101
Tabela 4. Skala opisowa skutków w zależności od zdarzenia 102
Tabela 5. Skala punktowa standardowej matrycy ryzyka 108
Tabela 6. Skala punktowa dla zdarzeń zawartych w tabeli 3 108
Tabela 7. Pożądane cechy i zdolności sił przeciwterrorystycznych w kontekście obszarów determinujących ich użycie w aglomeracjach miejskich 114
Tabela 8. Skutki napromieniowania-dawki jednorazowe na całe ciało pochłonięte w krótkim okresie czasu 160
Tabela 9. Przypadki ujawnionych prób nielegalnego przewozu materiałów radioaktywnych w Porcie Lotniczym Warszawa 161

WYKAZ RYSUNKÓW

Rys. 1. Schemat tworzenia pododdziału antyterrorystycznego 31

Rys. 2. Organizacja pododdziału antyterrorystycznego. 33

Rys. 3. Rozmieszczenie jednostek antyterrorystycznych Policji 35

Rys. 4. Struktura organizacyjna Komendy Głównej Straży Granicznej 39

Rys. 5. Struktura organizacyjna Komendy Głównej PSP 48

Rys. 6. Docelowa struktura Wojsk Specjalnych wraz z ich podległością 57

Rys. 7. Struktura organizacyjna Żandarmerii Wojskowej. 64

Rys. 8. Struktura organizacyjna Oddziału Specjalnego ŻW 74

Rys. 9. Elementy zabezpieczeń przed nieupoważnionymi działaniami stron trzecich 80

Rys. 10. Wymagane kroki SVA podczas analizy sił i środków do przeciwdziałania zagrożeniom terrorystycznym miast polskich 81

Rys. 11. Powiązania pomiędzy etapami w procesie zarządzania ryzykiem 94

Rys. 12. Schemat zarządzania ryzykiem w ochronie miast polskich w warunkach zagrożeń terrorystycznych. 100

Rys. 13. Schemat ideowy podkładanych urządzeń wybuchowych 136

Rys. 14. Obowiązkowe oznakowanie umieszczane na pojazdach przewożących materiały radioaktywne do portu lotniczego 155

Rys. 15. Pojemnik stosowany w transporcie lotniczym do przewozu materiałów promieniotwórczych o niskiej aktywności właściwej 156

Rys. 16. Oznaczenia przesyłek z materiałami promieniotwórczymi w transporcie lotniczym 159

Rys. 17. System cywilno – wojskowej ochrony miast polskich w warunkach zagrożeń terrorystycznych 168

Rys. 18. Cywilno – wojskowy system ochrony miast polskich w warunkach zagrożeń terrorystycznych 169

Rys. 19. Model systemu ochrony miast w warunkach zagrożeń terrorystycznych .. 170

Rys. 20. Ogólny schemat działania systemu ochrony miast podczas prawdopodobieństwa wystąpienia zdarzenia 173

BIBLIOTEKA GŁÓWNA - ARCHIWUM
Nr ewid. 74984
II
Akademii Obrony Narodowej